BeyondTrust

Privileged Remote Access
Disaster Recovery

TC:2/8/2019

Table of Contents

BeyondTrust PRA Appliance Disaster Recovery

Two key concerns of any strategic hardware deployment are availability and up-time. In the event of a disaster, recovery time can be decreased if the necessary steps have already been taken to prepare for such an event. Please follow the best practices outlined in this guide to prepare for any issues that might arise with the BeyondTrust Appliance and to minimize downtime.

BeyondTrust Support

BeyondTrust Support is responsible for supporting BeyondTrust products worldwide and is available to help resolve any incidents experienced while using BeyondTrust products. It is important to understand the role of BeyondTrust Support in a disaster recovery situation. Incidents should be reported to BeyondTrust Support via chat, phone, or incident form at help.bomgar.com. Some of these options require a login, which is given to existing customers upon purchasing BeyondTrust. Anyone can email BeyondTrust Support, even without purchasing BeyondTrust, using any of the following three email addresses:

- General email: support@bomgar.com
- EMEA region: emea.support@bomgar.com
- APAC region: apac.support@bomgar.com

BeyondTrust offers support in English during our normal business hours from 2:00 AM to 7:00 PM CST/CDT, Monday - Friday. The site help.bomgar.com is available 24 hours a day to provide assistance.

BeyondTrust observes the following holidays (USA):

Holiday	Date
New Year's Day	January 1st
Martin Luther King Day	Third Monday in January
President's Day	Third Monday in February
Good Friday	Varies
Memorial Day	Last Monday in May
Independence Day	July 4th
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veterans Day	November 11th
Thanksgiving Day	Fourth Thursday in November
Day after Thanksgiving	Fourth Friday in November
Christmas Eve	December 24th
Christmas Day	December 25th

Note: *If the holiday falls during a weekend, the nearest weekday is observed instead.*

Support Process

BeyondTrust's support process ensures incidents with BeyondTrust products are handled and resolved efficiently and professionally. BeyondTrust Support provides solutions, workarounds, knowledge transfer, and appropriate, timely status updates to BeyondTrust customers. When an incident occurs and requires additional information about BeyondTrust products, information about any BeyondTrust product can be found online at www.beyondtrust.com/docs. Incidents reported outside of BeyondTrust's normal support hours are considered to be received at the beginning of the next business day. As a general rule, the more specific the details provided, the better chance the BeyondTrust Support representative will be able to provide a resolution quickly. If a support request is open with BeyondTrust and an email correspondence is necessary, the subject of the email should begin with **Incident #**, followed by the incident number (e.g., Incident# 40100).

When submitting an incident, please include the following information:

- **Inquirer's Name**
- **Name of the organization**
- **BeyondTrust product version**
- **Specific error messages received**
- **Steps for reproducing the issue**
- **Actions taken prior to the incident**
- **Changes made to the BeyondTrust product** (such as information about the network environment and workstation involved with the issue)
- **Length of time the issue has persisted**
- **Operating system** (if software-related)
- **Assigned server roles** (if server-related)
- **Log files**
- **Screen shots**

When an incident or request is submitted, it is logged and is given an incident number and a severity rating. The content of the incident initially supplied is used to identify the incident severity level. Severity levels range from **Severity Level 1** (critical) to **Severity Level 3** (low priority). In collaboration with the customer, BeyondTrust Support makes a reasonable determination of the severity level for the incident and responds accordingly. The severity level may also be adjusted as the incident progresses towards a resolution.

Severity Level	Basic Description	Reporting and Response	Roles and Responsibilities
Severity Level 1	Production system down and inoperable. The issue cannot be solved by a restart, a bypass, or a workaround.	Incident must be documented via email and followed up by telephone call. Maximum target time for First Response (start of resolution) is 30 minutes. Maximum target time for Customer Response Time is 30 minutes.	Both parties will make all commercially reasonable attempts to focus support resources on Severity Level 1 issues.
Severity Level 2	Production system is operational but impacted due to issue with documented product functionality. Workaround exists for core product functionality.	Incident must be reported via email to document the issue and may be followed up by telephone. Maximum target time for First Response (start of resolution) is 24 hours. Maximum target time for Customer Response Time is 24 hours.	Both parties will make all commercially reasonable attempts to focus support resources on Severity Level 2 issues during BeyondTrust Support's normal support hours.
Severity Level 3	Cosmetic impairment. Limited impact to use of system. No immediate resolution required. Request for enhancements. Request for general information.	Incident must be reported via email. Maximum target time for First Response (start of resolution) is 24 hours.	Solutions provided for cosmetic, enhancements, or other incidents are possibly implemented in future versions, depending on the product road map.

Response times are based on normal business hours, unless otherwise noted. **First Response** is the time frame, within normal business hours, that BeyondTrust Support is able to respond to the reported incident. Valid responses include but are not limited to providing a solution or a work-around. **Customer Response** is the time frame in which a customer should respond to BeyondTrust Support after a request for additional information has been made. **Failure to Respond** within the Customer Response Time results in a lower priority level being placed on the issue.

BeyondTrust Support verifies that a current maintenance agreement with BeyondTrust is in effect and that they are speaking with a valid company representative. If either of these cannot be validated, BeyondTrust Support is unable to provide any further support. If multiple items are submitted at one time, individual incidents may be opened for each item. BeyondTrust recommends reporting all **Severity Level 1** incidents initially with a detailed email to support@bomgar.com followed by a telephone call.

Responses to incidents occur within the response times designated for the incident's severity level. Responses received may include any of the following:

- **The information requested or an immediate resolution**
- **Indication that the incident is a known issue**
- **Request for additional information**
- **Explanation of a feature or design decision**
- **Links to a published technical document**
- **Software patch or upgrade with instructions**
- **Resolution options**
- **Confirmation that the feature request was logged with Product Management**

If BeyondTrust Support indicates the problem is a known issue, explanation of when a product fix will be available along with any available workarounds is provided. Common examples of additional information BeyondTrust Support requests include:

- **Details about the problematic behavior or environment**
- **Specific tests to isolate the issue or instructions for generating detailed logs**

If no further information or action is necessary, BeyondTrust Support sets the incident status to **Resolved Pending Confirmation**. At this point, the incident closes automatically in a few days. A notification is sent prior to closing. If further action and/or information is necessary to resolve the incident, BeyondTrust Support sets the status to **Customer Information Requested** or **Software Change Required**. These incidents also auto-close if no response is received, but a notification is sent by email prior to closure.

Once an incident has been closed, it can be re-opened whenever necessary, or a new incident can be opened. BeyondTrust does not bill on a per-incident basis. When your incident requires a more in-depth technical resource, it escalates to a Product Support Engineer. As necessary, the Product Support Engineer works with additional resources to bring the incident to a timely resolution. At any point in the support process, a request can be made to speak to a support supervisor or support manager. BeyondTrust Support is very interested in receiving feedback from our customers about any support process. At any time, an email can be sent to support@bomgar.com, support.supervisor@bomgar.com, or support.manager@bomgar.com with comments and suggestions. BeyondTrust Support may additionally provide survey opportunities on a per-incident or per-support session basis.

Service Limitations

As an authorized account representative requesting support, you have several responsibilities to ensure the support process goes smoothly:

- **Provide Contact:** During the initial evaluation or purchase process, the authorized contact is responsible for indicating which individual(s) are the primary technical contacts for all product updates. The technical contact person needs to have solid, relevant network and server administration experience, to have an accurate understanding of the network environment and to have obtained a level of competence with the BeyondTrust software.
- **Track BeyondTrust Updates:** While BeyondTrust Support does their best to communicate product updates and changes, it is the responsibility of the authorized contact to review the BeyondTrust Support Portal, the BeyondTrust Change Log, and other various marketing materials for any available software updates.
- **Follow Backup Procedures:** As a BeyondTrust customer, the authorized contact agrees to keep full and current backups of BeyondTrust data, using the tools provided. It is extremely important to perform backups prior to any upgrades or updates.
- **Read Documentation:** Authorized contacts are responsible for utilizing the latest documentation provided via www.beyondtrust.com/docs, the BeyondTrust Support Portal, and/or email for handling and operating the BeyondTrust software.
- **Comply with Instructions:** When BeyondTrust Support communicates with authorized contacts, it is expected that a commercially reasonable effort has been made to both comprehend the material and execute any instructions provided.
- **Report in Detail:** Before submitting an incident report, it is expected that any changes made to the BeyondTrust Appliance and the environment have been documented and a reasonable attempt has been made to reproduce the reported incident, if appropriate. In order to provide an efficient resolution to the incident reported, an accurate and detailed account must be provided about the issue, and all responses to BeyondTrust Support must occur in a timely fashion when additional information is requested.
- **Provide Qualified Staff:** When participation or access to staff is needed to arrive at a satisfactory resolution, the staff member (s) must be available at times mutually agreed upon. It is the responsibility of the authorized contact that staff members assigned to work with BeyondTrust Support possess the required skills, experience, equipment, and/or administrative access required to assist in resolving the incident.

When failing to fulfill any of the responsibilities, BeyondTrust Support reserves the right to revise the timetable for the delivery of support services. In this event, a notification is sent.

BeyondTrust Support does not provide services that include or result from:

- **Uses of or changes to your BeyondTrust hardware or software not explicitly authorized by BeyondTrust or the EULA.**
- **Network, systems, operation, or other environmental factors not within the direct control of BeyondTrust.**
- **Failure to install product updates according to the instructions provided.**
- **Consultative advice and assistance, such as:**
  - **Configuration/reconfiguration of new or existing network equipment.**
  - **Customization of the BeyondTrust product, including the public portals' graphics and layout.**
  - **Programming code or code snippets for use in customizing BeyondTrust public portals or integrations with BeyondTrust.**
- **Services related to non-BeyondTrust products including any updates required for compatibility with BeyondTrust products.**

Release Versions

BeyondTrust Engineering is constantly working to enhance its products by making improvements to the existing feature set, as well as adding new ones. BeyondTrust's goal is to provide the best products to our customers. To achieve this goal, BeyondTrust continues to add new features and to release new versions of products. As BeyondTrust provides newer versions, older versions are retired according to a planned schedule. New appliances are delivered with the latest version available at the time of purchase. BeyondTrust uses the combined values of X and Y numerals in X.Y to denote a major version (e.g. 15.2). A maintenance version is denoted by Z in X.Y.Z (15.2.2). Maintenance versions are subsumed under their corresponding major versions for the purposes of support.

BeyondTrust provides support for any major product versions for a minimum of two years from the generally available (GA) release date. During the two-year life cycle, there may be several maintenance versions associated with the active major version. A GA release and all associated maintenance releases are retired after two years. There may be occasions that dictate BeyondTrust choosing a later date for retirement, but this is an exception. Retired versions may be upgraded to the latest version but are no longer supported unless specifically noted.

BeyondTrust Cloud customers have the ability to install released BeyondTrust software updates when they are made available. During the BeyondTrust Cloud installation process, the administrator elects to participate in one of two update schedules. These automated upgrade schedules apply when an available BeyondTrust software release has not been applied manually before the scheduled time.

- **Level 1:** If no explicit choice was made, the default option is for a BeyondTrust Cloud appliance to be updated two weeks after any BeyondTrust Software version is released.
- **Level 2:** If this option was selected, the BeyondTrust Software is updated five months after each major BeyondTrust Software version is released.

With either option, authorized contacts are notified no less than one week before a scheduled upgrade is to take place.

Any critical security update is applied immediately to all BeyondTrust Cloud customers regardless of the level chosen above. A security update must be deemed critical by the BeyondTrust Security team before being approved for deployment in this manner.

Back Up Procedures

Backing up the site data from BeyondTrust on a regular basis is an essential part of appliance administration and maintenance. Most of the settings and data from the /login administrative web interface can be captured as a single .nsb file. In most cases, the /appliance administrative web interface contains the SSL certificates and network configuration of the appliance. These are essential to the functionality of the appliance and must be configured during the recovery process.

With the exception of certificates, /appliance configuration cannot be downloaded as a single, password-protected file in the way /login configuration can. The /appliance configuration must be backed up using screenshots and/ or text data. These files should be given an identifying name, including the appliance version, appliance serial number, base software version, and system time as shown on the **Status** page of the appliance at the time of the backup.

BeyondTrust-hosted sites do not have access to /appliance, but administrators should maintain backups of hosted site /login data. BeyondTrust Cloud sites have a minimal version of the /appliance web interface accessible from the **Appliance** tab of the /login administrative web interface. Since BeyondTrust manages the network configuration of BeyondTrust Cloud sites and provides a working default certificate, BeyondTrust Cloud administrators need to backup only their certificates, SSL/TLS configuration, and/or updates schedule, if these have been manually customized.

Failover

BeyondTrust failover enables the synchronization of data between two peer appliances, creating a simplified process for securely swapping from a failed appliance. Two appliances host the same installed software package for a single site. DNS directs support traffic of the site to one of these peer appliances, the primary appliance, where all settings are configured. The backup appliance synchronizes with the primary appliance, according to the settings configured in the appliance's /login interface. To set up failover between appliances, refer to Failover Dynamics and Options at www.beyondtrust.com/docs/remote-support/how-to/failover.htm .

Once two appliances are in failover mode, the backup of settings and data from the primary to the backup should occur.

1. Log into the /login admin web interface of the backup appliance.
2. Browse to **Management > Failover**.
3. Check **Enable Backup Operations**.

   > ***Note: Automatic Data-Sync Interval*** *and* ***Data-Sync Bandwidth Limit*** *do not need to be changed in most environments.*

4. Click **Sync Now** to manually force synchronization under the **Backup Site Instance Status**. Failover sync captures all users, files, and configuration in /login with the exception of failover configurations, including settings on the **Failover** page and the **Inter-Appliance Pre-Shared Key** under **Management > Security**.

It is important to note that failover appliances do not sync any settings or data under /appliance. This means that certificates and network configuration are not replicated. It is not necessary to back up certificates from each appliance; however, failover appliances should have identical certificate configuration. Once replicated, a single backup copy of the certificates from either appliance is sufficient. Network configuration and any other customized /appliance settings must be backed up for each appliance; however, /login data can be backed up for each appliance as well. This applies especially to failover settings, which are not included in the failover sync. Saving backups of /login settings serves as a safeguard in case failover sync fails.

Back Up Certificates

Network configuration and SSL certificates are necessary for the operation of BeyondTrust Appliances. BeyondTrust-hosted sites and cloud appliances are managed automatically, but it is possible for administrators to install custom certificates on Cloud Appliances. If

an appliance fails, network configuration and SSL certificates must be restored to the new or repaired appliance in order to connect with the remote client software (e.g., rep consoles and Jump Clients). BeyondTrust-hosted sites are managed by BeyondTrust, but administrators of on-premises and Cloud Appliances should back up their certificates.

The SSL certificate issued to the BeyondTrust Appliance hostname is often unique to the appliance and is always used to validate its identity to remote client software. It is important that a backup of this certificate, all its intermediate certificates, and its root certificate are saved. Certificates are documented further in the article SSL Certificates and BeyondTrust at www.beyondtrust.com/docs/remote-support/how-to/sslcertificates.htm. The certificate backup file should be saved with a password in a secure location because in the event a malicious party obtaining a copy of this certificate, they could potentially access confidential data on the network.

1. To back up the appliance certificate(s), log into the /appliance administrative web interface.
2. Browse to **Security > Certificates**.
3. Locate the certificate with the **Alternative Names** of the appliance hostname.
4. With the **IP Address(es)** of the appliance, verify that the **Private Key?** field reads **Yes**.
5. Check the box next to the certificate.
6. From the **Export from the** dropdown, click **Apply**.
7. Wait for the export page to load.
8. Check **Include Certificate**, **Include Private Key**, and **Include Certificate Chain**.
9. Enter a **Passphrase**.
10. Click **Export**.
11. Save the resulting .p12 certificate file in a secure location.

Back Up /appliance

Network configuration for BeyondTrust should be saved by the networking team in a network diagram. This should include firewall rules, antivirus whitelists, and IDS /IPS settings, as appropriate. A backup copy of the appliance network configuration can be saved by taking screenshots of the /appliance **Networking > IP Configuration** page. If static routes and/or SNMP are used, this information is captured from the **Networking > Static Routes** and **Networking > SNMP** pages, respectively. BeyondTrust Cloud customers and BeyondTrust-hosted sites do not have these options and do not need to be backed up. They are managed automatically.

If the appliance has custom SSL/TLS configuration or special user account, network, and/or port restrictions, take a screenshot of these from **Security > SSL/TLS Configuration** and **Security > Appliance Administration**. The appliance may also be configured to send logs to a syslog server. If this is the case, make note of the syslog server's hostname and/or IP along with its preferred message format. These settings can be found under **Security > Appliance Administration** in the **Syslog** section.

Certain companies have policies requiring users to accept legal agreements before accessing certain interfaces, such as the BeyondTrust /appliance administrative web interface. If the appliance is configured with such an agreement, the agreement is located under **Security > Appliance Administration > /appliance Prerequisite Login Agreement**. If it is configured, capture a screenshot of the agreement.

The appliance may also be configured with an SMTP server for sending email. The email configuration settings in /appliance are located in **Security > Email Configuration**. These settings are separate from the email configuration settings in /login. The /appliance email settings are used by the appliance to send SSL certificate expiration reminders. If the appliance is configured for reminders, take a screenshot of the page.

Back Up /login

The users, settings, and data in /login can be saved in a single BeyondTrust backup file, which uses the .nsb extension. This file can be generated from the BeyondTrust API, from the BeyondTrust integration client, or from the /login administrative web interface. BeyondTrust recommends manually downloading .nsb backups before installing any updates. To perform manual downloads, click

Download Backup under the **/login > Management > Software Management** tab.The resulting .nsb backup file includes the data listed below even if **Include logged history** is not checked at the time of the download:

- **Local User Accounts**
- **Security Provider Configuration**
- **Group Policy Configuration**
- **Jumpoint Configuration**
- **Jump Client Configuration**
- **Team Configuration**
- **Language Configuration**
- **Security Configuration**
- **Inter-appliance Communication Pre-shared Key**
- **Failover Configuration**
- **Outbound Event Configuration**
- **Kerberos Keytab**

Backups taken from a BeyondTrust Remote Support site (as opposed to BeyondTrust Privileged Remote Access) also include the following:

- **Canned Messages Configuration**
- **Client Branding & Messaging**
- **Exit Survey Configuration**
- **Public Site Configuration**
- **File Store** (first 50 files up to 200KB in size)
- **Created/Scheduled Presentations**

If **Include logged history** is checked, the .nsb backup file includes the following data:

- **Logged Session Data**
- **Logged Presentation Information** (BeyondTrust Remote Support only)
- **Logged License Usage** (BeyondTrust Remote Support only)
- **Logged Support Team Information**

In either case, the .nsb backup file does not include the following:

- **Session Recordings**
- **Command Shell Recordings**
- **Presentation Recordings**
- **File Store files larger than 200KB**
- **File Store files beyond the first 50**
- **Settings, users, or data from /appliance**

In addition to manual downloads at each upgrade, BeyondTrust also recommends downloading .nsb backups on a regular basis, using the automated schedule via the integration client. The integration client can dowload the following types of data:

- **Session Data**
- **Session Recordings**

- **Command Shell Recordings**
- **Site Backups**
- **Show My Screen Recordings**

Please see the Integration Client Guide at www.beyondtrust.com/docs/remote-support/how-to/integrations/ic/.htm for setup and configuration instructions. The client installation package is available from **Downloads** in the BeyondTrust Self-Service Center. It is released only as a 32-bit Windows client; however, this runs on 64-bit Windows systems. It is available in a number of different versions, so check the BeyondTrust product release version on the **/login > Status > Information** tab to make sure to download the right integration client version.

In addition to the **Download Backup** button and the integration client, the BeyondTrust API provides a variety of commands to download backup data. This is useful for automating backups using custom tools and/or scripts. The .nsb backups can be downloaded using the BeyondTrust Backup API. Session reports, session recordings, Show My Screen recordings, command shell recordings, presentation recordings, and exit surveys can be downloaded using the Reporting API.

Appliance Recovery

BeyondTrust Appliances are available in virtual, hardware, and Cloud versions in addition to hosted sites, which run on shared appliances in BeyondTrust's data centers. When any of these go offline unexpectedly, the process necessary to repair and/or replace the failed site or appliance varies depending on the appliance or site in question. The various repair/replacement scenarios are described below so an effective strategy can be developed to prepare for them in advance.

Failover and Spare Appliances

BeyondTrust recommends using a preconfigured failover relationship between a "primary" and a "backup" BeyondTrust Appliance. This ensures that the BeyondTrust software is available in the event either BeyondTrust Appliance should fail. BeyondTrust customer clients and representative consoles are built to attempt connection with the primary BeyondTrust Appliance at a specific address. In the event of a primary appliance failure, this address is used to redirect clients from the failed appliance to the backup appliance. This can done using one of three network routing methods: shared IP, DNS swing, or NAT swing. For more information, please see Configuring Failover at www.beyondtrust.com/docs/privileged-remote-access/how-to/failover/failover-setup.htm.

Though client traffic is redirected to the backup appliance, this appliance does not accept connections until it takes the primary role. Once a backup appliance takes the primary role, it begins accepting client connections and provides all the same services the failed appliance did. This role change can be triggered manually or automatically.

Given the above information, here are the basic steps to take in the event of a primary appliance failure in a failover pair:

1. Redirect network traffic from the primary to the backup appliance. If the appliances are configured with:
    a. **Shared IP**: The backup appliance automatically takes over the IP address of the failed appliance.
    b. **DNS swing**: Update the DNS A-record of the primary appliance to resolve the IP address of the backup appliance.
    c. **NAT swing**: Update the firewall NAT rule(s) to resolve the client-facing / public IP of the failed appliance to the private IP of the backup appliance.
2. Make the backup appliance take over the primary role. If **Enable Automatic Failover** is:
    a. **Enabled**: If the backup appliance can reach the **Network Connectivity Test IPs** and cannot reach the primary appliance during the **Primary Site Instance Timeout** period, the backup appliance automatically takes the primary role.
    b. **Disabled**: Use the **Become Primary** button or the **API command:** set_failover_role. To use the button, log into the backup appliance's /login administrative web interface. Browse to **Management > Failover**. Click **Become Primary**, leaving the adjacent box not checked.
3. Confirm the clients are working, and proceed to perform maintenance on the failed appliance.

In the event that there is a cold spare instead of a failover appliance, begin the recovery process by restoring settings and data from the backup(s) to the spare appliance. Once the data is restored, redirect the client traffic to the spare appliance using DNS or NAT swing. If the spare appliance is on the same local network as the failed appliance, attempt to assign the IP of the failed appliance to the spare appliance. However, if the spare appliance is on the same switch as the failed appliance, this switch must be rebooted for the change to take effect.

Virtual Appliances

BeyondTrust's virtual appliances are certified for VMware vCenter 5.0+ and Hyper-V 2012 R2. These appliances support virtual machine **snapshots** (VMware) and **checkpoints** (Hyper-V). A checkpoint or snapshot represents the state of a virtual machine at the time it was taken and includes the following:

- Files and memory state of the virtual machine's guest operating system
- Settings and configuration of the virtual machine and its virtual hardware.

> ***Note:*** *If the BeyondTrust Virtual Appliance experiences a failure and there is a recent snapshot or checkpoint, try restoring it first. This is often the fastest way to restore functionality.*

If the BeyondTrust Virtual Appliance is under an active support maintenance contract, BeyondTrust Support sends an up-to-date VMware or Hyper-V deployment file for the appliance upon request the event of a failure and/or loss of the virtual appliance. To receive a copy, contact BeyondTrust Support with company information from an authorized email address. This address would normally be the same used to communicate with BeyondTrust during the initial deployment of the appliance and/or subsequent administrative-level incident management. A local copy of the virtual appliance file should be saved in case the appliance needs to be restored outside of BeyondTrust Support's normal business hours.

To re-install the virtual appliance, follow the procedures outlined in the BeyondTrust Virtual Appliance Installation Guide at www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/virtual/index.htm. Access to the VMware or Hyper-V administrative management tool is needed to complete this process.

1. Log into the Hyper-V Manager or VMware infrastructure client.
2. Deploy the **BeyondTrust OVA** (VMware) or **EXE** (Hyper-V) file.
3. Use the Hyper-V Manager or VMware client to power on the virtual appliance.
4. Open the virtual console.
5. Enter the IP address, subnet mask, and default gateway of the appliance.

The network settings of the appliance should already be saved from previous configuration. Otherwise, contact the company network administrator for the appropriate settings. Once the appliance is accessible on the network, log into the /appliance administrative web interface, update the appliance, and restore settings, as needed.

Hardware Appliances

In the event of hardware failure, the first task is to restore the BeyondTrust service on the network. If there is a backup or spare hardware appliance, bring it online. If this is not an option, it may be possible to repair the failed appliance remotely with assistance from BeyondTrust Support. In the event that this is not possible, BeyondTrust Support can provide access to a temporary BeyondTrust site hosted on BeyondTrust's servers while new hardware is being shipped. Shipment of new hardware is covered under the maintenance contract with BeyondTrust, and BeyondTrust Support remains actively involved throughout the the process of shipment, installation, and return of the failed hardware. BeyondTrust makes all reasonable attempts to help retain data but cannot guarantee that any or all data will remain intact through this process.

Temporary Hosted Site

As mentioned above, BeyondTrust can provide access to temporary hosted sites on shared appliances in BeyondTrust's data centers. However, hosted sites have limitations. In most cases, client software from the original site (e.g., Jump Clients, Jumpoints, and rep consoles) do not transfer to the hosted site, and new clients deployed from the hosted site are not normally transferred back to the original site, once it is back online.

Because hosted sites exist outside of the network, endpoints planning to be supported from a hosted site must be able to access these data centers over the public internet. If there is an up-to-date backup, user data can be uploaded and configured in the hosted site. If these users and/or configurations rely on resources internal to the network (e.g., Active Directory, RADIUS, and/or Kerberos servers), these resources are usually inaccessible from the hosted site. Traffic to and from the hosted site is encrypted with BeyondTrust's SSL certificates and connects with a domain name in BeyondTrust's namespace (e.g., "tempsite.beyondtrust.com"). The original company certificate(s) and hostname(s) are not used.

If a temporary hosted site would be helpful, follow these steps to obtain a hosted site and to upload the settings of a backup:

1. Contact BeyondTrust Technical Support at help.bomgar.com.
2. Wait for credentials.
3. Log into the new site.
4. Go to **Management > Software Management**.
5. Use **Restore Settings** to browse for the software backup.
6. Enter the backup password created, if applicable.
7. Click **Upload Backup**.

Return Materials Authorization (RMA)

As outlined in the BeyondTrust Maintenance Service Agreement, BeyondTrust Support provides support for BeyondTrust hardware. Every reasonable attempt is made to restore BeyondTrust Appliances to full operation while still at the location. This typically involves a technician going to wherever the appliance is located and connecting a PS/2 keyboard and VGA monitor to the back of the appliance. To do this, a torx 8 or 10 screwdriver is required to remove the backplate. It is best practice to have all this hardware on-site prior to a failure event. If the appliance is racked in a data center with a KVM switch, this can be used instead. It is also best practice to allow the appliance outbound access to the internet over TCP 443. This allows BeyondTrust Support to establish a secure connection with the appliance for low-level troubleshooting and recovery. If BeyondTrust Support determines that at-location repair is not possible, the RMA process is initiated.

Hardware RMAs may include one or more completely new appliances and/or Field Replaceable Units (FRU). An FRU can be issued only for B300 and B400 appliances. Replaceable items include hard disk drives and power supplies. Any other hardware problems result in a full RMA of the entire appliance. To process an RMA, BeyondTrust Support needs the following information:

- Contact name, email, and phone
- Shipping address
- Appliance serial number
- Value Added Tax (VAT) number, if necessary

When shipping BeyondTrust hardware internationally, BeyondTrust Support must begin by confirming whether the appliance is to be returned to BeyondTrust temporarily and shipped back after repair or returned to BeyondTrust permanently and replaced with new hardware.The former option can take up to four weeks. Because the latter option may incur VAT fees for international shipments, it is important to send documented consent to BeyondTrust Support for the payment of any fees incurred by this process. Replacements for appliances located in Ireland or the European Union are usually shipped from BeyondTrust's inventory in Ireland. No VAT fees are expected for these shipments.

Once the RMA request has been opened, a printable packing slip for the old appliance is emailed along with tracking and setup instructions for the new or repaired hardware. For RMAs in the United States, a return shipping label is sent. For appliances outside the United States, either BeyondTrust's DHL account number is given to schedule a DHL pickup, or BeyondTrust Support arranges for the Waste Electrical and Electronic Equipment (WEEE) scrapping of the appliance. In any of these cases, BeyondTrust Support follows up to ensure the replacement hardware is installed and functional before closing the RMA incident.

If replacement hardware was sent prior to the receipt of the failed hardware, BeyondTrust Support must verify that the old appliance is returned. If a replacement appliance is received, it is a requirement that the defective appliance be returned to BeyondTrust within two weeks of the new appliance becoming operational. Outstanding appliances are invoiced at list price. The packing materials of a new appliance, the above-mentioned DHL number, and the return shipping label can be used to return the old appliance.

Hardware Installation

Once the replacement appliance has been received and powered on, the settings can be restored using either the local console or appliance administrative web interfaces. It is usually more convenient to use the web interfaces. The /appliance administrative web interfaces of a hardware appliance can be accessed locally using either of its NIC ports. These are provisioned with non-routable IP address(es) on the 169.254.1.0/16 network. To gain access, follow these steps:

1. Rack the appliance.
2. Plug the power cable into a safe power source.
3. Use a patch cable to connect a computer to NIC1 or NIC2 on the rear of the BeyondTrust Appliance.
4. Press and release the **Power** button on the front of the appliance.
5. Edit the IP configuration of the connected computer:
    a. **IP address**: 169.254.1.5
    b. **Subnet mask**: 255.255.0.0
    c. **Default gateway**: none
    d. **DNS server**: none
6. Wait for the appliance to finish booting.
7. Launch a web browser.
8. Enter the address **https://169.254.1.1/appliance/login.ns** in the URL address field.

The /appliance login page should load. If not, try alternately substituting ".2", ".3" and ".4" for the last decimal in the address above. Load each of these addresses separately until one responds. If none of these responds, try all four addresses using the other NIC of the appliance.

Once the /appliance login page has loaded, log in and enter the IP network settings of the appliance. Replacement appliances typically ship with default login credentials. For IP settings, reference a saved copy of the IP settings from the previous appliance. To restore IP configuration, follow these steps:

1. Log in with the default credentials, **admin** and **password**.
2. Enter a new password.
3. Save this password in a secure location. It is difficult to recover if lost.
4. Browse to **Networking > IP Configuration**.
5. Click **Add New IP**.
6. Fill out the resulting page with settings appropriate for the network.
7. Save the new IP address.
8. Add the default gateway in the **Global Configuration** section.

These are the basic settings required to bring an appliance online in most situations; however, the network may have additional DNS, NTP, syslog, SMTP, and/or other servers and settings. Ideally, these have been saved in backup files. Like IP configuration, these other settings cannot be restored automatically. Instead, they must be manually entered. Once all the /appliance settings and/or IP configuration settings are restored, proceed to restore the certificates and /login administrative interface.

BeyondTrust Software-as-a-Service (SaaS)

BeyondTrust's SaaS products include Starter Service Licenses and BeyondTrust Cloud Appliances. Both of these are hosted by BeyondTrust, but Starter Service Licenses do not provide all of the isolation or functionality provided by Cloud Appliances. BeyondTrust's Starter Service is limited to five total licenses by default, and their functionality is more limited in some ways than regular licenses. In contrast, each BeyondTrust Cloud instance is a single-tenant virtual appliance and has none of the Starter Service licensing limitations.

In the event that the Production Starter Service or Cloud Appliance site goes down and becomes inoperable unexpectedly, follow these steps:

1. Log into the /login administrative web interface and attempt a restart.
2. If a Cloud Appliance is owned, log into the /appliance administrative web interface. Check the settings to ensure there are no errors, warnings, or anomalies.

3. If all this fails, try to find a bypass or workaround solution (such as an alternative site or remote access product).
4. Contact BeyondTrust Support with a description of the situation and the steps taken thus far. In cases where the production site is offline and there is no workaround or alternative solution, BeyondTrust Support's maximum target time for First Response (start of resolution) is 30 minutes within normal business hours.

Data Recovery

Once an appliance or site has been repaired and/or replaced, it is usually necessary to restore its settings and data. This is always necessary in cases where BeyondTrust has shipped an entirely new appliance from the factory. The settings and data to restore includes /appliance settings and certificates as well as /login users and configuration. Before restoring any of this, first complete the appliance IP network configuration. Once that is done, remaining /appliance configuration, certificates, and /login settings can be restored remotely as described below.

Failover

When an appliance in a failover pair has failed and been replaced, the second appliance in the pair should be servicing clients while the failed appliance is restored. The restore process for the failed appliance varies depending on its type. Once the appliance has been restored, restore its certificates either from a backup or by exporting them from the primary appliance.

Once the failed appliance is online and has the primary appliance's certificates installed, restore its /login administrative interface. Since the primary appliance should already have all settings and data, it us generally not advisable to restore backup files to a backup appliance manually. However, installing a /login site package is needed. Once that is done, establish failover from the active appliance to the repaired one and sync them as described in Establish the Primary/Backup Failover Relationship Between Two Appliances at www.beyondtrust.com/docs/remote-support/how-to/failover/backup.htm .

It is still possible to download and restore backup files to failover appliances; however, it is not ideal unless the primary failover appliance is missing crucial data that exists only in a backup file. If a backup is restored, failover settings are overwritten with the values contained in the backup. This includes both **/login > Management > Failover** settings and the **Inter-appliance Communication Pre-shared Key** found in **/login > Management > Security**. This means that if a backup is restored to an appliance in active failover, the failover connection is likely to have issues. Because of this, the best practice is to break failover, restore the backup, reset the pre-shared key, and re-establish the failover relationship. For details, please see Failover Dynamics and Options at www.beyondtrust.com/docs/privileged-remote-access/how-to/failover/failover-dynamics.htm.

If the restored appliance in a failover pair has formerly been the primary appliance in the failover relationship, it re-enters the failover relationship as the backup appliance. Sometimes, it can remain this way, but in other scenarios, it is desirable to make it primary once again. If this is the case, follow the instructions in Establish Failover for Planned Maintenance at www.beyondtrust.com/docs/remote-support/how-to/failover/planned-maintenance.htm. The process varies slightly, depending on how the network is routing traffic to the primary appliance. The routing methods are IP failover, DNS swing, or NAT swing.

Atlas

Like failover, Atlas clusters have special requirements. An Atlas cluster typically consists of a failover pair of master appliances that route traffic between a number of traffic node appliances. If one of the master appliances fail, refer to the failover recovery guidelines described immediately above. If one fails, follow these steps:

1. Restore the appliance.
2. Install a /login site package on the appliance.
3. Add the recovered appliance back into the Atlas cluster. Please see Configure the Traffic Nodes in an Atlas Cluster at www.beyondtrust.com/docs/remote-support/how-to/atlas/atlas-slave.htm for more information.
4. Sync the recovered appliance in order to restore the /login settings.
    a. Log into the primary master appliance's /login administrative web interface.
    b. Browse to **Management > Cluster**.
    c. Click **Sync Now**.

Once completed, the traffic node is fully operational. To test, follow these steps:

1. Log into the traffic node's /login web interface.
2. While logged into a rep console from a geographic region that is expected to route through the restored traffic node, check **Status > Connected Clients**.
3. If the value for connected rep consoles increases by one immediately after authenticating to the console, the traffic node is working.

If a backup is restored from an Atlas master node, it does not overwrite the existing Atlas configuration. As a result, copying the configuration of a master node to each of its traffic nodes is supported; however, manually performing this task is not standard practice. Synchronizing data from the primary master appliance is the standard method for restoring /login settings to a traffic node.

Recover Certificates

BeyondTrust requires SSL certificates. If any client software from a previous appliance is expected to reconnect with the replacement appliance, this appliance needs a copy of the original SSL certificate(s). Most Cloud Appliances share a standard certificate which validates the BeyondTrust Cloud domain. If the certificate and domain are changed, the non-standard certificate must be restored. Hardware and virtual appliances have no such standard configuration and therefore have unique certificates configured by the administrator that must be restored in a disaster recovery scenario. The steps to restore certificates are given below, and they assume that the necessary steps have been taken to bring the web interfaces online.

> ***Note:*** *The steps to bring the web interfaces online vary based on the appliance type.*

1. Log into the /appliance web interface of the BeyondTrust Appliance.
2. Go to **Security > Certificates**.

   > ***Note3****If a* ***BeyondTrust Appliance*** *certificate is listed, ignore it. This is a standard certificate that ships with all BeyondTrust Appliances.*

4. In **Security :: Certificate Installation**, click **Import**.
5. Browse to the certificate file.
6. Enter the password for the certificate file.
7. Click **Upload**.

The BeyondTrust Appliance certificate appears in the **Security :: Certificates** section.If the certificate was issued by a third-party Certificate Authority (CA), the intermediate certificate and root certificate are also listed here. If your appliance uses a CA certificate, all intermediate certificate and their root certificate must be present for the appliance to function properly. Here is a description of each type of certificate:

- **Self-Signed Certificate:** This has identical values for **Issued To** and **Issued By** and have the appliance's fully qualified domain name (FQDN) in the **Alternative Name(s)** field.
- **CA-Signed Certificate:** This has an **Issued To** field and/or an **Alternative Name(s)** field matching the BeyondTrust Appliance's FQDN. If a CA-signed certificate exists, the appliance also has one or more intermediate and/or root certificate(s) listed on the **Certificates** page.
- **Intermediate certificates:** These have different **Issued To** and **Issued By** fields, neither of which is an FQDN. Usually, there are only one or two intermediate certificates. Sometimes, there are none, depending on the CA.
- **Root certificate:** This has identical values for the **Issued To** and **Issued By** fields, neither of which are an FQDN. Every CA-signed certificate must have exactly one root certificate.

If a self-signed certificate is being used, a warning is present beaneath it. The warning is expressing that this kind of certificate should normally be used only temporarily until a CA-signed certificate is obtained. If a CA-signed certificate has already been obtained and

one or more of its intermediate and/or root certificate(s) are missing, a warning appears beneath the CA-signed certificate. To resolve this, contact the CA. For more information, please see FAQ 755 in the BeyondTrust Technical Support Self Service Center at ssc.bomgar.com/SSC/SolutionFAQ.aspx?id=755.

1. Once there are not any certificate warnings, click the **Assign IP** link in the certificates entry for the appliance's CA-signed or self-signed certificate.
2. At the bottom of the resulting page, check the IP address of the appliance.
3. Click **Save Configuration**. This completes the restore process for the certificate(s). However, the appliance still needs /login restored before it is fully operational.

Recover /login

Unlike /appliance, the /login administrative web interface is not installed by default on new appliances. Therefore, in cases where a new virtual appliance has been installed or a new hardware appliance has been shipped, the new appliance does not usually have a /login administrative web interface. If the appliance was repaired or restored from a snapshot instead of replaced or re-installed, the repaired appliance still has a /login site package installed, but it may be necessary to upgrade the site to the same version as the failover appliance or to a version compatible with the backup file. In these cases, contact BeyondTrust Support for the necessary /login site updates. To get the updates, send BeyondTrust Support an email including these items:

- **Screenshot of the /appliance Status page**
- **Appliance FQDN registered in DNS**
- **Version of the most recent backup file**

After receiving this information, Support registers the appliance on the BeyondTrust update servers, builds the necessary update package(s), and sends the installation instructions. There are one or more base software updates to install prior to the /login site package. Follow the instructions from BeyondTrust Support to update the appliance and log into the /login web interface, using the default admin and password credentials. The system forces the password to be changed at login.

In failover and Atlas scenarios, /login data is recovered using data synchronization rather than backup files. Outside of this, the .nsb backup files should be saved in order to restore /login settings, users, and data. However, before restoring a backup file, take into account the BeyondTrust product release version from which the backup was downloaded as well as the version of the site receiving the backup file. BeyondTrust does not test restoring backups from every version to every other version. Only backups from the supported upgrades of a particular version are tested. Supported upgrade versions are listed in the release notes for each version. Release notes are available at www.beyondtrust.com/support/changelog.

The version of a particular backup can be found by checking the filename of the backup. By default, BeyondTrust backup file names begin with **BeyondTrust** followed by the BeyondTrust product release version of the backup, the name of the site which generated the backup, the date on which the backup was downloaded, and the unique ID of the backup file. Check the version of the site to which the backup is being uploaded to by viewing the **Product Version** field on the **/login > Status > Information** page.

When attempting to restore backups from an old release version to a newer version of BeyondTrust not listed as the backup's supported upgrade version, unexpected issues and/or data loss can occur. When attempting to restore backups from newer versions of BeyondTrust to older, major issues occur. This is simply not supported. However, as long as the rules concerning release versions are followed, backups can be successfully restored between physical appliances (i.e., B200, B300, and B400) and virtual appliances and between physical appliances of different hardware revisions.

Once the restore method is validated, restore the /login site backup by following these steps:

1. Browse to **/login > Management > Software**.
2. Locate **Software :: Restore Settings**.
3. Click **Choose File**.
4. Select the backup file using the file browser.

5. Enter the backup password, if one was assigned.
6. Click **Upload Backup**.

The backup password is assigned by the administrator who downloads the backup originally. If it is lost, the backup cannot be restored. Once it is restored, all users (including the local administrator), settings, and most data are restored to the state at which the backup was originally downloaded.

After /login is online and the backup is restored, the appliance should be fully operational, assuming the network's traffic has been properly routed. To test the appliance:

1. Open the rep console.
2. Log in with the user credentials that worked prior to the failure event.
3. Verify that all Jump Clients, Jumpoints, options, and settings function as expected.

There should be no need to deploy new client software. Instead, the original clients should reconnect with the new appliance automatically.

Return the Defective Appliance

In cases where you have replaced a failed hardware appliance, it will be necessary to dispose of the failed hardware. First, you may wish to wipe the appliance of all sensitive data. You can wipe the appliance by taking these steps:

1. Log into the **/appliance** web interface of the defective appliance.
2. Browse to the **Status > Basics** page.
3. Click **Reset Appliance to Factory Defaults**.
4. Wait for the reset to complete.
5. Click **Shut Down This Appliance**.

Once done, ask BeyondTrust Support for a return shipping label, if you have not been sent one already. Once you have the return label, use it to ship the appliance back. Many administrators choose to use the packaging materials of the replacement appliance to return the defective one.