BeyondTrust

# Remote Support
# Appliance Upgrade Guide



TC:2/8/2019

# Table of Contents

# Upgrade the BeyondTrust Software

Please visit the Product Change Log to get the details of each release of BeyondTrust remote support software.

> ***Note:*** *If your BeyondTrust software has not been updated in some time and is several revisions behind the latest version, you will probably need to install several intermediate versions before installing the latest software. See the third bullet below for details.*

## Upgrade Preparation

- Prior to upgrading, always create a backup of your settings and configuration from **/login > Management > Software Management**. As a best practice, also export a copy of your SSL certificates and private key, and save them locally to ensure continuity in case of a failure on the upgrade.
- For major software releases, customers with current maintenance contracts are placed into a rollout schedule. Once your upgrade is ready, BeyondTrust alerts you via email to begin this upgrade procedure.
- If your appliance is many months or years out of date, it is unlikely to be able to upgrade directly to the latest version of BeyondTrust in a single installation. In this case, some upgrade packages may be grayed out in the updates list and require another package to be installed first. Select **Install This Update** on the available package to enable the dependent one.
    - If uncertain which updates to install or in which order, contact BeyondTrust Technical Support at help.bomgar.com with a screenshot of your **/appliance > Status > Basics** page to determine the specific updates needed for your appliance.
    - In cases where intermediate BeyondTrust updates must be installed before the latest version, BeyondTrust software clients are not expected to auto-update successfully unless they are allowed time to retrieve the intermediate updates. Therefore, BeyondTrust recommends that you wait at least 24 hours after installing each package prefixed by "BeyondTrust".
    - Base updates do not require a waiting period, but they are typically prerequisite to "BeyondTrust" packages. As such, Base updates are normally installed immediately prior to "BeyondTrust" packages.
    - If it is impossible to allow 24 hours for automatic client upgrades to complete, the alternative to automated updating is first to remove all existing client software, including representative consoles, Jump Clients, Jumpoints, Bomgar Buttons, connection agents, etc. Install each "BeyondTrust" and Base upgrade in sequence until the latest version is reached. Then, manually reinstall all client software.
- Installation usually takes between 15 minutes to an hour. However, if you are storing a large amount of data on your appliance (e.g., session recordings), the installation could take significantly longer.
- BeyondTrust recommends performing upgrades during scheduled maintenance windows. Your BeyondTrust site will be temporarily unavailable during the upgrade. All logged in users and active sessions will be terminated.
- BeyondTrust also recommends testing the update in a controlled environment prior to deploying into production. Testing can best be performed when you have two appliances in a failover relationship and when you update asynchronously. (See "Verify and Test" on page 15).
- If you experience any issues during the Base update, do not restart the BeyondTrust Appliance. Please contact BeyondTrust Technical Support.
- If you have two appliances set up in a failover configuration, consider whether you want to update synchronously or asynchronously.
    - With synchronous updating, the primary appliance is updated first and maintains its role as primary. This method does involve some downtime; it is recommended for simple deployments and scenarios that will not suffer from being offline during the update.

- With asynchronous updating, the backup appliance is updated first and then assumes the role of primary. This method has minimal downtime; it is recommended for larger deployments and scenarios that rely on maintaining solid uptime. Some complexity is involved, as the network may have to be modified in order to fail over to the backup appliance.

## Client Upgrades

Only certain upgrades require client software to update. Base software updates and license add-ons do not require client software updates. Site version updates do require client updates, however. Most client updates occur automatically, but the expected update procedure for each type of client is reviewed below.

**IMPORTANT!**

*When upgrading to a newly built site software package, verify that all certificate stores are managed appropriately and are up-to-date prior to upgrading to a new BeyondTrust version. Failure to do so may cause a majority of your existing Jump Clients to appear offline.*

- Your installed representative consoles will need to be upgraded after the site upgrades. Typically, this occurs automatically the next time the representative run the representative console.
  - Representative consoles previously deployed on locked-down computers using MSI may need to be re-deployed once the upgrade is complete.
  - If the extractable representative console or extractable Jump Client feature has been enabled for your site by BeyondTrust Technical Support, then you can download an MSI installer to update representative consoles and/or Jump Clients prior to upgrading the appliance. To do this, check for the new update either manually or automatically. Click the **Rep Console Installers** or **Jump Client Installers** link to download the MSI for distribution. Note that the updated clients will not come online until their appliance is updated. It is not necessary to uninstall the original client prior to deploying the new one, as the new one should automatically replace the original installation. It is a best practice, however, to keep a copy of the old MSI to remove the outdated installations after the appliance is updated should this removal prove necessary. The new MSI is unable to do so.
- After an upgrade, deployed Jump Clients automatically update.
  - If large numbers of Jump Clients attempt to update simultaneously, they may flood the appliance, severely crippling performance both on the appliance and the network, depending on the available bandwidth and hardware. To regulate the amount of bandwidth and resources consumed by Jump Client updates, go to **/login > Jump > Jump Clients** and set a lower value for **Maximum Number of Concurrent Jump Client Upgrades** and/or **Maximum bandwidth of concurrent Jump Client upgrades**.
  - Active and passive Jump Clients queue for update upon their first check-in with the appliance subsequent to the appliance's update. These check-in events occur at regular intervals outbound from the Jump Client host over TCP port 443 to the appliance. Active Jump Clients check in immediately after an upgrade is complete on the appliance. Passive Jump Clients check in upon boot up, upon having a connection made from the representative console, upon being told to check in from the system tray icon, and at least once every 24 hours.
  - If a Jump Client has not yet been updated, it is labeled as **Upgrade Pending**, and its version and revision number appear in the details pane. While you can modify an outdated Jump Client, you cannot Jump to it. Attempting a Jump does, however, move that Jump Client to the front of the upgrade queue.
- If your BeyondTrust Appliance is out of date, multiple release versions may need to be installed to reach the current version. In this case, BeyondTrust recommends allowing at least 24 hours between updates to allow Jump Clients to upgrade. Passive Jump Clients may take longer than this depending on how long their host systems remain offline.

***Note:*** *When upgrading to a new software version, please allow some time for all Jump Clients to come back online before moving forward with any other upgrading processes.*

- Once a Jump Client appears as online in the representative console or the **/login > Status > Information** page, it has updated successfully. An effective means of confirming that all Jump Clients have updated is to log into the representative console as an administrative user with permission to modify all Jump Clients in the system. Export the list of Jump Clients. In the resulting report, sort the Jump Clients by **Status Details** and confirm that all the dates listed are more recent than the date of the last BeyondTrust Appliance upgrade.
- If too many release versions are installed back-to-back without first allowing Jump Clients to upgrade, Jump Clients may require manual redeployment.
- After an upgrade, Bomgar Buttons update automatically upon being used for the first time subsequent to an upgrade.
- After an upgrade, deployed Jumpoints should automatically update.
- BeyondTrust Connection Agents update automatically after the site upgrades.
- BeyondTrust Integration Clients do not automatically update after the site upgrades. Integration Clients must be re-installed manually. Integration Client installers are available from the **Downloads** page of help.bomgar.com.
- Upon upgrading, it is necessary to regenerate any installer packages previously created for Bomgar Buttons, Jump Clients, and representative consoles. The clients themselves update as described above. However, the installer files for them invalidate once the appliance which generated them is upgraded.

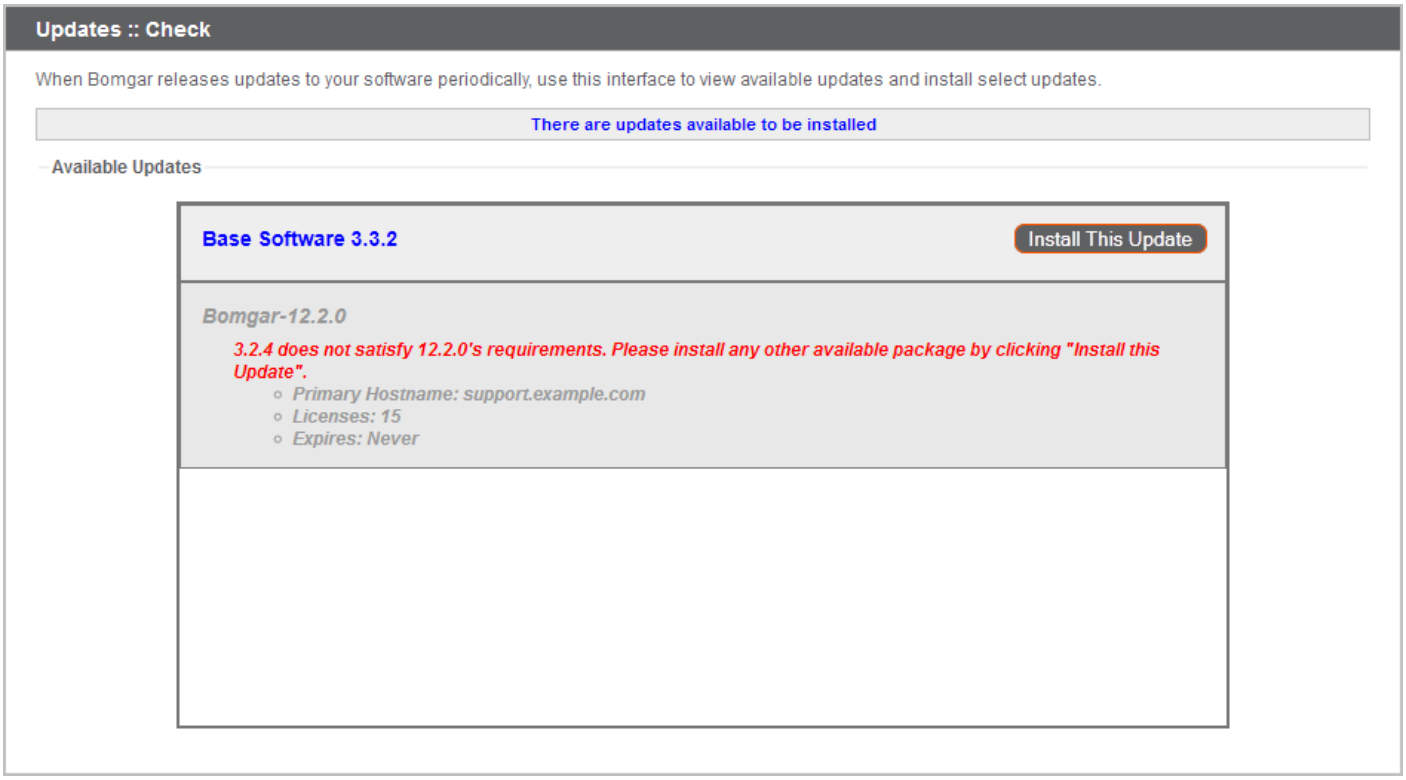
# Upgrade a Single BeyondTrust Appliance Using Automatic Updates

In most cases, BeyondTrust customers can download and install updates with no assistance from BeyondTrust Technical Support. To see if an upgrade is available, log in to your BeyondTrust Appliance (/appliance). On the **Updates** page, click on **Check for updates**.


If a software update is available, it will appear under **Available Updates**. Once you click **Install This Update**, the appliance will download and automatically install the new version of the BeyondTrust software.

**IMPORTANT!**

*When upgrading to a newly built site software package, verify that all certificate stores are managed appropriately and are up-to-date prior to upgrading to a new BeyondTrust version. Failure to do so may cause a majority of your existing Jump Clients to appear offline.*




***Note:*** *Some packages require another package to be installed first. Install the available package to enable the dependent one.*

If automatic updates fail when expected to work, please review the Check for Updates troubleshooting FAQ at www.ssc.bomgar.com/SolutionFAQ.aspx?id=377. If you are still unable to perform automatic updates, please see "Upgrade a Single BeyondTrust Appliance Using Manual Updates" on page 8.

# Upgrade a Single BeyondTrust Appliance Using Manual Updates

If you are unable to use automatic updates (e.g., if your appliance exists on a restricted network), you may perform manual updates.

Log into your BeyondTrust Appliance and go to the **Updates** page. Starting with Base 3.3.2, click the **Appliance Download Key** link to generate a unique appliance key; prior to Base 3.3.2, you must contact BeyondTrust Technical Support to request this key. From a non-restricted system, submit this key to BeyondTrust's update server at https://update.bomgar.com. Download any available updates to a removable storage device and then transfer those updates to a system from which you can manage your appliance.

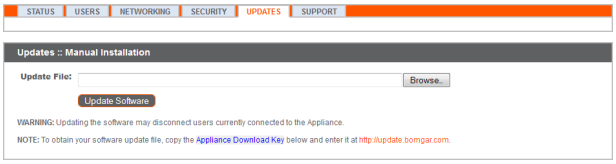
From the **Updates** page, browse to the file from the **Manual Installation** section and then click the **Update Software** button to complete the installation. The appliance will install the new version of the BeyondTrust software.

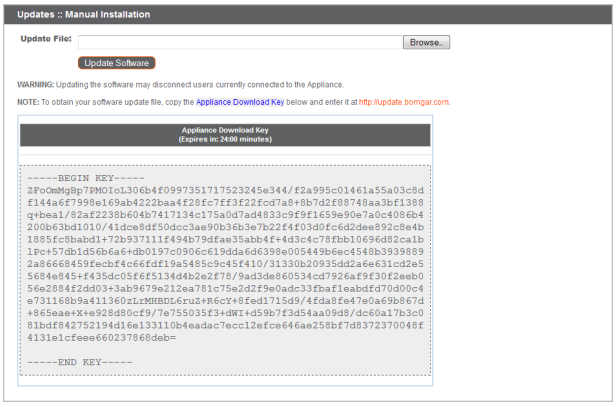
**IMPORTANT!**

*When upgrading to a newly built site software package, verify that all certificate stores are managed appropriately and are up-to-date prior to upgrading to a new BeyondTrust version. Failure to do so may cause a majority of your existing Jump Clients to appear offline.*

***Note:** Be prepared to install software updates directly after download. Once an update has been downloaded, it no longer appears in your list of available updates. Should you need to re-download an update, contact BeyondTrust Technical Support.*

***Note:** If you receive an error, please make sure the time listed on the **/appliance > Status > Basics** page is correct. Many functions of the BeyondTrust Appliance, including the Appliance Download Key, rely on this time being correct. If the time is not correct, please check the NTP setting on the **Networking > IP Configuration** page.*



# Upgrade Two BeyondTrust Appliances in a Failover Configuration

**IMPORTANT!**

*BeyondTrust recommends scheduling maintenance windows during low traffic hours.*

There are two alternatives for upgrading in a failover environment: synchronous upgrade and asynchronous upgrade.

**Synchronous Upgrade of Two Appliances in a Failover Relationship**

With synchronous updating, the primary appliance is updated first and maintains its role as primary. This method does involve some downtime; it is recommended for simple deployments and scenarios that will not suffer from being offline during the update.

**Benefit:** No failover event.
**Drawback:** Longer production site downtime.

**Asynchronous Upgrade of Two Appliances in a Failover Relationship**

With asynchronous updating, the backup appliance is updated first and then assumes the role of primary. This method has minimal downtime; it is recommended for larger deployments and scenarios that rely on maintaining solid uptime. Some complexity is involved, as the network may have to be modified in order to fail over to the backup appliance.

**Benefit:** Minimal production down time.
**Drawback:** Requires failover activity.

## Considerations

1. Select the failover upgrade alternative that best fits your downtime and continuity needs.
2. Schedule two separate maintenance windows in which to complete the upgrade.
3. Expect the upgrade process to take the same amount of time on both appliances.
4. Plan an interim period between the two maintenance windows adequate enough to confirm the new software version in your production environment but brief enough to minimize the exposure of temporarily not having a failover configuration.

# Synchronous Upgrade of Two Appliances in a Failover Relationship

With synchronous updating, the primary appliance is updated first and maintains its role as primary. This method does involve some downtime; it is recommended for simple deployments and scenarios that will not suffer from being offline during the update.

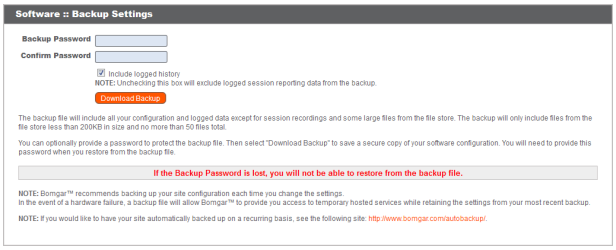
BeyondTrust recommends performing upgrades during scheduled maintenance windows. Your BeyondTrust site will be temporarily unavailable during the upgrade. All logged in users and active sessions will be terminated. You will need to schedule two separate maintenance windows in which to complete the upgrade. Installation usually takes between 15 minutes to an hour. However, if you are storing a large amount of data on your appliance (e.g., session recordings), the installation could take significantly longer. Plan an interim period between the two maintenance windows adequate enough to confirm the new software version in your production environment but brief enough to minimize the exposure of temporarily not having a failover configuration. BeyondTrust also recommends testing the update in a controlled environment prior to deploying into production. If you experience any issues during the Base update, do not restart the BeyondTrust Appliance. Please contact BeyondTrust Technical Support.

In these instructions, **Appliance A** is the primary appliance (i.e., the appliance to which the primary hostname resolves), while **Appliance B** is the backup appliance.

## Backup and Sync

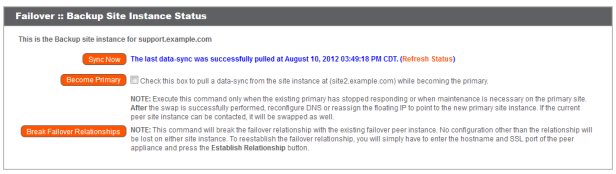
Prior to upgrading, make a backup of your current BeyondTrust software settings. On **Appliance A**, go to **/login > Management > Software Management**.


Click the **Download Backup** button, and save the backup file to a secure location.




Go to **/login > Management > Failover**, click **Sync Now**, and wait for synchronization to complete.

Once synchronization has finished, click **Break Failover Relationships**.




## Update Appliance A

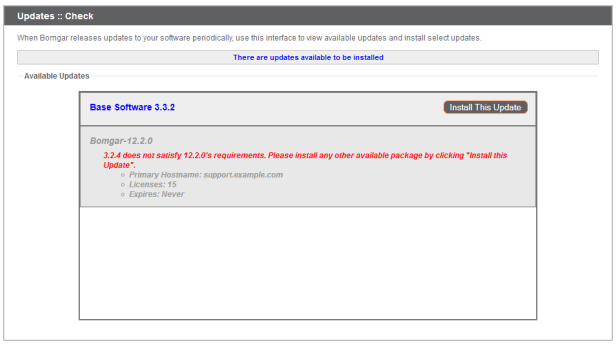
Update **Appliance A** using either the automatic or the manual update method.

**Automatic**

In most cases, BeyondTrust customers can download and install updates with no assistance from BeyondTrust Technical Support. To see if an upgrade is available, go to **/appliance > Updates**.

Click on **Check for updates**.


If a software update is available, it will appear under **Available Updates**. Once you click **Install This Update**, the appliance will download and automatically install the new version of the BeyondTrust software.




> ***Note:*** *"BeyondTrust" software updates often depend on one or more "Base Software" updates. Install the available Base Software updates to enable the dependent BeyondTrust updates. Then download a backup and immediately install the BeyondTrust software updates before doing anything else, such as failing over or installing updates on another appliance.*

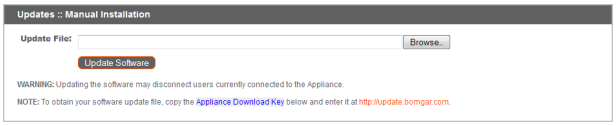
If automatic updates fail when expected to work, please review the Check for Updates troubleshooting FAQ at help.bomgar.com/SSC/Main.aspx?rurl=377.

**Manual**

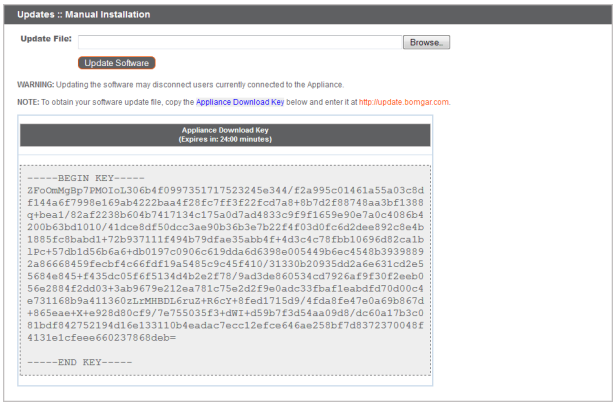
If you are unable to use automatic updates (e.g., if your appliance exists on a restricted network), you may perform manual updates.

Go to **/appliance > Updates**.


Starting with Base 3.3.2, click the **Appliance Download Key** link to generate a unique appliance key; prior to Base 3.3.2, you must contact BeyondTrust Technical Support to request this key. From a non-restricted system, submit this key to BeyondTrust's update server at https://update.bomgar.com. Download any available updates to a removable storage device and then transfer those updates to a system from which you can manage your appliance.




From the **Updates** page, browse to the file from the **Manual Installation** section and then click the **Update Software** button to complete the installation. The appliance will install the new version of the BeyondTrust software.




> ***Note:*** *Be prepared to install software updates directly after download. Once an update has been downloaded, it no longer appears in your list of available updates. Should you need to re-download an update, contact BeyondTrust Technical Support.*

## Verify and Test

After completing the upgrade process, verify that the update completed successfully and that your software is working as expected. Your installed representative consoles will need to be upgraded after the site upgrades. Typically, this occurs automatically the next

time the representative run the representative console.To check the software build that a console is running, log into the console and then click **Help > About**. Also be sure that you can make a connection to a remote computer via a session.

> ***Note:*** *Representative consoles previously deployed on locked-down computers using MSI may need to be re-deployed once the upgrade is complete. If the extractable representative console or extractable Jump Client feature has been enabled for your site by BeyondTrust Technical Support, then you can download an MSI installer to update representative consoles and/or Jump Clients prior to upgrading the appliance. To do this, check for the new update either manually or automatically. Click the* ***Rep Console Installers*** *or* ***Jump Client Installers*** *link to download the MSI for distribution. Note that the updated clients will not come online until their appliance is updated. It is not necessary to uninstall the original client prior to deploying the new one, as the new one should automatically replace the original installation. It is a best practice, however, to keep a copy of the old MSI to remove the outdated installations after the appliance is updated should this removal prove necessary. The new MSI is unable to do so.*

## Update Appliance B

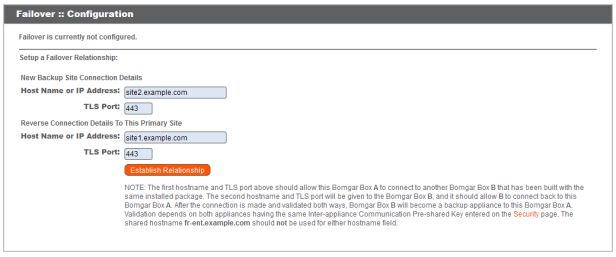
Update **Appliance B** using either the automatic or the manual update method as defined above. Then verify and test that the update completed successfully.

## Reestablish Failover Relationship

From **Appliance A**, go to **/login > Management > Failover**.


> ***Note:*** *To configure a valid connection, both appliances must have identical Inter-Appliance keys. See the* ***/login > Management > Security*** *page to verify the key for each appliance.*

Reestablish the failover relationship with the backup appliance, using **Appliance B** as the backup and keeping **Appliance A** as the primary.




Establishing the relationship between the two appliances occurs on the **Failover** page of the appliance intended to be the primary appliance. The addresses that are entered here will establish the relationship and allow either appliance to connect to each other at any time. The fields on this page called **New Backup Site Connection Details** tell the primary appliance how to connect to the appliance that will become the backup appliance. The fields called **Reverse Connection Details to this Primary Site** will be given to the backup appliance and tell it how to connect back to this primary appliance. You must use a valid hostname or IP address and the TLS port number for these fields. When all of these fields are set, click the **Establish Relationship** button to attempt to establish the relationship.

> ***Note:*** *Whenever possible, BeyondTrust recommends using the unique IP address of each appliance when configuring these settings.*

Once the relationship has been established, extraneous tabs will be removed from the backup site. It takes about 60 seconds for the first data synchronization to initiate, but you may also click the **Sync Now** button to force synchronization and pull the most current information from the primary appliance into the memory of the backup appliance. Synchronization itself may take anywhere from a

few seconds to a few hours, depending on the amount of data that needs to be synchronized. The **Failover** page will list the last date and time of data synchronization when synchronization is completed.

Failover synchronization syncs all user accounts, all /login configuration settings, files in the file store, logs and recordings. All of this information which exists on the backup appliance will be overwritten by that which resides on the primary appliance. If the primary appliance is the master node in an Atlas cluster, the backup appliance will automatically become the new backup master node in this cluster.

# Asynchronous Upgrade of Two Appliances in a Failover Relationship

With asynchronous updating, the backup appliance is updated first and then assumes the role of primary. This method has minimal downtime; it is recommended for larger deployments and scenarios that rely on maintaining solid uptime. Some complexity is involved, as the network may have to be modified in order to fail over to the backup appliance.

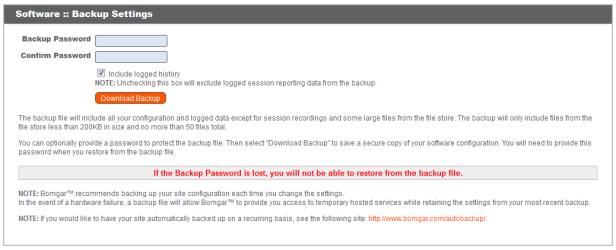
BeyondTrust recommends performing upgrades during scheduled maintenance windows. Your BeyondTrust site will be temporarily unavailable during the upgrade. All logged in users and active sessions will be terminated. You will need to schedule two separate maintenance windows in which to complete the upgrade. Installation usually takes between 15 minutes to an hour. However, if you are storing a large amount of data on your appliance (e.g., session recordings), the installation could take significantly longer. Plan an interim period between the two maintenance windows adequate enough to confirm the new software version in your production environment but brief enough to minimize the exposure of temporarily not having a failover configuration. BeyondTrust also recommends testing the update in a controlled environment prior to deploying into production. If you experience any issues during the Base update, do not restart the BeyondTrust Appliance. Please contact BeyondTrust Technical Support.

In these instructions, **Appliance A** is the primary appliance (i.e., the appliance to which the primary hostname resolves), while **Appliance B** is the backup appliance.

## Backup and Sync

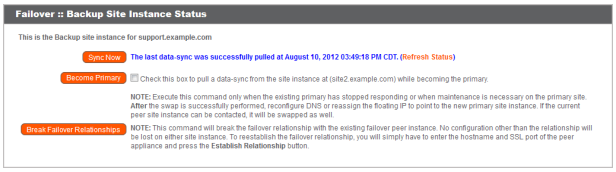
Prior to upgrading, make a backup of your current BeyondTrust software settings. On **Appliance A**, go to **/login > Management > Software Management**.


Click the **Download Backup** button, and save the backup file to a secure location.




Go to **/login > Management > Failover**, click **Sync Now**, and wait for synchronization to complete.

Once synchronization has finished, click **Break Failover Relationships**.




## Update Appliance B

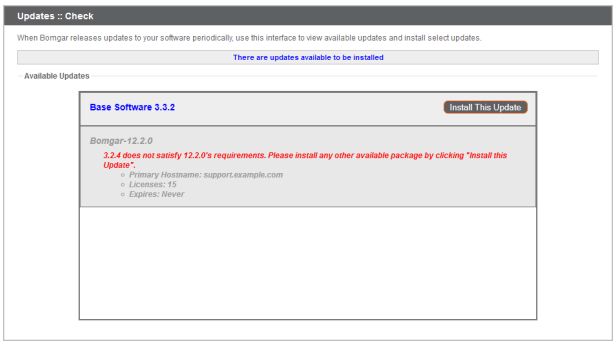
Update **Appliance B** using either the automatic or the manual update method.

**Automatic**

In most cases, BeyondTrust customers can download and install updates with no assistance from BeyondTrust Technical Support. To see if an upgrade is available, go to **/appliance > Updates**.

Click on **Check for updates**.


If a software update is available, it will appear under **Available Updates**. Once you click **Install This Update**, the appliance will download and automatically install the new version of the BeyondTrust software.




> ***Note:*** *"BeyondTrust" software updates often depend on one or more "Base Software" updates. Install the available Base Software updates to enable the dependent BeyondTrust updates. Then download a backup and immediately install the BeyondTrust software updates before doing anything else, such as failing over or installing updates on another appliance.*

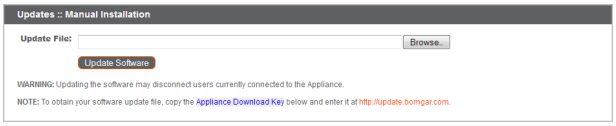
If automatic updates fail when expected to work, please review the Check for Updates troubleshooting FAQ at help.bomgar.com/SSC/Main.aspx?rurl=377.

**Manual**

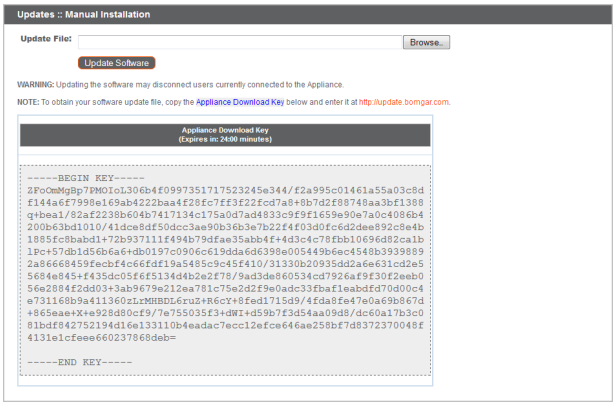
If you are unable to use automatic updates (e.g., if your appliance exists on a restricted network), you may perform manual updates.

Go to **/appliance > Updates**.


Starting with Base 3.3.2, click the **Appliance Download Key** link to generate a unique appliance key; prior to Base 3.3.2, you must contact BeyondTrust Technical Support to request this key. From a non-restricted system, submit this key to BeyondTrust's update server at https://update.bomgar.com. Download any available updates to a removable storage device and then transfer those updates to a system from which you can manage your appliance.




From the **Updates** page, browse to the file from the **Manual Installation** section and then click the **Update Software** button to complete the installation. The appliance will install the new version of the BeyondTrust software.




> ***Note:*** *Be prepared to install software updates directly after download. Once an update has been downloaded, it no longer appears in your list of available updates. Should you need to re-download an update, contact BeyondTrust Technical Support.*

## Verify and Test

After completing the upgrade process, verify that the update completed successfully and that your software is working as expected.

On a minimum of two local machines that can access **Appliance B**, edit the hosts file so that your site hostname resolves to the IP address of **Appliance B**. On one computer, run the representative console. Your installed representative consoles will need to be upgraded after the site upgrades. Typically, this occurs automatically the next time the representative run the representative console.To check the software build that a console is running, log into the console and then click **Help > About**. Also be sure that you can make a connection to a remote computer via a session.

> ***Note:*** *Representative consoles previously deployed on locked-down computers using MSI may need to be re-deployed once the upgrade is complete. If the extractable representative console or extractable Jump Client feature has been enabled for your site by BeyondTrust Technical Support, then you can download an MSI installer to update representative consoles and/or Jump Clients prior to upgrading the appliance. To do this, check for the new update either manually or automatically. Click the* ***Rep Console Installers*** *or* ***Jump Client Installers*** *link to download the MSI for distribution. Note that the updated clients will not come online until their appliance is updated. It is not necessary to uninstall the original client prior to deploying the new one, as the new one should automatically replace the original installation. It is a best practice, however, to keep a copy of the old MSI to remove the outdated installations after the appliance is updated should this removal prove necessary. The new MSI is unable to do so.*

## Make Appliance B the Primary Appliance

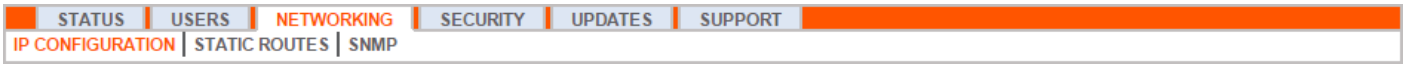
Set **Appliance B** to the primary role following the steps previously determined in your failover plan: shared IP switch, DNS swing, or NAT swing.

> ***Note:*** *If you are using the BeyondTrust Integration Client and have configured it based on IP address rather than hostname, be sure to verify that it can extract data from* ***Appliance B*** *after redefining* ***Appliance B*** *as the primary appliance.*

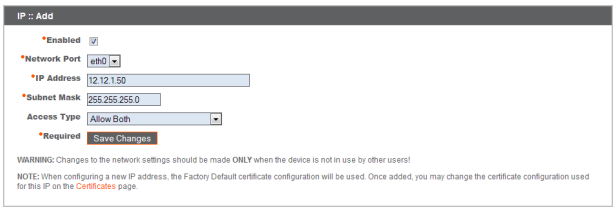
> ***Note:*** *Data from remote support sessions completed on either appliance while failover is not enabled will automatically sync once the failover relationship has been re-established.*

**Shared IP Switch**

On **Appliance A**, go to **/appliance > Networking > IP Configuration**.




Click on the shared IP address to edit it, and uncheck the **Enabled** box. Then click **Save Changes**.




Immediately, go to **/appliance > Networking > IP Configuration** on **Appliance B**. It is helpful to have this page already open in a separate browser tab.

Click on the shared IP address to edit it, and check the **Enabled** box. Then click **Save Changes**.

As soon as the switch is made, you can resume normal activity. All requests to your site will be served by **Appliance B**.

**DNS Swing**

Access the DNS controller and locate the DNS entry for your BeyondTrust site. Edit the entry to point to the IP address for **Appliance B**. Once the DNS entry has propagated, you can resume normal activity. All requests to your site will be served by **Appliance B**.

**NAT Swing**

Access the NAT controller and locate the NAT entry for your BeyondTrust site. Edit the entry to point to the IP address for **Appliance B**. As soon as the change is made, you can resume normal activity. All requests to your site will be served by **Appliance B**.

## Update Appliance A

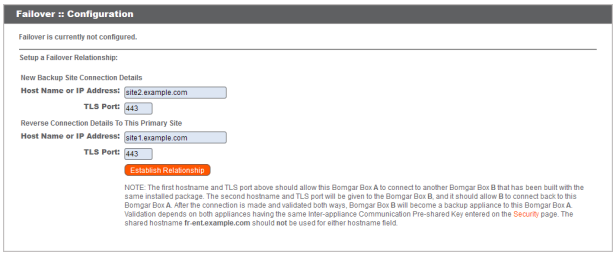
> ***Note:*** *Each customer environment is different, and while BeyondTrust does test each feature, we cannot test each and every scenario a customer may encounter. Please confirm that the BeyondTrust software is working in your environment before updating Appliance A.*

Update **Appliance A** using either the automatic or the manual update method as defined above. Then verify and test that the update completed successfully.

## Reestablish Failover Relationship

From **Appliance B**, go to **/login > Management > Failover**.


> ***Note:*** *To configure a valid connection, both appliances must have identical Inter-Appliance keys. See the* ***/login > Management > Security*** *page to verify the key for each appliance.*




Reestablish the failover relationship with the backup appliance, using **Appliance A** as the backup and **Appliance B** as the primary.

Establishing the relationship between the two appliances occurs on the **Failover** page of the appliance intended to be the primary appliance. The addresses that are entered here will establish the relationship and allow either appliance to connect to each other at any time. The fields on this page called **New Backup Site Connection Details** tell the primary appliance how to connect to the appliance that will become the backup appliance. The fields called **Reverse Connection Details to this Primary Site** will be given to the backup appliance and tell it how to connect back to this primary appliance. You must use a valid hostname or IP address and the TLS port number for these fields. When all of these fields are set, click the **Establish Relationship** button to attempt to establish the relationship.

> ***Note:*** *Whenever possible, BeyondTrust recommends using the unique IP address of each appliance when configuring these settings.*

Once the relationship has been established, extraneous tabs will be removed from the backup site. It takes about 60 seconds for the first data synchronization to initiate, but you may also click the **Sync Now** button to force synchronization and pull the most current information from the primary appliance into the memory of the backup appliance. Synchronization itself may take anywhere from a few seconds to a few hours, depending on the amount of data that needs to be synchronized. The **Failover** page will list the last date and time of data synchronization when synchronization is completed.

Failover synchronization syncs all user accounts, all /login configuration settings, files in the file store, logs and recordings. All of this information which exists on the backup appliance will be overwritten by that which resides on the primary appliance. If the primary

appliance is the master node in an Atlas cluster, the backup appliance will automatically become the new backup master node in this cluster.

# Upgrade Multiple BeyondTrust Appliances in an Atlas Cluster

Upgrading BeyondTrust Atlas clusters is more involved than upgrading failover pairs or individual appliances. For details on how to set up and configure Atlas, see the Atlas Configuration Guide at www.beyondtrust.com/docs/remote-support/how-to/atlas. The following section explains how to properly upgrade Atlas clusters.

## With Failover Configured

These steps assume that there are two master nodes operating in a failover configuration. These are referred to as **Appliance A** (the primary master node in the failover pair) and **Appliance B** (the backup master node). If failover is not configured and there is no backup master node, skip to the section "Without Failover Configured" on page 21.

> ***Note:*** *The failover process does cause downtime. Please plan accordingly.*

**Preparation**

1. On **Appliance A**, go to **/login > Management > Software Management**.
    a. Download the available updates, but do not install them.
    b. Click the **Distribute to Cluster** button to push the package to all other nodes.

    > ***Note:*** *This does not install any new software but only prepares for it to be installed.*

2. On **Appliance A**, go to **/login > Management > Cluster**.
    a. Identify half of the traffic nodes to be temporarily disable per geographical region.
    b. On the identified nodes, uncheck **Accepting New Client Connections**. These are referred to as the offline traffic nodes.
3. On each offline traffic node, go to **/login > Status > Information**.
4. Looking at the **Connected Clients** table, wait for all active customer client and representative console connections to end. This waiting period prevents the interruption of existing sessions.

**Upgrade the Backup**

1. On **Appliance B**, go to **/appliance > Updates**.
2. Click the **Install** button to upgrade the software to the latest version, making sure to install updates in the appropriate sequence.

    > ***Note:*** *Base software updates are typically installed before licensing software updates. If the order is unclear, contact BeyondTrust Technical Support before installing any updates. The appliance automatically reboots as part of the Base software update process.*

    Updating the software automatically causes Appliance B to mark all traffic nodes as not accepting new client connections in the cluster configuration.

> ***Note:*** *Do not make changes to the configuration of* ***Appliance A*** *during this upgrade. Any such changes will be overwritten upon the first data-sync after the upgrade.*

3. Repeat the upgrade process above for each of the offline traffic nodes. Once done, **Appliance A** and half of the traffic nodes should be on the old version of BeyondTrust. **Appliance B** and the other half of the traffic nodes should be on the new version.

**Put the New Primary into Production**

> ***Note:*** *This failover process does cause downtime. Please plan accordingly.*

1. On **Appliance A**, go to **/login > Management > Failover**.
2. Check **Become backup even if the peer site cannot be contacted**.
3. Click the **Become Backup** button.

> ***Note:*** *This process causes the backup appliance to take the primary role in the failover pair.*

4. If necessary, swing DNS and/or NAT to Appliance B. If shared IP failover is configured, neither DNS or NAT settings need be changed; instead, the shared IP address auto-deactivates on Appliance A.
5. Switch to **Appliance B** and go to **/login > Management > Failover**.
6. Click **Become Primary**.
7. Uncheck the **Enable Backup Operations** checkbox.

**Bring Upgraded Traffic Nodes Back Online**

1. On **Appliance B**, go to **/login > Management > Cluster**.
2. For each traffic node which has been upgraded, check the **Accepting New Client Connections** checkbox.
3. In the **Cluster :: Status** section, click **Sync Now**.

**Upgrade the Rest of the Deployment**

1. On each traffic node which has not yet been upgraded, go to **/appliance > Updates**.
2. Click **Install** to upgrade to the new version, making sure to install updates in the appropriate sequence. Wait for the updates to finish installing.
3. Switch to **Appliance B** and go to **/login > Management > Cluster**.
4. For each traffic node upgraded in the previous step, check **Accepting New Client Connections**.

**Upgrade Appliance A**

1. On **Appliance A**, go to **/appliance > Updates**.
2. Click **Install** to upgrade to the new version, making sure to install updates in the appropriate sequence.

**Restore the Cluster Configuration**

1. On **Appliance A**, go to **/login > Management > Failover**.
2. Check **Enable Backup Operations**.

3. Switch to **Appliance B** and go to **/login > Management > Cluster**.
4. In the **Cluster :: Status** section, click **Sync Now**.

## Without Failover Configured

### Preparation

1. Go to **/login > Management > Software Management**.
    a. Download the available updates, but do not install them.
    b. Click the **Distribute to Cluster** button to push the package to all other nodes.

    > ***Note:*** *This does not install any new software but only prepares for it to be installed.*

2. Go to **/login > Management > Cluster**.
    a. Identify half of the traffic nodes to be temporarily disable per geographical region.
    b. On the identified nodes, uncheck **Accepting New Client Connections**. These are referred to as the offline traffic nodes.
3. On each offline traffic node, go to **/login > Status > Information**.
4. Looking at the **Connected Clients** table, wait for all active customer client and representative console connections to end. This waiting period prevents the interruption of existing sessions.

### Upgrade the offline nodes

1. On each offline traffic node, go to **/appliance > Updates**.
2. Click the **Install** button to upgrade the software to the latest version, making sure to install updates in the appropriate sequence.

    > ***Note:*** *Base software updates are typically installed before licensing software updates. If the order is unclear, contact BeyondTrust Technical Support before installing any updates. The appliance automatically reboots as part of the Base software update process.*

### Upgrade the master node

1. On the master node, go to **/appliance > Updates**.
2. Click the **Install** button to upgrade the software to the latest version, making sure to install updates in the appropriate sequence. Updating the software automatically causes the master node to mark all traffic nodes as not accepting new client connections in the cluster configuration.

### Bring Upgraded Traffic Nodes Back Online

1. On the master node, go to **/login > Management > Cluster**.
2. For each traffic node which has been upgraded, check the **Accepting New Client Connections** checkbox.
3. In the **Cluster :: Status** section, click **Sync Now**.

### Upgrade the Rest of the Deployment

1. On each traffic node which has not yet been upgraded, go to **/appliance > Updates**.
2. Click **Install** to upgrade to the new version, making sure to install updates in the appropriate sequence. Wait for the updates to finish installing.

**Restore the Cluster Configuration**

1. Switch to the master node and go to **/login > Management > Cluster**.
2. For each traffic node upgraded in the previous step, check **Accepting New Client Connections**.
3. In the **Cluster :: Status** section, click **Sync Now**.

# Upgrade BeyondTrust Hardware

When you upgrade your BeyondTrust Appliance from either one physical appliance to another or between a physical and a virtual appliance, you must both install the new appliance and transfer data from the original appliance.

1. Install the new appliance per the appropriate setup guide.
    - BeyondTrust Virtual Appliance Installation: www.beyondtrust.com/docs/remote-support/getting-started/deployment/virtual
    - BeyondTrust Appliance Hardware Installation: www.beyondtrust.com/docs/remote-support/getting-started/deployment/hardware
2. Back up your current appliance's software settings.
    a. On your current appliance, go to **/login > Management > Software Management**.
    b. In the **Software :: Backup Settings** section, click the **Download Backup** button.
    c. Save the backup file to a secure location.
3. Import your existing SSL certificate chain into the new appliance.

> ***Note:*** *For full details about SSL certificates and BeyondTrust, see www.beyondtrust.com/docs/remote-support/how-to/sslcertificates.*

    a. On your current appliance, go to **/appliance > Security > Certificates**.
    b. 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.*

    c. 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.
    d. On your new appliance, go to **/appliance > Security > Certificates**.
    e. In the **Security :: Certificate Installation** section, click the **Import** button.
    f. Browse to the certificate file that you exported previously and then click **Upload**.
4. Assign an IP address to the certificate.
    a. On your new appliance, go to **/appliance > Security > Certificates**.
    b. In the **Security :: Certificates** section, locate the entry for your SSL certificate. This usually has an **Issued To** field containing the fully qualified domain name of your appliance (e.g., support.example.com).
    c. Confirm there are no warnings listed for the new certificate. If there is a warning, see FAQ 755 in the BeyondTrust Technical Support Self Service Center for details on how to resolve the warning: ssc.bomgar.com/ssc/SolutionFAQ.aspx?id=755.
    d. Once all warnings are resolved, click the **Assign IP** link in the certificate row. At the bottom of the page, check the IP address to assign and then click the **Save Configuration** button.

5. Install the new software package.
    a. On your new appliance, go to **/appliance > Updates**.
    b. Either click **Check for Updates** or use the **Appliance Download Key** per the on-screen instructions.
    c. Click **Install This Update**. A EULA will need to be signed prior to installation.
6. Import your software configuration settings from the old appliance.
    a. Log into your new appliance's /login interface. The first-time login credentials are **admin** and **password**.
    b. Go to **/login > Management > Software Management**.
    c. In the **Software :: Restore Settings** section, browse to the backup file you downloaded earlier and then click **Upload Backup** to restore the backup to the new appliance.

At this point, you can update your DNS server to direct traffic to the IP address of the new appliance, and you can start testing remote support on your new appliance. Once you have confirmed that it is functioning properly, you can return the old appliance, if physical, or delete it, if virtual. To return a physical appliance, take these steps:

1. Log into the **/appliance** web interface of the old appliance.
2. Browse to the **Status > Basics** page, and click **Reset Appliance to Factory Defaults**.
3. Wait for the reset to complete, and then click **Shut Down This Appliance**.
4. Package the appliance for shipping.
5. Affix the BeyondTrust return shipping label to the outside of the box and contact your shipper for a pickup. If you do not have a label for shipment, contact BeyondTrust Technical Support.

# Disclaimers, Licensing Restrictions and Tech Support

## Disclaimers

This document is provided for information purposes only. BeyondTrust Corporation may change the contents hereof without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. BeyondTrust Corporation specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionality, services, and processes described herein are subject to change without notice.



## Licensing Restrictions

One BeyondTrust Remote Support license enables one support representative at a time to troubleshoot an unlimited number of remote computers, whether attended or unattended. Although multiple accounts may exist on the same license, two or more licenses (one per concurrent support representative) are required to enable multiple support representatives to troubleshoot simultaneously.

## Tech Support

At BeyondTrust, we are committed to offering the highest quality service by ensuring that our customers have everything they need to operate with maximum productivity. Should you need any assistance, please contact BeyondTrust Technical Support at help.bomgar.com.

Technical support is provided with annual purchase of our maintenance plan.