



BeyondTrust

Privileged Remote Access Failover Configuration

Table of Contents

Failover Dynamics and Options with BeyondTrust Privileged Remote Access	4
Set Up the Primary/Backup Failover Relation Between Two B Series Appliances	5
Best Practices for Primary and Backup PRA Environments	8
Methods of Network Configuration for PRA B Series Appliance Failover	9
Set Up a Shared IP Address for PRA Failover B Series Appliance Configuration	10
Configure Networking on the B Series Appliances	10
Example Shared IP Configuration	10
Set Up DNS Swing for PRA Failover B Series Appliance Configuration	12
Configure Networking on the B Series Appliances	12
Example DNS Swing Configuration	12
Set Up NAT Swing for PRA Failover B Series Appliance Configuration	13
Configure Networking on the B Series Appliances	13
Example NAT Method Configuration	13
Replicate SSL Certificate Configuration on the Backup PRA B Series Appliance	14
Perform Failover for Planned Maintenance of the PRA Environment	16
Perform Failover for Unplanned Maintenance of the PRA Environment	17
Unplanned Maintenance with No Recent Change in /login	17
Unplanned Maintenance with Recent Changes in /login	17
Use the BeyondTrust API to Check PRA B Series Appliance Health and Perform Failover	19
Check B Series Appliance Health	19
Set Failover Roles	20
Resolve Conflicts in a PRA Failover Setup	21
Replace a BeyondTrust Appliance B Series in a Failover Scenario	22
Install the New B Series Appliance	22
Restore the Failover Configuration	23
Return the Defective B Series Appliance	24
Appendix: PRA Administration Settings for Failover	25
Configuration	25
Status	25
Primary or Backup Site Instance Status	26

Primary or Backup Site Instance Configuration	26
Backup Settings	26

Failover Dynamics and Options with BeyondTrust Privileged Remote Access

BeyondTrust failover enables synchronization of data between two peer B Series Appliances, creating a simplified process for secure swap from a failed B Series Appliance. Two B Series Appliances host the same installed software package for a single site. You can check this from the /login admin web interface. If the **Product Version** and **Product Build** match, the same site software package is installed. DNS directs support traffic of the site to one of these peer B Series Appliances, the primary B Series Appliance, where all settings are configured. The backup B Series Appliance synchronizes with the primary, according to your settings configured in the /login interface.

This document describes how to use a second B Series Appliance as a backup and failover device for a PRA site and how to switch operations to the backup B Series Appliance in a disaster recovery situation. There are three network configuration methods available with PRA failover for redirecting network traffic so that your support site remains available:

1. Shared IP
2. DNS Swing
3. NAT Swing

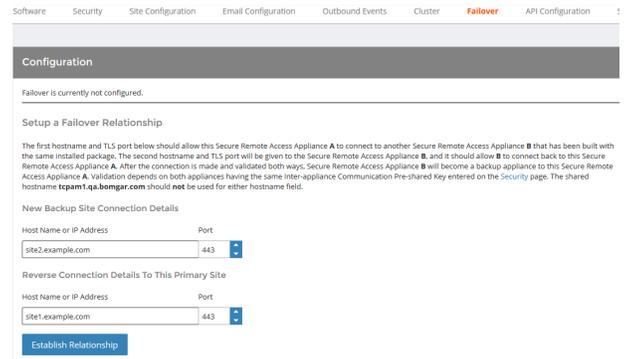
Configuration details regarding each of these methods follow in this document, and detailed failover steps are also covered. Your B Series Appliances have a peer relationship, so implementing the Shared IP failover configuration with automatic data synchronization enabled is recommended. Both B Series Appliances must be on the same IP subnet to support Shared IP failover; therefore, it may be necessary to use DNS or NAT swing failover methods. Failover can be further managed and automated using the BeyondTrust API.



For more information on the pros and cons of each option, please see ["Methods of Network Configuration for PRA B Series Appliance Failover"](#) on page 9.

Set Up the Primary/Backup Failover Relation Between Two B Series Appliances

BeyondTrust failover enables automatic synchronization of data between two B Series Appliances, creating a simplified, two-way process. To start automatically synchronizing site data between two B Series Appliances, you must first establish a trusted relationship between them. On the B Series Appliance you intend to be primary, go to **/login > Management > Failover**.



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

Establishing the relationship between the two B Series Appliances occurs on the **Failover** page of the B Series Appliance intended to be the primary B Series Appliance. The addresses that are entered here will establish the relationship and allow either B Series Appliance to connect to each other at any time. The **New Backup Site Connection Details** tell the primary B Series Appliance how to connect to the B Series Appliance that will become the backup B Series Appliance. The **Reverse Connection Details to this Primary Site** are given to the backup B Series Appliance and tell it how to connect back to this primary B Series Appliance. You must use a valid hostname or IP address and 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 B Series Appliance when configuring these settings.

Once the relationship has been established, extraneous tabs are removed from the backup site.

If you are on the primary B Series Appliance, you will see **Failover** page sections indicating **Primary Site Instance**. If you are on the backup B Series Appliance, you will only see **Failover** page sections indicating **Backup Site Instance**. The **Backup Settings** section refers to settings enabled only when the site instance you are on is the backup site instance.



On the primary B Series Appliance's **Failover** page, the top of the page displays the address and status of the host/primary site and the peer/backup site, as well as the date and time of the last status check. Select **Status History** to expand or collapse a table of status events that have occurred.

When you establish a new failover relationship, an initial data synchronization automatically occurs. It takes about 60 seconds for the first data sync to begin.

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 B Series Appliance will be overwritten by that which resides on the primary B Series Appliance.

 **Note:** If the primary B Series Appliance is the primary node in an Atlas cluster, the backup B Series Appliance will automatically become the new backup primary node in this cluster.

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.

Later, you will set up a schedule for automatic data syncs. However, you may also click the **Sync Now** button to force synchronization and pull the most current information from the primary B Series Appliance into the memory of the backup B Series Appliance.

To manually switch B Series Appliance roles, click **Become Backup** from the primary site or **Become Primary** from the backup site.

If you want to synchronize data from the peer B Series Appliance prior to swapping roles, select the checkbox next to the **Become Primary** or **Become Backup** button. If this option is selected, all users on the existing primary B Series Appliance will be disconnected during the data sync, and no other operations will be available until the swap is complete.

On the primary site instance, you also have the option to become the backup even if the peer B Series Appliance cannot be contacted. If this option is unchecked, failover will be canceled if both B Series Appliances cannot be kept in sync in terms of their failover roles (one primary and one backup).

For example, if you know the current backup B Series Appliance is online but cannot be reached by the primary due to a network connection issue, you may wish to check this option to make the primary the backup before the network connection is restored. In this example, you would also need to access the current backup and make it the primary.

If you want to break the relationship so that the primary B Series Appliance is no longer linked to the backup B Series Appliance, click the **Break Failover Relationship** button. Data will no longer be synchronized between the two, and if the primary B Series Appliance goes offline, the other B Series Appliance will not take over.

 **Note:** This will not remove configuration settings and session data that has already been copied from the primary to the backup.

From **Primary Site Instance Configuration**, control the shared IP address the site instance uses in the event of a failover by selecting the checkbox for the failover IP address. If you change the relationship between the sites, the checked IP addresses will disable when a primary site becomes a backup, and will enable when a backup becomes a primary site. You should manually mirror the setting on the peer site, as the setting is not shared. Select **Save Changes** when finished.

From **Backup Settings**, configure how the B Series Appliance should behave when in the backup role. These settings must be configured on both the primary and backup B Series Appliances.

Enable or disable backup operations, such as data-syncs and automatic failovers.

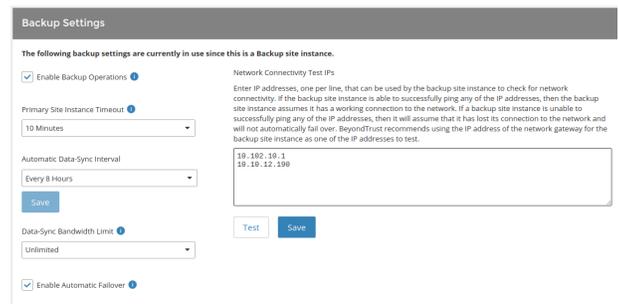
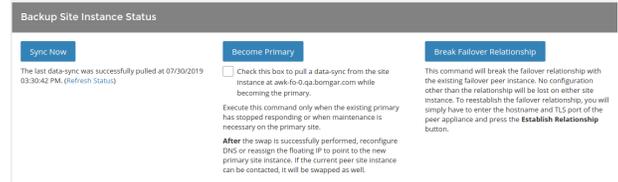
Set how long the primary site must be unreachable before failover occurs.

Set how often data should automatically synchronize, as well as the maximum bandwidth that can be used for data syncs.

Enable or disable automatic failover. If disabled, failover must be performed manually.

 **Note:** In order to use BeyondTrust's built-in automatic failover, your two B Series Appliances must be on the same subnet. If you wish to use automatic failover with B Series Appliances on different networks, you must use the failover API.

You also may enter IP addresses for the backup site to check to determine whether the backup's inability to reach the primary is because the primary is offline or because the backup has lost its network connection.





For more information about failover settings, please see "[Best Practices for Primary and Backup PRA Environments](#)" on page [8](#).

After failover is configured, the primary B Series Appliance will send an email alert if no backup B Series Appliance pulls its data for a given length of time. This allows you to be aware if relationships have been disrupted. To activate this alert email, enter connection parameters for a working SMTP server on the primary B Series Appliance's **/login > Management > Email Configuration** page. The next synchronization will copy the settings to the backup.

If the backup B Series Appliance determines that the primary B Series Appliance is down, it will send a series of emails to the B Series Appliance administrator notifying them of the failure and counting down the time until automatic failover will occur. The backup B Series Appliance will attempt to reach the primary for the length of time specified by the **Primary Site Instance Timeout**. If it is unable to reach the primary during this time, then the backup will enable the shared IP and will assume the role of primary if automatic shared IP failover is configured; otherwise, you must configure failover manually. As soon as the switch is made, you can resume normal support activity. All requests to your support site will be served by the backup B Series Appliance.

Best Practices for Primary and Backup PRA Environments

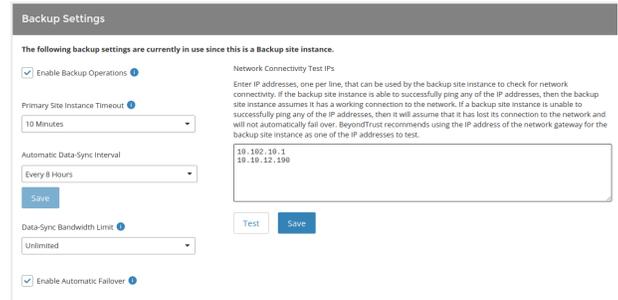
Here are best practices for using failover in the backup environment and planned and unplanned maintenance environments.

! IMPORTANT!

Deviation from these best practices may result in data loss.

In an ideal environment, you should select one B Series Appliance as the normal primary and another B Series Appliance as the normal backup. The normal primary will almost always be primary unless there is a maintenance event, and once the event is over, the original primary will be restored to the role of primary. This practice allows you to select the proper backup options (bottom section of the **Management > Failover** page in the **/login** interface) for each site and presents the greatest likelihood that no data is lost. The options are presented in the table below.

Backup options are per-site (not synchronized) settings and are only in use when the site's role is **backup**. Since you have established each site as normally primary or normally backup, it may be helpful to think of these settings in a categorical framework of **normal** and **maintenance** modes, where the Backup Site Settings are in effect during normal operations and the Primary Site Settings are in effect during maintenance. In short, turn off **Enable Backup Operations** on the normal primary site. Do this because enabling that option will generate administrative emails and could cause a data-sync to start. This, of course, is not helpful while maintenance is being performed and could cause data loss.



The screenshot shows the 'Backup Settings' configuration page. It includes a warning that the following settings are currently in use because this is a Backup Site instance. The settings are:

- Enable Backup Operations (Info icon)
- Primary Site Instance Timeout: 10 Minutes
- Automatic Data-Sync Interval: Every 8 Hours
- Data-Sync Bandwidth Limit: Unlimited
- Enable Automatic Failover (Info icon)

 There is also a 'Network Connectivity Test IPs' section with a text area containing '10.102.10.1' and '10.10.12.199', and 'Test' and 'Save' buttons.

Setting	Primary Site Setting	Backup Site Setting	Reason
Enable Backup Operations	Off	On	Controls probing and data-syncs as well as auto-failover, both of which will be problematic if the normal primary is down.
Auto Data-Sync Interval	<i>not applicable</i>	<i>user's choice</i>	Data syncs should generally be at least once a day, but the more frequent the better. The bigger the gap, the more potential for losing data not captured with synchronization.
Bandwidth Limiting	<i>user's choice</i>	<i>user's choice</i>	Does not matter what this is set to, as long as data-syncs can occur fast enough not to overlap the next time it is supposed to sync. Remember that the backup site's setting will be the one used when they differ.
Enable Automatic Failover	Off	On for Shared IP User's choice for DNS and NAT Swing	Presents the possibility for data loss if a data-sync does not occur before the role change. Obviously, with hardware failure, sometimes this cannot be avoided.
Primary Site Instance Timeout	<i>not applicable</i>	<i>user's choice</i>	Depends on user's choice for automatic failover.

Methods of Network Configuration for PRA B Series Appliance Failover

BeyondTrust endpoint clients and access consoles are built to attempt connection to the B Series Appliance at a specific address. In order to stop the clients from connecting to the normal primary B Series Appliance and instead connect to the backup B Series Appliance, a network change must be made in order to reroute the traffic to its new destination. There are currently three methods supported to achieve this goal, each with advantages and disadvantages.

Method	Description	Pros	Cons
Shared IP	In this configuration, the hostname of the PRA site and IP address that is used to represent it remain constant. Both B Series Appliances share that IP in the /appliance interface, but only the B Series Appliance that is acting as primary has that IP enabled. The backup B Series Appliance will not use that IP unless it becomes primary.	No network equipment configuration change. Links and processes referencing your site domain or IP address will be adjusted properly based on roles and will be served by the backup B Series Appliance. Once the backup B Series Appliance is redefined as the primary and the shared IP is enabled, the backup B Series Appliance will take the place of the primary. Does not suffer from the propagation time lag as a DNS entry change would.	Potential for IP conflict if the shared IP is enabled on both B Series Appliances. If both B Series Appliances are online and conflicted, go back to /login > Management > Failover and reconfigure the settings so that the roles are accurately set.
DNS Swing	Change the DNS entry for your Privileged Remote Access site from the IP address for the primary B Series Appliance to the IP address of the backup B Series Appliance. Since DNS changes must propagate through your network, this change might require some time.	Links and processes referencing your site domain do not need to be changed and are served by the backup B Series Appliance. Can be used in sites that are on different subnets.	Requires a change to networking equipment configuration that coordinates with changes to the failover roles in the /login interface. The DNS entry change takes some time to propagate depending on the DNS record time to live. Until the new DNS entry is propagated, users may not be able to reach the site.
NAT Swing	Change the routing of requests for the Privileged Remote Access site at the NAT device from the primary B Series Appliance to the backup B Series Appliance.	Links and processes referencing your site domain or IP address do not need to be changed and are served by the backup B Series Appliance. Does not suffer from the propagation time as a DNS entry change would. Can be used in sites that are on different subnets.	Requires a change to networking equipment configuration that coordinates with changes to the failover roles in the /login interface.

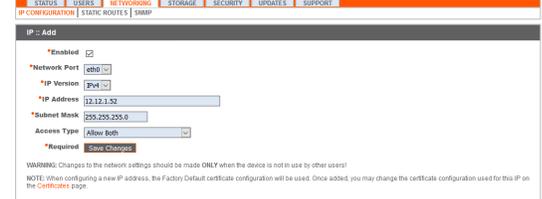
When the primary B Series Appliance in a failover cluster fails and the backup B Series Appliance takes the primary role, any [connection agents](#) for the primary B Series Appliance dynamically connect with the new primary, regardless of the failover method. No restart of the client or its host is needed; however, it is important that DNS, network, and firewall systems allow traffic from the connection agent to the backup B Series Appliance in addition to the primary. These agents use the HTTPS protocol over TCP 443 to make their connections.



Note: To configure a valid connection, both B Series Appliances must have identical Inter-Appliance keys. Go to **/login > Management > Security** to verify the key for each B Series Appliance.

Set Up a Shared IP Address for PRA Failover B Series Appliance Configuration

In this configuration, the hostname of the Privileged Remote Access site and IP address that is used to represent it remain constant. Both B Series Appliances share that IP in the `/appliance` interface, but only the B Series Appliance that is acting as primary has that IP enabled. The backup B Series Appliance does not use that IP unless it becomes primary.



Configure Networking on the B Series Appliances

Log into the `/appliance` administrative interface for your primary B Series Appliance, accessible from either its unique hostname or IP address (e.g., <https://site1.example.com/appliance> or <https://12.12.1.50/appliance>).

Go to the **Networking > IP Configuration** page, click **Add New IP**, and enter the IP and subnet mask for the shared IP, keeping the IP **Enabled**. If the B Series Appliances' hostnames or IP addresses cannot communicate, you must give each B Series Appliance a unique IP address which can reach the other. Unlike the shared IP, the unique IP of each B Series Appliance should remain enabled at all times.

Log into the `/appliance` administrative interface for your backup B Series Appliance, accessible from either its unique hostname or IP address (e.g., <https://site2.example.com/appliance> or <https://12.12.1.51/appliance>).

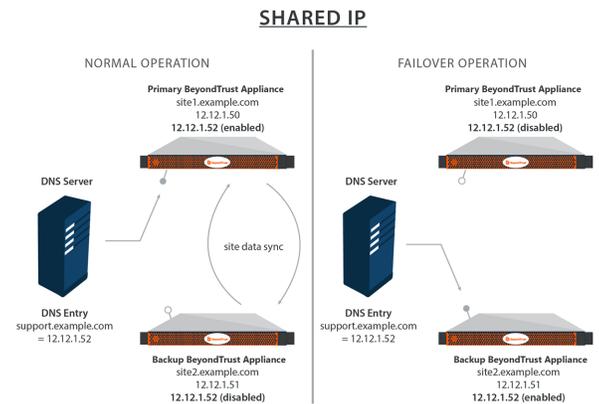
For the backup, go to the **Networking > IP Configuration** page. If you have not already configured your static IP, click **Add New IP** and enter the static IP and subnet mask, making sure to keep this IP **Enabled**. Then click **Save Changes**. Add the shared IP to this B Series Appliance following these same steps and disable the shared IP for the backup B Series Appliance to prevent an IP conflict on the network.

From the **Primary/Backup Site Instance Configuration** section in the `/login` interface, you control the IP addresses which the site instance uses if a failover event occurs. This must be set to the shared failover IP on both the primary and the backup B Series Appliances. Once this is set, the primary site in the failover relationship will enable the IP you selected. The backup site will disable that IP when the roles change.

Because traffic from BeyondTrust security providers can flow out of any IP address on a B Series Appliance, it is important to ensure the network firewall allows access from all BeyondTrust IP addresses on both B Series Appliances in failover to the necessary authentication systems. For example, when two B Series Appliances in shared IP failover are configured to authenticate users on an Active Directory (AD) server using LDAPS port 636, the firewall between the B Series Appliances and the AD server must allow traffic over TCP 636 to pass from *any* of the IP addresses on *either* B Series Appliance in order to insure reliable authentication performance.

Example Shared IP Configuration

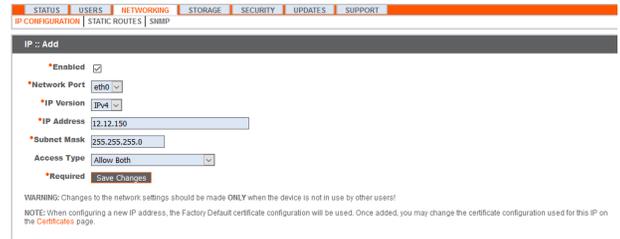
	Primary B Series Appliance	Backup B Series Appliance
Definition	The B Series Appliance used during normal operations.	The B Series Appliance used during failover operations.
Hostname/IP Address	site1.example.com (12.12.1.50)	site2.example.com (12.12.1.51)



	Primary B Series Appliance	Backup B Series Appliance
Site Name/Shared IP	access.example.com (12.12.1.52)	

Set Up DNS Swing for PRA Failover B Series Appliance Configuration

Change the DNS entry for your Privileged Remote Access site from the primary B Series Appliance IP address to the IP address of the backup B Series Appliance.



Configure Networking on the B Series Appliances

Log into the **/appliance** administrative interface for your primary B Series Appliance, accessible from either its unique hostname or IP address (e.g., <https://site1.example.com/appliance> or <https://12.12.1.50/appliance>).

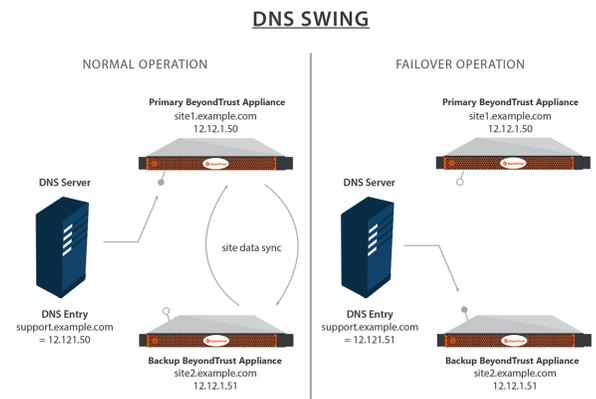
Because DNS directs the site domain, **access.example.com**, to this IP address, this is the primary B Series Appliance. All session activity will occur on this B Series Appliance.

Log into the **/appliance** administrative interface for your backup B Series Appliance, accessible from either its unique hostname or IP address (e.g., <https://site2.example.com/appliance> or <https://12.12.1.51/appliance>).

Go to the **Networking > IP Configuration** page. If you have not already configured your static IP, click **Add New IP** and enter the static IP and subnet mask, making sure to keep this IP **Enabled**. Then click **Save Changes**.

In the event that you encounter a potential failover situation, try to reserve failing over as an absolute last resort. If the primary B Series Appliance, Appliance A, is down, it is often quicker and has less of an impact to bring it back up rather than failing over to the backup B Series Appliance, Appliance B.

To fail over, access the DNS controller and locate the DNS entry for your Privileged Remote Access site (e.g., **access.example.com**). Edit the entry to point to the backup IP. Click **Become Primary** from the backup B Series Appliance **Failover** page. Once the DNS entry has propagated, you can resume normal activity. All requests to your site will be served by the backup B Series Appliance. Exact methods for achieving this task vary depending on your DNS provider and software, so consult your DNS documentation for exact steps to do this.



Example DNS Swing Configuration

	Primary B Series Appliance	Backup B Series Appliance
Definition	The B Series Appliance used during normal operations.	The B Series Appliance used during failover operations.
IP Address	12.12.1.50	12.12.1.51
Hostname	site1.example.com	site2.example.com
Site Name	access.example.com (12.12.1.50 or 12.12.1.51 as determined by DNS Server setting)	

Set Up NAT Swing for PRA Failover B Series Appliance Configuration

Configure Networking on the B Series Appliances

Log into the **/appliance** administrative interface for your primary B Series Appliance, accessible from either its unique hostname or IP address (e.g., <https://site1.example.com/appliance> or <https://192.168.1.50/appliance>).

Go to the **Networking > IP Configuration** page. If you have not already configured your static IP, click **Add New IP** and enter the static IP and subnet mask, making sure to keep this IP **Enabled**. Then click **Save Changes**.

Because NAT directs the IP for the Privileged Remote Access site domain, access.example.com, to this IP address, this is the primary B Series Appliance.

Log into the **/appliance** administrative interface for your backup B Series Appliance, accessible from either its unique hostname or IP address (e.g., <https://site2.example.com/appliance> or <https://192.168.1.51/appliance>).

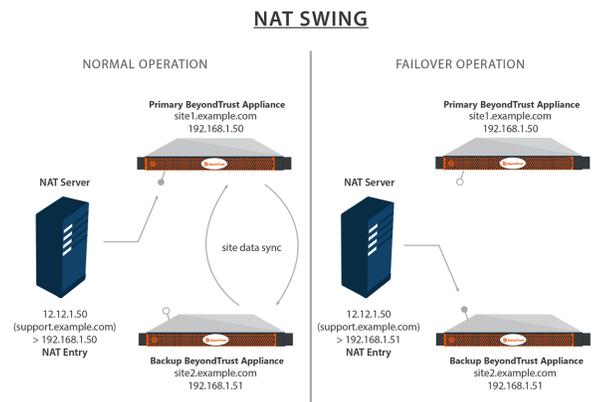
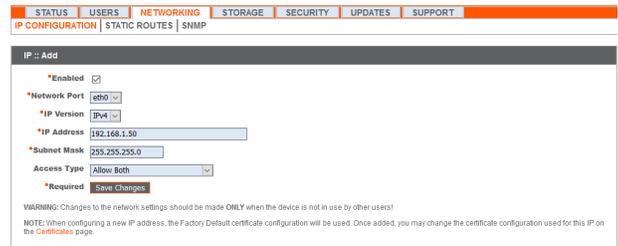
Go to the **Networking > IP Configuration** page. If you have not already configured your static IP, click **Add New IP** and enter the static IP and subnet mask, making sure to keep this IP **Enabled**. Then click **Save Changes**.

In the event that you encounter a potential failover situation, try to reserve failing over as an absolute last resort. If the primary B Series Appliance is down, it is often quicker and has less of an impact to bring it back up rather than failing over to the backup B Series Appliance.

To fail over, access the NAT controller and locate the NAT entry for your Privileged Remote Access site (e.g., **access.example.com**). Edit the entry to point to the backup IP. Click **Become Primary** from the backup B Series Appliance **Failover** page. As soon as the NAT change is made, you can resume normal activity. All requests to your site will be served by the backup B Series Appliance.

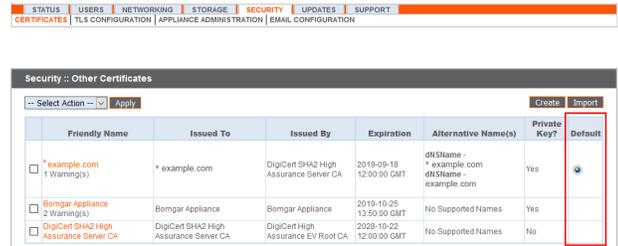
Example NAT Method Configuration

	Primary B Series Appliance	Backup B Series Appliance
Definition	The B Series Appliance used during normal operations.	The B Series Appliance used during failover operations.
Private IP Address	192.168.1.50	192.168.1.51
Hostname	site1.example.com	site2.example.com
Site Name	access.example.com (Translated to 192.168.1.50 or 192.168.1.51 by NAT Server)	



Replicate SSL Certificate Configuration on the Backup PRA B Series Appliance

The primary and backup B Series Appliances must have identically matching SSL certificates for failover to be successful. Otherwise, in the event of failover, the backup B Series Appliance will be unable to connect with any BeyondTrust clients, such as access consoles, endpoint clients, and so forth.



! IMPORTANT!

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

To replicate the SSL certificate configuration that is on your primary B Series Appliance, log into the **/appliance** web interface of the primary B Series Appliance. Navigate to **Security > Certificates** and check the box beside the desired certificate. Then, from the dropdown menu, select **Export**.

Export this certificate, along with its private key and certificate chain. The **Passphrase** field allows you to protect the certificate export with a passphrase. This is strongly recommended when exporting a private key.



Log into the **/appliance** web interface of the backup B Series Appliance. Navigate to **Security > Certificates** and click the **Import** button.

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



The imported certificate chain will now appear in the table of certificates. Click the name of the newly imported server certificate. The **Friendly Name** and/or an **Alternative Name** should match the URL of the B Series Appliance.

Security :: Other Certificates							
-- Select Action -- Apply						Creates	Import
Friendly Name	Issued To	Issued By	Expiration	Alternative Name(s)	Private Key?	Default	
<input type="checkbox"/> * example.com 1 Warning(s)	* example.com	DigiCert SHA2 High Assurance Server CA	2019-09-18 12:00:00 GMT	dNSName - * example.com dNSName - example.com	Yes	<input checked="" type="radio"/>	
<input type="checkbox"/> Bomgar Appliance 2 Warning(s)	Bomgar Appliance	Bomgar Appliance	2019-10-25 13:50:00 GMT	No Supported Names	Yes	<input type="radio"/>	
<input type="checkbox"/> DigiCert SHA2 High Assurance Server CA	DigiCert SHA2 High Assurance Server CA	DigiCert High Assurance EV Root CA	2028-10-22 12:00:00 GMT	No Supported Names	No	<input type="radio"/>	

For connections that do not supply a Server Name Indication (SNI) or supply an incorrect SNI, select a default SSL certificate from the list to provide for these connections by clicking the button under the **Default** column. The default SSL certificate cannot be a self-signed certificate nor the default B Series Appliance certificate provided for initial installation.

Security :: Other Certificates							
-- Select Action -- Apply						Creates	Import
Friendly Name	Issued To	Issued By	Expiration	Alternative Name(s)	Private Key?	Default	
<input type="checkbox"/> * example.com 1 Warning(s)	* example.com	DigiCert SHA2 High Assurance Server CA	2019-09-18 12:00:00 GMT	dNSName - * example.com dNSName - example.com	Yes	<input checked="" type="radio"/>	
<input type="checkbox"/> Bomgar Appliance 2 Warning(s)	Bomgar Appliance	Bomgar Appliance	2019-10-25 13:50:00 GMT	No Supported Names	Yes	<input type="radio"/>	
<input type="checkbox"/> DigiCert SHA2 High Assurance Server CA	DigiCert SHA2 High Assurance Server CA	DigiCert High Assurance EV Root CA	2028-10-22 12:00:00 GMT	No Supported Names	No	<input type="radio"/>	

 For more information about SNI, please see [Server Name Indication](https://www.cio.gov/sni/) at <https://www.cio.gov/sni/>.

Perform Failover for Planned Maintenance of the PRA Environment

IMPORTANT!

These flows depend on using the backup settings described in the topic "[Best Practices for Primary and Backup PRA Environments](#)" on page 8.

This is the preferred method of maintenance. This method provides a path for ensuring that all settings, recordings, and data are migrated from original primary to new primary, then back to the original primary. This method is also sufficient for upgrading B Series Appliances as well.

1. Go to the primary or backup failover page at **/login > Management > Failover**.
2. Click **Check this box to pull a data-sync from the site instance while becoming the backup** next to **Become <role>**.
3. Click **Become <role>** and wait.
 - The page will come back, and a data-sync will be in progress.
 - All clients will be disconnected from the B Series Appliance and will not be able to log back in during this time. This ensures no new session data is generated during the sync.
 - When the sync is over, the roles will swap, assuming both sides are reachable.
 - Do not panic if you refresh the page and the roles are both **Backup** momentarily. The role swap is handled serially, so it will only be a moment that this occurs. Wait a little longer, and the old backup should become primary.
4. If necessary, swing DNS or the NAT after you see that the roles swap. If configured for Shared IP, skip this step.
5. The original backup B Series Appliance is now the primary B Series Appliance.
6. Perform maintenance on the primary.



Note: During failover sync, **/login** settings on the currently active primary take precedence over those found on the backup B Series Appliance. This means that in case of conflicts, changes to the **/login** settings of the current primary will overwrite those of the backup site during failover sync. If you make changes to the backup site, consider noting the changes or downloading a backup (without logged history) from the **Management > Software Management** tab.

- During this time, track any changes made in **/login** of the new primary site.
 - Sessions may be performed normally.
 - The settings of the current primary may be modified in the **/login** interface just as if it were the normal primary. They will not be lost when the original primary takes over again.
7. When the primary is ready to resume its normal duties and is back on the network, repeat steps 1-4, but change the original primary to back to primary.



Note: Instead of going to the **/login** interface to change roles, you can use the BeyondTrust failover API. For details, see "[Use the BeyondTrust API to Check PRA B Series Appliance Health and Perform Failover](#)" on page 19.

Perform Failover for Unplanned Maintenance of the PRA Environment

! IMPORTANT!

These flows depend on using the backup settings described in the topic "[Best Practices for Primary and Backup PRA Environments](#)" on page 8. This method may result in situations where `/login` interface settings might be lost, but that can be mitigated if you are careful to track what changes were made in `/login` during the maintenance period.

This flow assumes the normal primary site is already down and unreachable from the backup. If it is reachable, use the "[Perform Failover for Planned Maintenance of the PRA Environment](#)" on page 16. This flow also assumes automatic failover is off. If automatic failover is on and has already occurred, you can skip down to step 3 for the appropriate flow.

If no changes have been made in the `/login` interface since the last data-sync, use the first flow. Otherwise, use the second flow.

Unplanned Maintenance with No Recent Change in `/login`

1. Go to the backup failover page at `/login > Management > Failover`.
2. Click **Become Primary** and wait.
 - This site will be missing any session data and recordings since the last data-sync.
 - Care should be taken to not make changes to settings in `/login` while the backup is acting as primary. Any changes that are made will be lost when the site is made the backup again. Any support session recordings and data will not be lost, however.
3. If necessary, perform a DNS or NAT swing after you see that the roles swap. If configured for Shared IP, skip this step.
4. Perform maintenance on the primary.
5. When the primary is ready to resume its normal duties, repeat steps 1-3 to reverse the roles, but check the **Check this box to pull a data-sync from the site instance while becoming the backup** BEFORE clicking **Become Primary**.

Unplanned Maintenance with Recent Changes in `/login`

1. Go to the backup failover page at `/login > Management > Failover`.
2. Click **Become Primary** and wait.
 - This site will be missing any session data, recordings, and `/login` setting changes since the last data-sync.
 - Care should be taken to not make changes to settings in `/login` while the backup is acting as primary. Any changes that are made will be lost when the site is made the backup again. Any session recordings and data will not be lost, however.
3. If necessary, perform a DNS or NAT swing after you see that the roles swap. If configured for Shared IP, skip this step.
4. Perform maintenance on the primary.
 - During this time, track any changes made in `/login` of the new primary site with the exception of the failover page.
5. When the primary is ready to resume its normal duties, repeat steps 1-3 to swap roles back.
6. Re-apply any settings changes in `/login` from the changes list.
7. Perform a data-sync.



Instead of going to the `/login` interface to change roles, you can use the BeyondTrust failover API. For details, please see ["Use the BeyondTrust API to Check PRA B Series Appliance Health and Perform Failover"](#) on page 19.

Use the BeyondTrust API to Check PRA B Series Appliance Health and Perform Failover

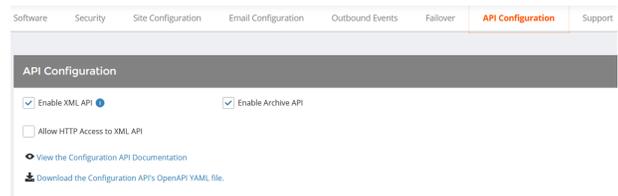
The BeyondTrust API includes calls to manage and automate failover. Following the basic flows set forth in "[Perform Failover for Planned Maintenance of the PRA Environment](#)" on page 16 and "[Perform Failover for Unplanned Maintenance of the PRA Environment](#)" on page 17, you can automate certain parts of these flows using the BeyondTrust API. This section provides some examples of how you can use the BeyondTrust failover API calls. You must modify the examples to fit your environment.



IMPORTANT!

Using the built-in failover in `/login` and the API failover commands together could result in conflict.

To use the BeyondTrust API, ensure that the **Enable XML API** option is checked on the `/login > Management > API Configuration` page.



For full instructions on using the BeyondTrust API, please see the [API Programmer's Guide](http://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/index.htm) at www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/index.htm.

Check B Series Appliance Health

To perform a health check on the B Series Appliance, use the API command `check_health`.



For more information, please see [API Command: check_health](http://www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/command/check_health.htm) at www.beyondtrust.com/docs/privileged-remote-access/how-to/integrations/api/command/check_health.htm.

You can use the XML responses `<last_data_sync_time>` and `<last_data_sync_status>` to make sure data syncs are occurring as expected.

If the XML response for the primary B Series Appliance includes `<success>1</success>`, then the B Series Appliance is functioning normally. You should not need to failover.

If the XML response for the primary B Series Appliance includes `<success>0</success>`, then you should take into account the time of the last successful health check. Also consider any `<error_message>` elements that are returned. You should put in place contingencies so that if the issue can be resolved in a reasonable time, then no action should be taken. However, if it is determined that failover is required, then you can use the API to switch failover roles.



Note: In addition to or alternative to using the API command above, you can use https://access.example.com/check_health to check the health of a B Series Appliance. This returns an HTTP status of 200 if the probe is successful and 500 (Server Error) if not. While you will see a simple human-readable message showing success or failure, no other data is exposed.

Set Failover Roles

To set the failover role on a B Series Appliance, use the API command `set_failover_role`. (In the API Programmer's Guide, see [API Command: set_failover_role](#) for full details.)

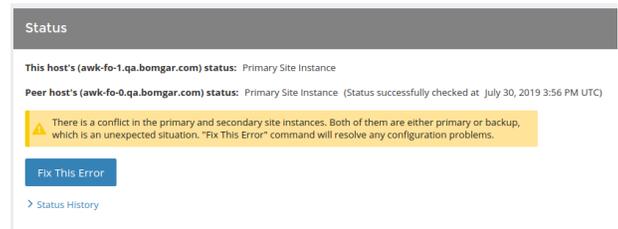
It is assumed that you will have in place systems for enabling/disabling a shared IP address if your two B Series Appliances are on the same network or else automatically performing a DNS swing or NAT swing.

Once the failover roles have successfully been changed, you should receive an XML response of `<success>`.

Resolve Conflicts in a PRA Failover Setup

If both B Series Appliances in failover take the same role at once (i.e., both primary or both backup), then the **Failover Status** page shows this error:

NOTE: There is a conflict in the primary and secondary site instances. Both of them are either primary or backup, which is an unexpected situation. "Fix This Error" command will resolve any configuration problems.



The screenshot shows a 'Status' section with the following content:

- This host's (awk-fo-1.qa.bomgar.com) status: Primary Site Instance
- Peer host's (awk-fo-0.qa.bomgar.com) status: Primary Site Instance (Status successfully checked at July 30, 2019 3:56 PM UTC)
- A yellow warning box with a triangle icon: "There is a conflict in the primary and secondary site instances. Both of them are either primary or backup, which is an unexpected situation. "Fix This Error" command will resolve any configuration problems."
- A blue button labeled "Fix This Error"
- A link labeled "> Status History"

This can happen when network connectivity is lost between the B Series Appliances and one takes on the role of the other. This can also occur automatically if **Failover Backup Settings** have **Enable Automatic Failover** enabled.

If both B Series Appliances are in the primary role and you know which B Series Appliance should be the backup, log into the **/login** admin web interface of this B Series Appliance, go to **Management > Failover**, and click **Become Backup**. Similarly, if both B Series Appliances are in the backup role and you know which B Series Appliance should be the primary, go to **Management > Failover** and click **Become Primary**. If you encounter errors during this process, log into the **/appliance** admin web interface of each B Series Appliance, go to **Support > Utilities**, and use the **TCP Connection Test** to determine if the B Series Appliances can connect over port 443. If not, check the **Networking > IP Configuration** tab and confirm the settings here are correct.

If you are not sure which B Series Appliance should be primary and which should be the backup B Series Appliance, you can click the **Fix This Error** button. Clicking this button automatically determines for you which role each B Series Appliance should have based on various criteria such as which B Series Appliance has the shared IP enabled or which has the IP to which the primary DNS address resolves. **Fix This Error** also implements the necessary role changes automatically.

Whether you resolve the error manually or automatically, the B Series Appliance which takes the backup role will have its configuration settings in **/login** overwritten by the primary B Series Appliance, with the exception of failover settings. Reports and recording data should be synchronized between both B Series Appliances so that all such data on either B Series Appliance will be extant on both B Series Appliances after synchronization is complete. When in doubt, download a configuration backup from **/login** using the **Download Backup** button located in **Management > Software Management**.

Replace a BeyondTrust Appliance B Series in a Failover Scenario

If your B Series Appliance should experience failure, BeyondTrust Technical Support is prepared to help you return to full functionality as quickly as possible. If you have already set up a failover B Series Appliance, you can continue working with minimal downtime. BeyondTrust Technical Support will work with you to determine if the offline B Series Appliance needs to be replaced. This quick guide gives you the steps to replace a B Series Appliance when you have it set up in a failover scenario.

This document is not comprehensive in its details. Rather, it is a tool to help you assemble the information you need to replace a B Series Appliance. You may need to refer to other BeyondTrust documents during this process. For your convenience, these documents are linked to below:

- [BeyondTrust Appliance B Series Hardware Installation Guide](#)
- [The BeyondTrust Appliance B Series in the Network](#)
- [BeyondTrust Appliance B Series Web Guide](#)
- [Failover Dynamics and Options With BeyondTrust](#)
- [Upgrade BeyondTrust PRA Hardware](#)

Install the New B Series Appliance



Note: Reference [BeyondTrust Appliance B Series Hardware Installation Guide](#) for installation details and [The BeyondTrust Appliance B Series in the Network](#) to determine where to set up your new B Series Appliance.



Please see [BeyondTrust Appliance B Series Web Interface](#) for further details regarding the `/appliance` interface.

1. Install the B Series Appliance and log in.
 - a. When you receive your new B Series Appliance, remove it from its packaging and connect the B Series Appliance to a switch.



Note: You may wish to save the packaging materials from the replacement B Series Appliance to return the defective B Series Appliance.

- b. Set an IP address of **169.254.1.4** on a workstation and connect to a port on the same switch as the B Series Appliance.
- c. Browse to **169.254.1.1/appliance** in a browser, and log in using the default username and password:
 - a. Username: **admin**
 - b. Password: **password**



Note: If **169.254.1.1** fails, try browsing to **169.254.1.2/appliance** or **169.254.1.3/appliance**.

2. Set up the IP configuration.
 - a. Browse to **Networking > IP Configuration**.
 - b. Enter the appropriate IP configuration settings for the network.
 - c. Save the changes and test connectivity over the new IP address.
3. Import SSL certificates.
 - a. Log into the **/appliance** web interface of the primary B Series Appliance, the B Series Appliance which is currently hosting all of your BeyondTrust support processes.
 - b. Browse to **Security > Certificates** and export the certificate chain that is assigned to the active IP address.
 - c. Log into the **/appliance** web interface of the new B Series Appliance.
 - d. Import the certificates from the primary B Series Appliance and assign the server certificate to the active IP address.

Restore the Failover Configuration



For detailed failover instructions, please see [Failover Dynamics and Options with BeyondTrust](#) and [Upgrade the BeyondTrust Software](#).

1. Register the B Series Appliance.
 - a. In the **/appliance** web interface of the new B Series Appliance, browse to the **Status > Basics** page and take a screenshot.
 - b. Email the screenshot of the **Status > Basics** page to your BeyondTrust Technical Support representative.
 - c. The BeyondTrust Technical Support team will build a new software package and email you installation instructions when it is ready.
2. Refer to the Failover Configuration section of the Upgrade Guide and follow either the synchronous or the asynchronous upgrade steps, depending on the preferred procedure.
 - a. Since the B Series Appliances will not begin in failover, skip the Break Failover Relationship step in the Upgrade Guide.
 - b. If you choose to upgrade asynchronously, you must begin by downloading a backup from the primary B Series Appliance's **/login > Management > Software Management** page. Then restore these settings to the new B Series Appliance.
 - c. Follow the rest of the failover procedure as outlined in the Upgrade Guide.



Note: If you have the original **.nss** software package that is installed on the primary B Series Appliance, you can install that software package on the backup B Series Appliance. You can then proceed to establish failover without installing the new software package mentioned above.

3. Notify your BeyondTrust Technical Support representative that the upgrade is complete. BeyondTrust Technical Support will then provide you with the return shipping label and instructions for the failed B Series Appliance.

Return the Defective B Series Appliance

1. Reset and shut down the defective B Series Appliance.
 - a. Log into the **/appliance** web interface of the defective B Series Appliance.
 - b. Browse to the **Status > Basics** page, and click **Reset Appliance to Factory Defaults**.
 - c. Wait for the reset to complete, and then click **Shut Down This Appliance**.
2. Use the shipping label and instructions from BeyondTrust Technical Support along with the packaging materials from the replacement B Series Appliance to return the defective B Series Appliance.

Appendix: PRA Administration Settings for Failover

Below is a list of all the administration settings available when setting up a backup B Series Appliance for failover. These are found in **/login > Management > Failover**. This information is also found in your [Administrative Guide](#).

Configuration

Setup a Failover Relationship

New Backup Site Connection Details

Host Name or IP Address

Enter the hostname or IP address of the B Series Appliance you wish to use as the backup in a failover relationship.

Port

Enter the TLS port allowing this primary B Series Appliance to connect to the backup B Series Appliance.

Reverse Connection Details To This Primary Site

Host Name or IP Address

Enter the hostname or IP address of this B Series Appliance, which you wish to use as the primary in a failover relationship.

Port

Enter the TLS port allowing the backup B Series Appliance to connect to this primary B Series Appliance.

Status

This host's status

View the hostname of this site, along with its status of primary site instance or backup site instance.

Peer host's status

View the hostname of this site, along with its status of primary site instance or backup site instance. Also view the date and time of the last status check.

Status History

Expand or collapse a table of status events that have occurred.

Primary or Backup Site Instance Status

Text confirms that you are either on the primary or backup site instance for your host site.

Sync Now

Manually force a data sync from the primary B Series Appliance to the backup B Series Appliance.

Become Backup/Primary

Switch roles with the peer B Series Appliance, essentially forcing a failover for planned maintenance or a known failover event.

Check this box to pull a data-sync from the site instance at **example.com** while becoming the backup/primary

If you want to synchronize data from the peer B Series Appliance prior to swapping roles, select this checkbox. If this option is selected, all users on the existing primary B Series Appliance will be disconnected during the data sync, and no other operations will be available until the swap is complete.

Check this box to become a backup even if the peer site instance at **example.com** cannot be contacted

On the primary site instance, you have the option to become the backup even if the peer B Series Appliance cannot be contacted. If this option is unchecked, failover will be canceled if both B Series Appliances cannot be kept in sync in terms of their failover roles (one primary and one backup).

For example, if you know the current backup B Series Appliance is online but cannot be reached by the primary due to a network connection issue, you may wish to check this option to make the primary the backup before the network connection is restored. In this example, you would also need to access the current backup and make it the primary.

Break Failover Relationships

Break the failover relationship, removing each B Series Appliance from its role as primary or backup.

Primary or Backup Site Instance Configuration

Shared IPs

Control the shared IP address the site instance uses in the event of a failover by selecting the checkbox for the failover IP address. If you change the relationship between the sites, the checked IP addresses will disable when a primary site becomes a backup, and will enable when a backup becomes a primary site. You should manually mirror the setting on the peer site, as the setting is not shared.

Backup Settings

The settings you configure here will be enabled only when the site instance you are configuring is in a backup role.

When on the primary site instance, select **Backup Settings** to expand or collapse the page displaying the configuration fields.

Enable Backup Operations

Enable or disable site backups.

Primary Site Instance Timeout

Set how long the primary site must be unreachable before failing over.

Automatic Data-Sync Interval

You can control the timing details of the automatic data-sync interval.

Data-Sync Bandwidth Limit

Set bandwidth parameters for data-sync.

Enable Automatic Failover

Quickly enable or disable automatic failover.

Network Connectivity Test IPs

Enter IP addresses for the backup site to check to determine whether the backup's inability to reach the primary is because the primary is offline or the backup has lost its network connection.