BOMGAR™

Configuring Failover

TC:8/31/2017

Table of Contents

Failover Dynamics and Options with Bomgar

Bomgar failover enables synchronization of data between two peer appliances, creating a simplified process for secure swap from a failed appliance. Two appliances host the same installed software package for a single public portal 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 appliances, the primary appliance, where all settings are configured. The backup appliance synchronizes with the primary, according to your settings configured in the appliance **/login** interface.

This document describes how to use a second Bomgar Appliance as a backup and failover device for a support site and how to switch operations to the backup appliance in a disaster recovery situation. There are three network configuration methods available with Bomgar 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 Bomgar Appliances have a peer relationship, so implementing the Shared IP failover configuration with automatic data synchronization enabled is recommended. Both 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 Bomgar API. The pros and cons of each option are covered in more detail later in the best practices.

Methods to Configure Failover Between Bomgar Appliances

Bomgar customer clients and representative consoles are built to attempt connection to the Bomgar Appliance at a specific address. In order to stop the clients from connecting to the normal primary Bomgar Appliance and instead connect to the backup Bomgar 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.

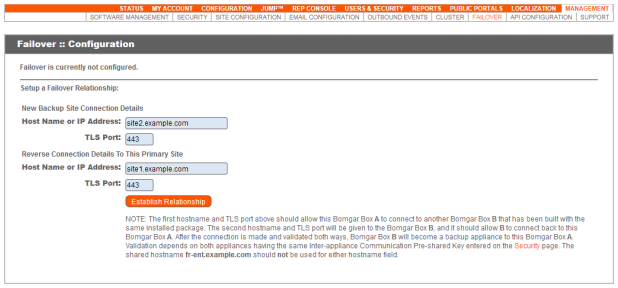
Method	Description	Pros	Cons
Shared IP	In this configuration, the hostname of the support site and IP address that is used to represent it remain constant. Both Bomgar Appliances share that IP in the **/appliance** interface, but only the Bomgar Appliance that is acting as primary has that IP enabled. The backup Bomgar Appliance will not use that IP unless it becomes primary.	No network equipment configuration change. Links and processes referencing your support site domain or IP address will be adjusted properly based on roles and will be served by the backup Bomgar Appliance. Once the backup appliance is redefined as the primary and the shared IP is enabled, the backup 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 Bomgar Appliances. If both 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 support site from the IP address for the primary Bomgar Appliance to the IP address of the backup Bomgar Appliance. Since DNS changes must propagate through your network, this change might require some time.	Links and processes referencing your support site domain do not need to be changed and will be served by the backup Bomgar 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 will take some time to propagate depending on the DNS record time to live. Until the new DNS entry is propagated, users and representatives may not be able to reach the site.
NAT Swing	Change the routing of requests for the support site at the NAT device from the primary Bomgar Appliance to the backup Bomgar Appliance.	Links and processes referencing your support site domain or IP address do not need to be changed and will be served by the backup Bomgar 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 Bomgar Appliance in a failover cluster fails and the backup appliance takes the primary role, any connection agents for the primary 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 (s) to the backup 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 appliances must have identical Inter-Appliance keys. Go to* ***/login > Management > Security*** *to verify the key for each appliance.*

Establish the Primary/Backup Failover Relationship Between Two Appliances

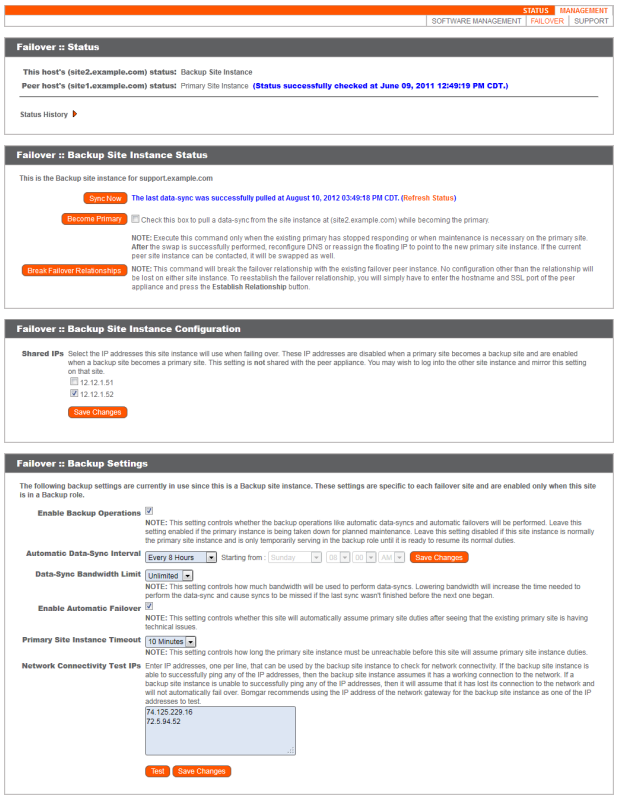
Bomgar failover enables synchronization of data between two appliances, creating a simplified, two-way process, regardless of which failover configuration you choose. Automatic synchronization of data can be enabled for any of the three supported failover configuration methods. To start automatically synchronizing site data between two appliances, you must first establish a trusted relationship between them. On the appliance you intend to be primary, 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.*

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, Bomgar 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.

You can disable synchronization, although this is recommended only in rare cases. See the best practices section "Establish Failover Settings for Primary and Backup Environments" on page 12.

If you want to break the relationship so that this appliance no longer backs up any primary appliances, click the **Break Failover Relationships** button. This will not remove configuration settings and session data already synchronized.

After failover is configured, the primary appliance can send an email alert if no backup 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 appliance's **/login > Management > Email Configuration** page. The next synchronization will copy the settings to the backup.

If the backup appliance determines that the primary appliance is down, it will send a series of emails to the Bomgar Appliance administrator notifying them of the failure and counting down the time until automatic failover will occur. The backup 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 appliance.

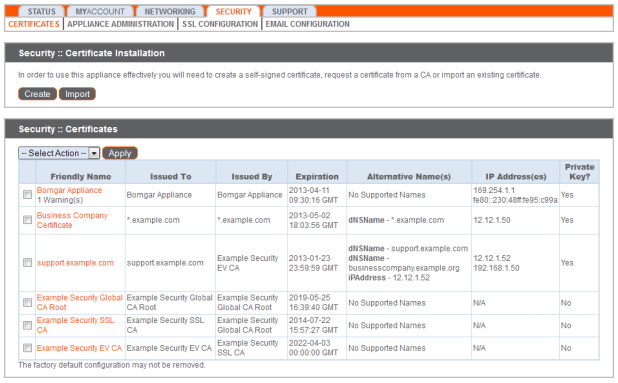
> ***Note:*** *In order to use Bomgar's built-in automatic failover, your two appliances must be on the same subnet. If you wish to use automatic failover with appliances on different networks, you must use the failover API.*

In the **Failover :: Backup Settings** section, set frequency of backup. Remember to set the backup frequency on the primary and backup since these settings are independent. See "Establish Failover Settings for Primary and Backup Environments" on page 12.

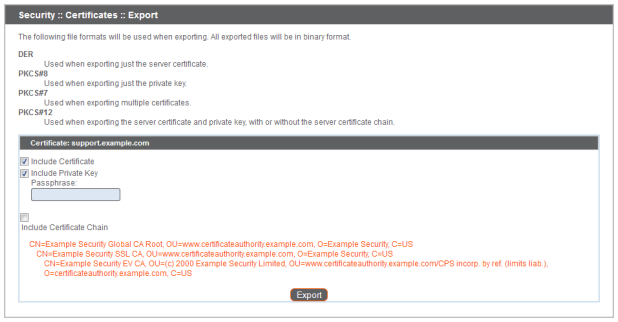
Replicate SSL Certificate Configuration on the Backup Appliance

The primary and backup appliances must have identically matching SSL certificates for failover to be successful. Otherwise, in the event of failover, the backup appliance will be unable to connect with any Bomgar clients, such as representative consoles, customer clients, and so forth.

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

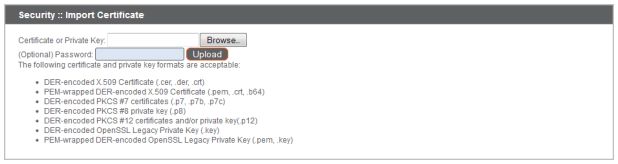


Export this certificate, along with its private key and certificate chain. The **Passphrase** field allows you to protect the certificate export with a passphrase. This is strongly recommended when exporting a private key.

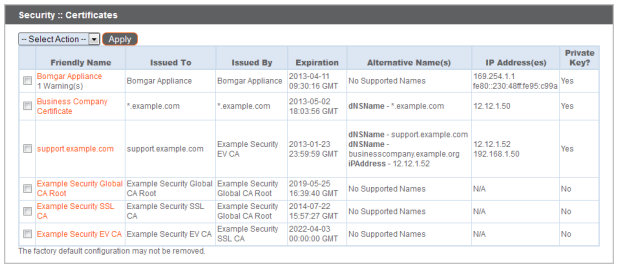


Log into the **/appliance** web interface of the backup appliance. Navigate to **Security > Certificates** and click the **Import** button.

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



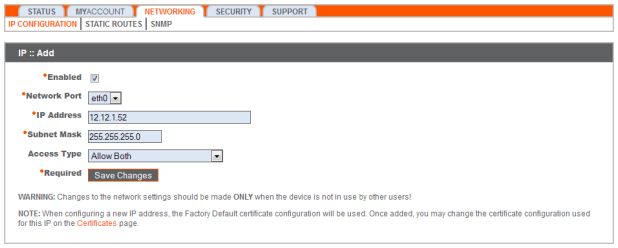
The imported certificate chain will now appear in the table of certificates. Click the name of the newly imported server certificate. The **Friendly Name** and/or an **Alternative Name** should match the URL of the appliance.



In the **IP Addresses** section, assign this certificate to the active IP address and, if applicable, to the shared IP address. Check the box for each IP address to which to assign this certificate, and then click **Save Configuration**.

Set Up a Shared IP Address for Failover Appliance Configuration

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



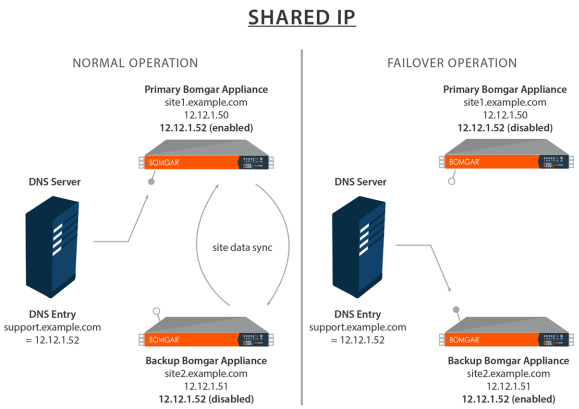
Configure Networking on the Appliances

Log into the **/appliance** administrative interface for your primary 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 unique hostname or IP address of the appliances cannot communicate, you will need to add a unique IP address to each appliance which is reachable from the other. Unlike the shared IP, the unique IP of each appliance should remain enabled at all times.

Log into the **/appliance** administrative interface for your backup 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 appliance following these same steps and disable the shared IP for the backup appliance to prevent an IP conflict on the network.



From the **/login** interface section **Failover :: Primary/Backup Site Instance Configuration**, you control via checkbox 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 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.

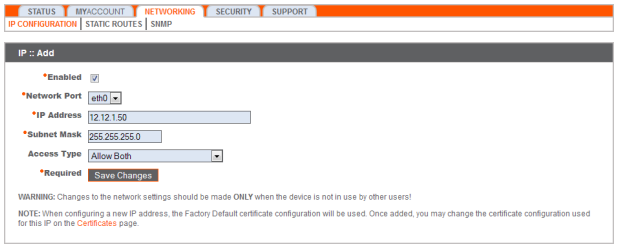
Because traffic from Bomgar Security Providers can flow out of any IP address on a Bomgar appliance, it is important to ensure the network firewall allows access from all Bomgar IP addresses on both appliances in failover to the necessary authentication systems. For example, when two appliances in shared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

Example Shared IP Configuration

	Primary Appliance	Backup Appliance
Definition	The appliance used during normal operations.	The appliance used during failover operations.
Hostname/IP Address	site1.example.com (12.12.1.50)	site2.example.com (12.12.1.51)
Site Name/Shared IP	support.example.com (12.12.1.52)	

Set Up DNS Swing for Failover Appliance Configuration

Change the DNS entry for your support site from the primary Bomgar Appliance IP address to the IP address of the backup appliance.



Configure Networking on the Appliances

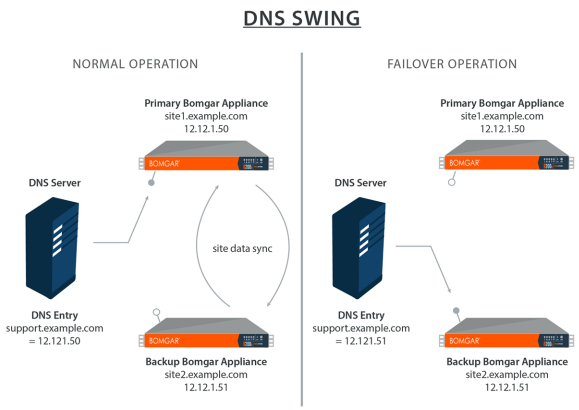
Log into the **/appliance** administrative interface for your primary appliance, accessible from either its unique hostname or IP address (e.g., **https://site1. example.com/appliance** or **https://12.12.1.50/appliance**).

Because DNS directs the support site domain, **support.example.com**, to this IP address, this is the primary appliance. All session activity will occur on this appliance.

Log into the **/appliance** administrative interface for your backup 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 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 appliance, Appliance B.



To failover, access the DNS controller and locate the DNS entry for your support site (e.g., **support.example.com**). Edit the entry to point to the backup IP. Click **Become Primary** from the backup appliance **Failover** page. Once the DNS entry has propagated, you can resume normal support activity. All requests to your support site will be served by the backup 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.

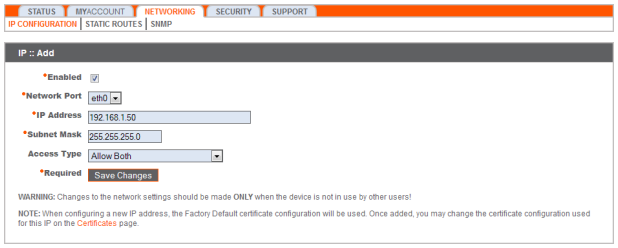
Example DNS Swing Configuration

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

Set Up NAT Swing for Failover Appliance Configuration

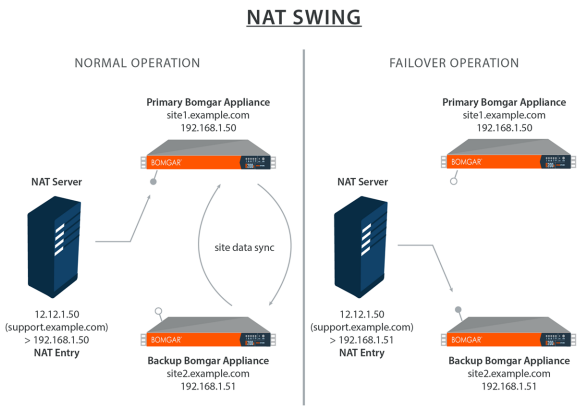
Configure Networking on the Appliances

Log into the **/appliance** administrative interface for your primary 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 support site domain, **support. example.com**, to this IP address, this is the primary appliance.



Log into the **/appliance** administrative interface for your backup 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 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 appliance, Appliance B.

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

Example NAT Method Configuration

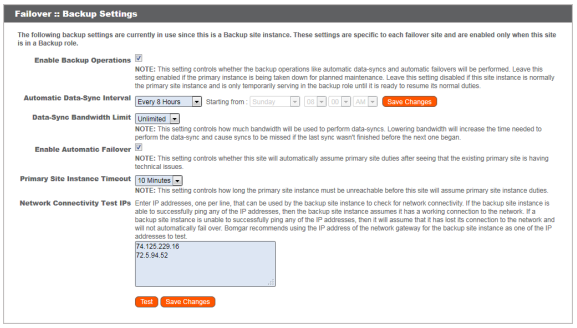
	Primary Appliance	Backup Appliance
Definition	The appliance used during normal operations.	The appliance used during failover operations.
Private IP Address	192.168.1.50	192.168.1.51
Hostname	site1.example.com	site2.example.com
Site Name	support.example.com (Translated to 192.168.1.50 or 192.168.1.51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

Establish Failover Settings for Primary and Backup 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 Bomgar Appliance as the normal primary and another 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.

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	*not applicable*	*user's choice*	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	*user's choice*	*user's choice*	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	*not applicable*	*user's choice*	Depends on user's choice for automatic failover.

Establish Failover for Planned Maintenance

IMPORTANT!

These flows depend on using the backup settings described in the topic "Establish Failover Settings for Primary and Backup Environments" on page 12.

This is the preferred method of maintenance. This method provides a path for ensuring that all settings, recordings, and data will be migrated from original primary to new primary, then back to the original primary. This method is also sufficient for upgrading 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 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 does occur. 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 appliance is now the primary 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 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** 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 Bomgar failover API. For details, see "Establish Failover Settings for Primary and Backup Environments" on page 12.*

Establish Failover for Unplanned Maintenance

IMPORTANT!

These flows depend on using the backup settings described in the topic "Establish Failover Settings for Primary and Backup Environments" on page 12.

*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 "Establish Failover for Planned Maintenance" on page 13. 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 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.
3. If necessary, swing DNS or perform a NAT swing after you see that the roles swap.
4. Perform maintenance on the primary.
5. When the primary is ready to resume its normal duties, repeat steps 1-3, 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

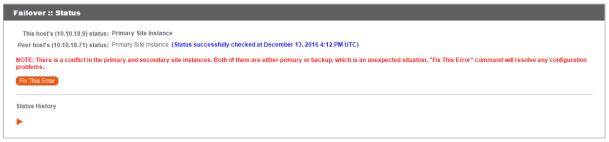
1. Go to backup failover page at **/login > Management > Failover**.
2. Click **Become Primary** and wait.
    - This site will be missing any session data and recordings and **/login** settings changes since the last data-sync.
    - Care should be taken to not make changes to settings in **/login** while the backup is acting as primary. Any changes that are made will be lost when the site is made the backup again. Any support session recordings and data will not be lost, however.
3. If necessary, swing DNS or perform a 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.

Note: *Instead of going to the* ***/login*** *interface to change roles, you can use the Bomgar failover API. For details, see* *"Establish Failover Settings for Primary and Backup Environments" on page 12*.

Resolving Conflicts

If both 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.



This can happen when network connectivity is lost between the 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 appliances are in the primary role and you know which appliance should be the backup, log into the **/login** admin web interface of this appliance, go to **Management > Failover**, and click **Become Backup**. Similarly, if both appliances are in the backup role and you know which 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 appliance, go to **Support > Utilities**, and use the **TCP Connection Test** to determine if the 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 appliance should be primary and which should be the backup appliance, you can click the **Fix This Error** button. Clicking this button automatically determines for you which role each appliance should have based on various criteria such as which 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 appliance which takes the backup role will have its configuration settings in **/login** overwritten by the primary appliance, with the exception of failover settings. Reports and recording data should be synchronized between both appliances so that all such data on either appliance will be extant on both appliances after synchronization is complete. When in doubt, download a configuration backup from **/login** using the **Download Backup** button located in **Management > Software Management**.

Use the Bomgar API to Check Appliance Health and Establish Failover

The Bomgar API includes calls to manage and automate failover. Following the basic flows set forth in Establish Failover for Planned Maintenance "Establish Failover for Planned Maintenance" on page 13 and Establish Failover for Unplanned Maintenance "Establish Failover for Unplanned Maintenance" on page 14, you can automate certain parts of these flows using the Bomgar API. This section provides some examples of how you can use the Bomgar failover API calls. You will need to 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 Bomgar API, ensure that the **Enable XML API** option is checked on the **/login > Management > API Configuration** page.

For full instructions on using the Bomgar API, see www.bomgar.com/docs/remote-support/how-to/integrations/api/index.htm

Check Appliance Health

To perform a health check on the Bomgar Appliance, use the API command **check_health**. (In the API Programmer's Guide, see API Command: check_health for full details.)

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 appliance includes `<success>1</success>`, then the appliance is functioning normally. You should not need to failover.

If the XML response for the primary 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://support.example.com/check_health** to check the health of an 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 Bomgar 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 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>`.

Appendix: Administration Settings

Below is a list of all the administration settings available when setting up a backup appliance for Failover. These are found in **/login > Management > Failover**. This information is also found in your Administrative Guide.

Failover :: Configuration

New Backup Site Connection Details: Host Name or IP Address

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

TLS Port

Enter the TLS port allowing this primary appliance to connect to the backup appliance.

Reverse Connection Details To This Primary Site: Host Name or IP Address

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

TLS Port

Enter the TLS port allowing the backup appliance to connect to this primary appliance.

Failover :: 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.

Failover :: 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 appliance to the backup appliance.

Become Backup/Primary

Switch roles with the peer 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 appliance prior to swapping roles, select this checkbox. If this option is selected, all users on the existing primary 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 appliance cannot be contacted. If this option is unchecked, failover will be canceled if both 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 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 appliance from its role as primary or backup.

Failover :: 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.

Failover :: 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.

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.

Primary Site Instance Timeout

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

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.