BOMGAR™

Configuring Failover

in Bomgar 10.6

TC:3/8/2011

Thank you for using Bomgar.

At Bomgar, customer service is a top priority. Help us provide you with excellent service. If you have any feedback, including any manual errors or omissions, please send an email to feedback@bomgar.com.

Configuring Failover

Table of Contents

Failover Dynamics 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. 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. The pros and cons of each option are covered in more detail later in our best practices.

Configuring Failover Between Bomgar Appliances

Failover Methods and Steps

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

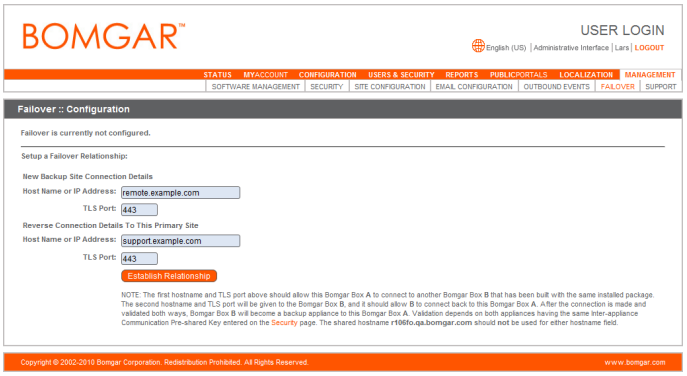
Methods of Configuring Failover Between Bomgar Appliances

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 Box and instead connect to the backup Bomgar Box, 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 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 the **/login** interface Failover page 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 normal 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 normal 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.

Establish the Primary/Backup Relationship

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 the **Failover** page under the **Management** tab of the /login administrative interface.



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

Establishing the relationship between the two appliances occurs on the **Failover::Configuration** 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 may 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.

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.

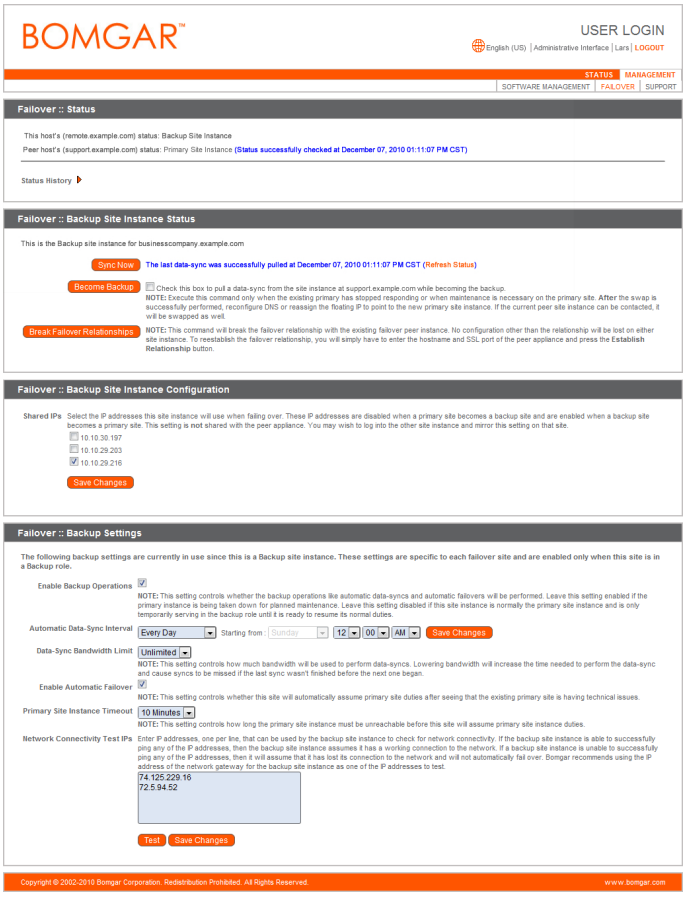
You can disable synchronization, although this is recommended only in rare cases. See our best practices section "Failover Setup Best Practices" on page 12

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.

You can configure the primary appliance to send an email alert if no backup appliance pulls its data for a given length of time so that you will be aware if relationships have been disrupted. Configure automatic email notifications in the **/login** interface, **Management** tab, **Email Configuration** page, on the primary site. 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 her 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.

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 "Failover Setup Best Practices" on page 12.



Shared IP Failover Configuration Setup

In this configuration, the hostname of the support site and 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.

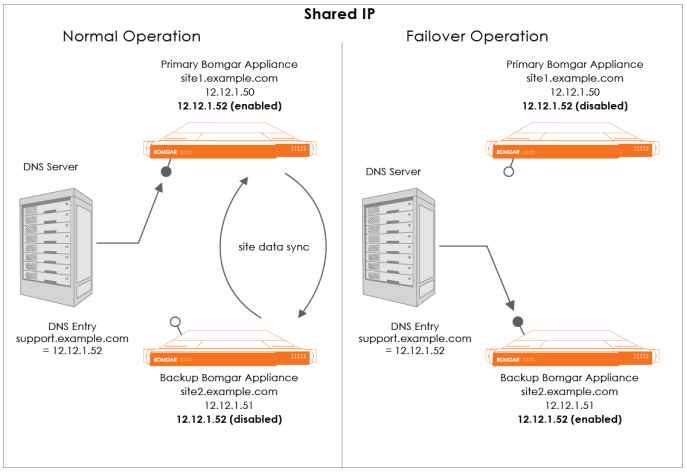
Configure Networking on the Appliances

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 **IP Configuration** page under the **Networking** tab. 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 keep the IP **Enabled**.

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**).

For the backup, go to the **IP Configuration** page under the **Networking** tab. 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 the IP addresses via checkbox which the site instance uses if a failover event occurs. This must be set on both the primary and the backup appliances. Now the primary site in the failover relationship will enable the IP you selected. The backup site will disable that IP when the roles change.

Example Shared IP Configuration

	Primary Appliance	Backup Appliance
Definition	The Bomgar Box used during normal operations.	The Bomgar Box 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)	

DNS Swing Failover Configuration Setup

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**).

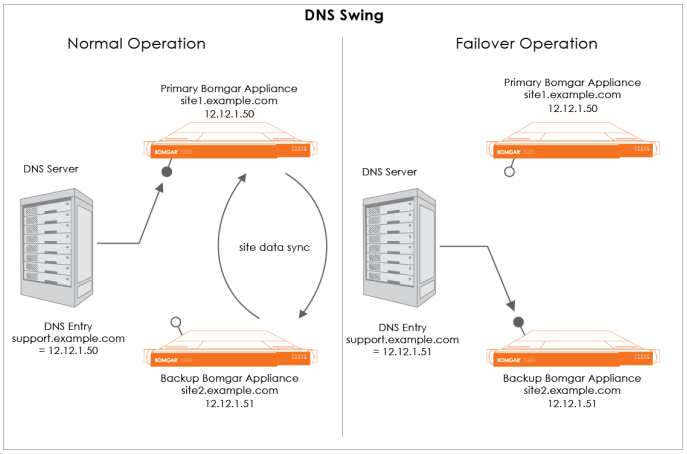
Because DNS directs the support site domain, **support.example.com**, to this IP address, this is the primary appliance. All session activity will occur on this appliance.

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**).

Go to the **IP Configuration** page under the **Networking** tab. 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, Box 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, Box 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. 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. Click **Become Primary** from the backup appliance Failover page.



Example DNS Swing Configuration

	Primary Appliance	Backup Appliance
Definition	The Bomgar Box used during normal operations.	The Bomgar Box 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)	

NAT Swing Failover Configuration Setup

Configure Networking on the Appliances

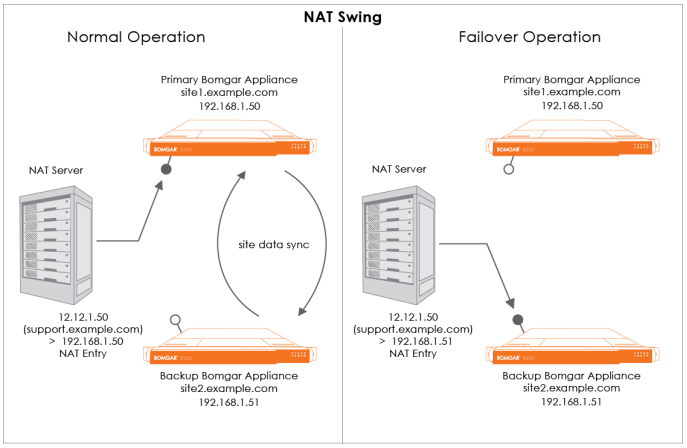
Log into the **/appliance** administrative interface for your primary appliance, accessible from either its unique hostname or IP address (e.g., **https:// site1. example.com/appliance** or **https://192.168.1.50/appliance**).

Go to the **IP Configuration** page under the **Networking** tab. 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 **IP Configuration** page under the **Networking** tab. 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, Box 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, Box 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. As soon as the 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 Bomgar Box used during normal operations.	The Bomgar Box 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)	

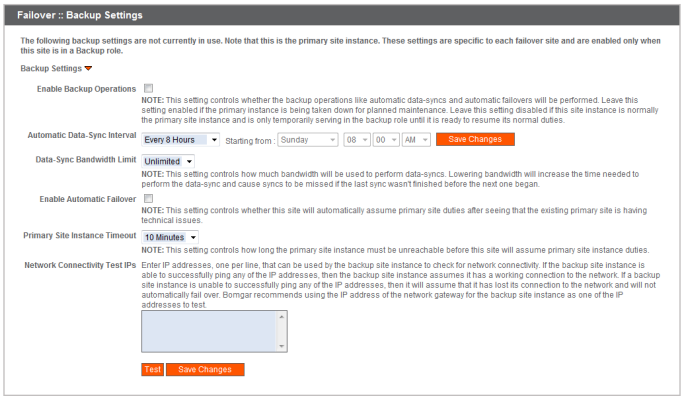
Failover Setup Best Practices

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

Note: Deviation from these best practices may result in data loss.

Establishing Failover Settings for Primary and Backup Environments

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 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 and 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 to not overlap the next time it's 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.

Establishing Failover for Planned Maintenance

IMPORTANT: These flows depend on using the backup settings described in the topic, "Failover Setup Best Practices" 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 back to the original primary. This method is also sufficient for upgrading appliances as well.

1. Go to the primary or backup failover page.
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 box and won't 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.

    - 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 was 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 primary.

Establishing Failover for Unplanned Maintenance

IMPORTANT: These flows depend on using the Bomgar best practices backup settings in the topic, "Failover Setup Best Practices" 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 "Establishing 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.

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

Unplanned Maintenance with No Recent Change in /login

1. Go to backup failover page.
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.
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, though.
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. Do a data-sync.