

# Bomgar Remote Support Admin Alerts

Several events trigger an email notification sent to the addresses specified at **/appliance > Security > Email Configuration**.

- Test email when configuring the setting
- Any RAID events that occur on the B300, such as RAID degradation or disk failure
- Any changes made to the syslog settings
- SSL certificates which are expiring in 90, 60, 30, 15, or 10 days, and then daily until expiration.

Also, several events trigger an email notification sent to the addresses specified at **/login > Management > Email Configuration**.

- Test email when configuring the setting
- Daily notice that communication is functioning properly
- Outbound event failure notifications
- Failover event notifications such as DNS issues or software version mismatches

Some of the notifications that may be sent are listed below.

## SSL Certificate Expiration

This email is to notify you that one or more in-use SSL Certificates are in danger of expiring on a Bomgar Box at the address:

example

The certificates nearing expiration are:

\*.support.example.com

Expiring in: 60 days

## Communication Notice

This notice is being sent only to inform you that alert communication is working properly. If this notice stops being received daily, then communication is not working, and you will not receive notification if any important alerts are triggered.

## Outbound Event Failure

A failure occurred while posting an outbound event to the recipient named: %RECIPIENT%

You will receive another notification in about %TIME% if the problem is not resolved.

## Hostname Resolves Incorrectly

The hostname (%HOST%) does not resolve to the site instance on this appliance. This alert is sent when a site instance is marked as the primary but the hostname for which the site is built (%HOST%) does not resolve to the site instance on this appliance.

The hostname may currently be pointed to the wrong location. DNS may be incorrectly configured for this appliance. The DNS servers may be unreachable or malfunctioning. Or perhaps the hostname is still cached to an old location in the DNS servers for which this appliance is configured.

### Backup Site Is Disabled

The operations normally performed by the backup site instance became disabled through the web interface. These operations are necessary for detecting that the primary site instance is experiencing issues. While disabling this setting is acceptable for planned outages and maintenance of the primary site instance, it is not intended to be disabled for long periods of time. If the primary site instance is functioning normally, please log into the backup site instance and restart the backup site operations. If the primary site instance is down and will not be returning to service soon, log into the backup site instance and select **Become Primary** in the failover section. The backup takes over the primary site duties.

***Note:** If the appliance sending this message is normally the primary site instance but became a backup instance due to a maintenance issue, then this message may be ignored until the original primary site instance is ready to resume its normal duties and the roles are switched again.*

### Probe of Peer Failed

A test of the peer site instance failed.

This alert is sent when the peer site instance appears to be malfunctioning. If the peer site instance is serving as the primary site, it may be necessary to fail service over to this site instance.

After verifying that the site instance currently pointed to by %HOST% is in fact not functioning properly and that it cannot quickly be resolved, you may use the administrative interface on this backup site instance to fail service over.

### Self-Probe of Backup Failed

A self test of a backup site instance for %HOST% failed.

This alert is sent when a backup site instance appears to itself to be malfunctioning.

### Software Versions Do Not Match

A test of the site instance at %HOST% revealed that it is of a different version than this backup site instance.

This may occur expectedly when software is being upgraded, but you are being alerted in case this is unexpected.

### No Data Syncs Are Being Performed

No data sync was performed in the configured time. It may be that the one of site instances is not functioning properly or that synchronizations were manually disabled on the backup site instance(s). This may occur predictably when software is being upgraded and the site instances are not running the same software version, but you are being alerted in case this is unexpected.

### Shared IP Not Being Shared Correctly

While checking the status of the IP addresses shared between the backup and the primary appliance, it was discovered that the state of a shared IP on one of the boxes is incorrect. If the IP is down and should be up, then this error means that the primary appliance could not claim the IP address as its own. If it is up and should be down, then a backup system is not releasing the IP address for some reason. Please check the status of these systems.

### Auto-Failover Shared IP Is Not an IP for the Appliance

One of the IP addresses listed as a shared IP in the automatic failover configuration is not listed as an IP address for the Bomgar Appliance under %HOST%/appliance. Please correct this error.

### Backup Site Could Not Ping Any Host

After successive attempts to probe the primary site instance (%HOST%) failed, the backup site instance attempted to ping the test IPs defined in the automatic failover configuration. All of these IPs were unreachable, so the backup site instance will assume it is down and not take over as the primary site instance.

If you are seeing this message, then there is possibly a wider network problem or just a malformed hostname in the test IPs field. Please check your configuration.

### Backup Site Could Not Ping Some Hosts

The backup site instance attempted to ping the test IPs defined in the automatic failover configuration as a routine test. The IPs listed below were unreachable. While only one IP from the list must be reachable in order for automatic failover to occur, it is possible that the IPs listed below are the only IPs listed.

If you are seeing this message, then there is possibly a wider network problem or just a malformed hostname in the test IPs field. Please check your configuration.

### Backup Site Has Performed Automatic Failover

After successive attempts to probe the primary site instance (%HOST%) failed, the backup site attempted to test its own connectivity to the network. These tests succeeded, so the backup site instance is now attempting to take over as the primary site. You should check the support site to ensure it is responding properly. The reason the probe of the primary site instance failed is shown. Once the primary site instance is back online, you may swap back to the original primary appliance if it is available.

### Primary Site on Probation

The backup site instance performed a probe on the primary site instance to determine if it was still operational. This probe failed, so the primary site instance is being placed on probation. These probes will continue for the amount of time specified in the automatic failover configuration. If the probes continue to fail, an automatic failover will occur.

## IMPORTANT!

*If you do not want an automatic failover to occur, please check the status of the primary site instance now or disable the backup site instance.*

### Primary Site off Probation

The probes of the primary site instance are now succeeding, so the primary site is off probation. The countdown time for auto-failover has been reset.

### Error Becoming Primary Site Instance

There was an error while becoming the primary site instance. Please try again later.

### Error Becoming Backup Site Instance

There was an error while becoming the backup site instance. Please try again later.

### Failover Status Codes

The Failover Status Code table documents the failover status codes that may be reported within the log visible on the website. This is confidential, internal-use only information.

New versions should not renumber, but only add new status codes.

## Failover Status Codes

### Data Sync Status Codes

Status Code	Description	Situation	Possible Causes
0	No error	Used for any normal log entry.	Functioning within parameters.
300	Appliances not ready to data-sync	The initial handshake showed that at least one appliance is not ready to data-sync.	Site install in progress; one side thinks a data-sync is already in progress.
301	Connection lost	The failover script received a SIGPIPE while trying to write to the socket. This happens when a write occurs on a socket and the other end has since disconnected. This could happen at any time during the sync operation.	Network interruption; Other end lost power/rebooted; etc.
302	File system error	The failover script was unable to create either the directory used to hold files that are being sent to the other appliance or the directory that will receive files from the other appliance. Both are created in <code>ingrediRoot/data/tmp</code>	Bug with file permissions; no disk space; (rarely returned).
303	Exchange algorithm error	Each appliance compares the DSIDs and LSIDs from the other side in order in order to determine what the other side needs to be sent. Something went wrong and the appliances were unable to sync at the end of that process.	Bug/Crash in algorithm; one side timed out (>1 hour) waiting for the other side to say it was finished.
304	Exchange filestores error	Sanity check after syncing the big filesystems (recordings, canned_scripts, etc.) failed.	Probably a qsync error (312) on the remote side caused this. Check the other appliance to see if it has a more specific error message.
305	Creating Backup failed	The primary calls <code>create_backup_file</code> to make a backup file to send to the backup. That script failed.	Bug in backup scripts; file permission problem; disk space problem.
306	Restoring backup failed	The backup calls <code>restore_backup_file</code> to load the backup file from the primary. That script failed.	Bug in backup scripts; file permission problem; disk space problem.
307	Loading database data failed	Each appliance loads the database entries that it was sent during the exchange. Loading the data apparently failed and this sanity check caught it.	Could be a database problem (311) on the remote side; file permission problem; disk space problem.
308	Add relationship error	Something was wrong with the slac handshake, and the appliance doesn't have all the information it needs to set up a relationship.	Should never happen, but could be a bug in slac; could be a rogue appliance or an appliance running a different version with different handshake.

Status Code	Description	Situation	Possible Causes
309	Probe failed	The probe of the remote appliance was unsuccessful.	Different versions; different inter-appliance passwords; failed to communicate to main service; the database service is down; appliance is overloaded; etc.
310	Role Setting failed	The setting of a role on the appliance failed.	Likely a bug or a misconfiguration of the shared IPs. Check the log of the appliance whose role is being set, for more information.
311	SQL error	Either the database data import utility failed importing new data or the database data export utility failed to export the new data out to file.	The result of running each command is in <code>failover_core.log</code> , so it will tell what went wrong.
312	qsync error	The qsync utility reported an error syncing some directory between the two appliances.	The result of running each qsync command is in <code>failover_core.log</code> , so it will tell what went wrong.