Replacing a Failed System

https://campus.barracuda.com/doc/41101833/

Before you replace your Barracuda Email Security Gateway, use the tools provided on the **ADVANCED > Troubleshooting** page to try to resolve the problem, or call Barracuda Networks Technical Support.

Barracuda Instant Replacement Service

In the event that a Barracuda Email Security Gateway fails and you cannot resolve the issue, customers that have purchased the Instant Replacement (IR) service can call Barracuda Networks Technical Support and arrange for a new unit to be shipped out within 24 hours. Whether or not you have subscribed to IR, if you plan to send your appliance back to Barracuda, do the following FIRST:

1. Create a backup file set.
2. Optional: You may want to create a screenshot of some or all of the web interface pages to have visual backup of your system settings. In case the backup/restore fails, this is a benefit for more complex configurations, providing for easy setup of the new appliance.
3. If the appliance is clustered, set it to *Standby* mode, remove the Shared Secret, and then delete the appliance from each of the other appliance **ADVANCED > Clustering** pages in the cluster. Now you should only see the local appliance's serial number listed on the **ADVANCED > Clustering** page of the unit you are returning.

After receiving the new appliance, ship the old Barracuda Email Security Gateway back to Barracuda Networks at the address below with an RMA number marked clearly on the package. Barracuda Networks Technical Support can provide details on the best way to return the unit.

Barracuda Networks

Attn: RMA # <your RMA number>
3175 S. Winchester Blvd
Campbell, CA 95008

Installing and Setting Up the New Appliance

1. Follow instructions in the Barracuda Email Security Gateway Quick Start Guide, which you can view or download from the Getting Started page.
2. Be sure the new appliance firmware version is equal to or greater than the firmware version of the failed unit. You may be able to edit or unzip the backup file you made (see step 1 above) and see the firmware version.

3. Once the new appliance has been brought to a stable point and is functional, it's time to either manually configure using the web interface or restore the backup(s). See How to Back Up and Restore System Information. After restoring the backup, you will be prompted to reboot to apply the changes.
4. If the new appliance is replacing one that was in a cluster, add this new unit to the cluster per instructions in How to Cluster the Barracuda Email Security Gateway, or click **Help** on the **ADVANCED > Clustering** page.
5. If you are using Barracuda Cloud Control, see How to Set Up Barracuda Cloud Control to add the new unit to your BCC account.

For information on returned device management, refer to How Barracuda Networks Manages Returned Device Drives.