
Replacing a Failed System

<https://campus.barracuda.com/doc/91985967/>

Replacing a Failed System

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

Using the Barracuda Instant Replacement Service

In the event that a Barracuda Web Security Gateway fails and you cannot resolve the issue, if you have purchased the Instant Replacement service, call [Barracuda Networks Technical Support](#) and arrange for a new unit to be shipped out within 24 hours. If you plan to send your appliance back to Barracuda Networks, do the following FIRST:

1. Create a backup file set. See [How to Back Up and Restore Your System Configuration](#).
2. Make a note of the firmware version of the failed appliance.
3. 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.
4. 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 > Linked Management** pages in the cluster. Now you should only see the local appliance's serial number listed on the **ADVANCED > Linked Management** page of the unit you are returning.

Note that no data is transferable from the 6 months of logged archives saved on the Barracuda Web Security Gateway (although you will have this data if you have been sending it to a syslog server).

After receiving the new appliance, ship the old Barracuda Web 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, Inc.

Attn: RMA # <your RMA number>

**5225 Hellyer Avenue
San Jose, CA 95138**

Installing and Setting Up the New Appliance

1. Follow instructions in the Barracuda Web Security Gateway Quick Start Guide, which you can view or download from the [Getting Started](#) page. Note that the **Default Gateway**, configured on the **Basic > IP Configuration** page of the web interface, is the IP address of the next outbound hop from the device. The Barracuda Web Security Gateway sends all egress traffic to the default gateway via the WAN port. For forward proxy deployment, use the same Default Gateway that is used by hosts on the network. The firewall must be on the same subnet as the Barracuda Web Security Gateway.
2. Be sure the new appliance firmware version is equal to or greater than the firmware version of the failed unit. You can see the firmware version in the backup filename.
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 Your System Configuration](#). 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 (click **Help**) on the **ADVANCED > Linked Management** 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.
6. If you are using LDAP with the Barracuda DC Agent, see the **Configure the Barracuda DC Agent** section of the article [How to Get and Configure the Barracuda DC Agent](#) so you can notify the agent of the IP address of the new appliance.

For information on returned device management, refer to [How Barracuda Networks Manages Returned Device Drives](#).

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.