Maintenance

https://campus.barracuda.com/doc/3866731/

Backing up and Restoring Your System

You should back up your system on a regular basis in case you need to restore this information on a replacement Barracuda Email Security Gateway or in the event that your current system data becomes corrupt. Please see How to Back Up and Restore System Information and make this a part of your routine maintenance plan.

Updating the Firmware on your Barracuda Email Security Gateway

This should be one of the steps the administrator performs in the initial installation of the Barracuda Email Security Gateway. Use the **ADVANCED > Firmware Update** page to manually update the firmware version of the system or revert to a previous version. The only time you should revert back to an old firmware version is if you recently downloaded a new version that is causing unexpected problems. In this case, call Barracuda Networks Technical Support before reverting back to a previous firmware version.

Updating the Firmware of Clustered Systems

If a system is part of a cluster, we recommend changing the system's **Mode** in the **Clustered Systems** section of the **ADVANCED > Clustering** page to *Standby* before you upgrade its firmware, and then repeat this process on each system in the cluster. Once the firmware on each system has been upgraded, you can then change the mode on each system back to *Active*.

Changing a clustered system to *Standby* mode before upgrading prevents a system on a more recent firmware version from trying to synchronize its configuration with a system on an earlier firmware version. If you have the latest firmware version already installed, the **Download Now** button on the **ADVANCED > Firmware Update** page is disabled.

Applying a new firmware version results in a temporary loss of service. For this reason, you should apply new firmware versions during non-busy hours. Before upgrading, BE SURE TO TAKE THE Barracuda Email Security Gateway OFFLINE. This will ensure that the inbound mail queue is emptied and all messages are scanned before the upgrade process begins. **DO NOT MANUALLY REBOOT YOUR SYSTEM at any time during an upgrade, unless otherwise**

instructed by Barracuda Networks Technical Support.

The current firmware version shows in the top section of the page, with the latest *General Release* version of the firmware shown below in the **Firmware Download** section. To download the latest firmware version, click the **Download Now** button. The web interface will display download progress. When the firmware download is complete, click the **Apply Now** button. The Barracuda Email Security Gateway will reboot and you will need to log in again to the web interface.

Updating the Definitions from Energize Updates

This should be one of the steps the administrator performs in the initial installation of the Barracuda Email Security Gateway. The **ADVANCED > Energize Updates** page allows you to manually update the Virus, Policy, and Security Definitions used on your Barracuda Email Security Gateway or to have them updated automatically. Barracuda Networks recommends that the **Automatic Updates** option be set to *On* for all three types of definitions so that your Barracuda Email Security Gateway receives the latest rules as soon as they are made available by Barracuda Networks.

Important: If you are using the Barracuda Exchange Anti-Virus Add-in with your MS Exchange mail server, make SURE to set the **Automatic Updates** option to *On* in the **Virus Definition Updates** section of the **ADVANCED > Energize Updates** page. This is necessary to ensure that the add-in receives constant updates of virus signatures from the Barracuda Email Security Gateway.

System Uptime, Reloading, Restarting, and Shutting Down the System

The System Management/Shutdown section on the **BASIC > Administration** page allows you to shut down, restart, and reload system configuration on the Barracuda Email Security Gateway. You can also take the system offline if necessary, which is recommended whenever you do a Firmware Update. A unit in Offline (Maintenance) mode will stop accepting incoming mail until it is put back online.

System uptime is displayed at the top of the System Management section of the page in days, hours and minutes.

Shutting down the system powers off the unit. Restarting the system reboots the unit. Reloading the system re-applies the system configuration.

You can also perform a hard reset of the Barracuda Email Security Gateway by pressing the **RESET** button on the front panel of the system. Caution should be used when pressing the reset button,

however, since doing so while the Barracuda Email Security Gateway is in the midst of a configuration update or other task can result in inadvertent corruption of the system.

When you press the Reset button, the following actions occur:

- Reboots the system
- Resets the IP address if held down for 5 seconds or more. Do not press and hold the **RESET** button for longer than a few seconds – doing so changes the IP address of the system. Pushing and holding the **RESET** button for:
  - 5 seconds changes the IP address to the default of 192.168.200.200
  - 8 seconds changes the IP address to 192.168.1.200
  - 12 seconds changes the IP address to 10.1.1.200

Bayesian Database Reset

If you have **Use Bayesian** set to *Yes* on the **BASIC > Spam Checking** page, read this section. For more information about how Bayesian Analysis works, please see Bayesian Analysis Inbound.

- For a global Bayesian database, the administrator should periodically (every 6 months or so) clear it out by resetting it from the **BASIC > Spam Checking** page, then, from the **BASIC > Message Log** page, marking at least 200 messages as either *Spam* or *Not spam* using the buttons on the page. Bayesian filtering will NOT take effect until 200 or more of each spam and not-spam messages are marked as such.
- If per-user Bayesian is enabled (from the **USERS > User Features** page), each user should reset their own Bayesian database and follow up with marking 200 or more messages as spam or not spam, either in their quarantine inbox (**QUARANTINE > Quarantine Inbox** page) or from their regular email client if they have installed either the MS Outlook add-in or Lotus add-in. For more information about mail client add-ins, see Barracuda Outlook Add-In Overview 6 and Above and the **USERS > User Features** page in the web interface.