Troubleshooting

https://campus.barracuda.com/doc/6160413/

The Barracuda Networks backup process does NOT back up your SSL certificates, therefore, if you do not manually back up SSL certificates, you must redeploy using a new certificate.

Basic Troubleshooting Tools

The **ADVANCED > Troubleshooting** page provides various tools that help troubleshoot network connectivity issues that may be impacting the performance of your Barracuda Web Security Gateway.

Examples include:

- Test the connection between the Barracuda Web Security Gateway to Barracuda Central to make sure it can successfully download the latest virus and spyware definitions.
- Open a support tunnel to allow Barracuda Support to connect with your appliance and troubleshoot any issues.
- Ping or telnet to devices from the Barracuda system
- Perform a traceroute from the Barracuda system to a destination server
- Run a packet capture
- Test what action the Barracuda Web Security Gateway would take with particular URLs, domains, MIME types, etc. based on block/accept polices and exceptions you create. See Policy Rule Checking.
- Barracuda recommends using the AUX port for management of the Barracuda Web Security Gateway, while the LAN/WAN ports are used for user data and web traffic.The Auxiliary (AUX) port for management of the Barracuda Web Security Gateway is available in all deployment modes.

This video describes how to use the troubleshooting tools available in the Barracuda Web Security Gateway.

LDAP Issues

If your LDAP server is slow in responding to search requests, increase the **LDAP Server Timeout** timeout value on the **USERS/GROUPS > Configuration** page. Default is 30 seconds.

Connect to Barracuda Support Servers

In the **Support Diagnostics** section of the **ADVANCED > Troubleshooting** page, you can initiate a connection between your Barracuda Web Security Gateway and the Barracuda Support, which allows technical support engineers to troubleshoot any issues you may be experiencing. See How to Open a Support Tunnel for details.

Rebooting the System in Recovery Mode

If your Barracuda Web Security Gateway experiences a serious issue that impacts its core functionality, you can use diagnostic and recovery tools that are available at the reboot menu to return your system to an operational state.

Before you use the diagnostic and recovery tools, do the following:

- Use the built-in troubleshooting tools on the **ADVANCED > Troubleshooting** page to help diagnose the problem.
- Perform a system restore from the last known good backup file.
- Contact Barracuda Networks Technical Support for additional troubleshooting tips.

As a last resort, you can reboot your Barracuda Web Security Gateway and run a memory test or perform a complete system recovery, as described in this section.

To perform a system recovery or hardware (memory) test:

1. Connect a monitor and keyboard directly to your Barracuda Web Security Gateway.
2. Reboot the system by doing one of the following:
   - In the web interface: Go to the **BASIC > Administration** page, navigate to the **System Reload/Shutdown** section, and click **Restart**.
   - At the front panel of the Barracuda Web Security Gateway: Press the **Power** button on the front panel to turn off the system, and then press the **Power** button again to turn the system on.
   The splash screen displays with the following three boot options:

```
Barracuda
Recovery
Hardware_Test
```

3. Use your keyboard to select the desired boot option, and press the **Enter** key.
   You must select the boot option within three seconds after the splash screen appears. If you do not select an option within three seconds, the Barracuda Web Security Gateway starts up in *Normal* mode (first option).
   For a description of each boot option, refer to **Reboot Options** below.

IMPORTANT!

After you start a hardware test, *the test will continue to run until you stop it manually.* To stop a hardware test, reboot your Barracuda Web Security Gateway by pressing the Ctrl-Alt-Del keys.

Reboot options

The table below describes the options available at the reboot menu.

Reboot Options	Description
Barracuda	Starts the Barracuda Web Security Gateway in the normal (default) mode. This option is automatically selected if no other option is specified within the first three seconds of the splash screen appearing.
Recovery	Displays the Recovery Console, where you can select the following options: • **Perform File System Repair** — Repairs the file system on XFS, EXT3 and EXT4 based filesystems. Full System re-image should only be done if problems persist after performing a file system repair. Select this option only if the serial number on your Barracuda Web Security Gateway is below 24364; otherwise select the Perform Full System Re-image option. • **Perform Full System Re-image** — Restores the factory settings on your Barracuda Web Security Gateway and clears out the configuration information. Select this option if the serial number on your Barracuda Web Security Gateway is 24364 or above. • **Enable Remote Administration** — Turns on reverse tunnel that allows Barracuda Networks Technical Support to access the system. Another method for enabling remote administration is to click **Establish Connection to Barracuda Support Center** on the **ADVANCED > Troubleshooting** page. • **Run Diagnostic Memory Test** — Runs a diagnostic memory test from the operating system. If problems are reported when running this option, we recommend running the Hardware_Test option next.
Hardware_Test	Performs a thorough memory test that shows most memory related errors within a two-hour time period. The memory test is performed outside of the operating system and can take a long time to complete. Reboot your Barracuda Web Security Gateway to stop the hardware test.

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.

Barracuda Instant Replacement Service

In the event that a Barracuda Web Security Gateway system fails and you cannot resolve the issue, customers who have purchased the Instant Replacement service can call Barracuda Networks Technical Support and receive a new unit within 24 hours.

After receiving the new system, ship the failed Barracuda Web Security Gateway back to Barracuda Networks at the address below with an RMA number marked clearly on the package. Barracuda Networks can provide details on the best way to return the unit.

Barracuda Networks

3175 S. Winchester Blvd

Campbell, CA 95008

attn: RMA # <your RMA number>

To set up the new Barracuda Web Security Gateway so it has the same configuration as your old failed system, restore the backup file from the old system onto the new system, and then manually configure the new system's IP information on the **BASIC > IP Configuration** page. For information on restoring data, refer to How to Back Up and Restore Your System Configuration.

Using the AUX Port

The AUX port on the Barracuda Web Security Gateway can be used for management of the device while the LAN/WAN ports are used for user data and web traffic. If the AUX port is the only port functional on the Barracuda Web Security Gateway, it can be used for minimal access to investigate a new installation issue.