

Backing Up and Restoring the JSON Configuration File

<https://campus.barracuda.com/doc/84313872/>

You can export the Barracuda Web Application Firewall configuration to a JSON-formatted file using the Export WAF Configuration File section on the **ADVANCED > Backups** page. You can either export the complete configuration, or choose **Only Changes** to export the configuration changes that were made on the Barracuda Web Application Firewall after the selected checkpoint was created.

Prerequisite

- It is recommended to use Barracuda Web Application Firewalls with a minimum of 2 CPU cores.

Creating a Configuration Checkpoint

You can create a checkpoint whenever you do a configuration change in the Barracuda Web Application Firewall. The checkpoint internally captures your changes and saves it in the JSON format. You can later use this checkpoint when exporting the WAF configuration in the JSON format to see the changes that were made after the checkpoint was created.

For example, consider you created two HTTPS services (service1 and service2) on the **BASIC > Services** page. To capture this configuration change, you create a checkpoint:

- **Name** - HTTPS_services
- **Comment** - Created two services for HTTPS traffic.

Later, you create another service (service3) on the **BASIC > Services** page and a new security policy on the **SECURITY POLICIES > Policy Manager** page. You can use the checkpoint that you created and see the changes that were made after the checkpoint was created and export the configuration in the JSON-formatted file. This can be accomplished by selecting **Only Changes** as **Backup** and the checkpoint you created (that is, HTTPS_services) from the **Changes After** drop-down list in the **Export WAF Configuration File** section.

The Barracuda Web Application Firewall provides a factory-shipped default configuration JSON file (named "base_config") that contains the factory-shipped configuration. The base_config checkpoint is only for reference purposes and cannot be exported. It is used internally for generating JSON differences. Administrators can also choose to create and download the configuration difference against the changes since the last checkpoint or the base configuration.

You can download and use this file to do the following:

- Validate the configuration of the unit.
- Modify the configuration of the unit.

- Restore the configuration of the unit.
- Configure other WAF units using this as a base configuration.

Export WAF Configuration to a JSON File

1. Go to the **ADVANCED > Backups** page.
2. In the **Export WAF Configuration File** section, do the following:
 1. **Backup** - Choose a type of export for exporting the configuration changes.
 1. **Complete Configuration** - Exports the entire WAF configurations including the base configuration.
 2. **Only Changes** - Exports only the configuration changes that were made on the Barracuda Web Application Firewall after the selected checkpoint was created.
 1. **Changes After** - Select the checkpoint to export the changes that were made after it was created.
 2. **Date** - Displays the date and time when the checkpoint was created.
 2. **Export JSON Configuration File** - Click **Export Now**. A message indicating the status of the export appears.
3. Click **OK**. The export process can take a few minutes for completion depending on the configurations installed. However, the status of completion is indicated on the User Interface. A **Success/Failure** message is displayed at the end of the export process.
4. Click **Download** to download and save the JSON file on your computer.

Restoring the Barracuda Web Application Firewall Configuration JSON File

The exported JSON configuration file can be restored on the same Barracuda WAF or another WAF. Before performing the restore, ensure that the Barracuda WAF does not have any configuration in it. In case the system has any configuration, clear the configuration, and then proceed with restore. It is recommended that you validate the JSON file before restoring the configuration.

The Restore WAF Configuration File section allows you to upload the JSON file for validating and restoring its configurations.

Validate and Restore the Configurations of the JSON File:

1. Go to the **ADVANCED > Backups** page.
2. In the **Restore WAF Configuration File** section, do the following:
3. From **Action Type**, specify the option that you want to perform on the JSON configuration file.
 1. **Validate** - Runs the configurations of the JSON file and validates for any errors. The file validation might take a few minutes depending on number of configuration objects

present in the file. A **SUCCESS/FAILURE** message is displayed if the configuration in the file is valid/not valid. In case of failure, click the Download link at the bottom of the section to learn more about the errors that occurred when the configurations were applied on a test stack .

2. **Apply Configuration** - Runs the JSON file and installs the configurations. The percentage progress bar indicates the percentage of configurations applied to a test stack. A **SUCCESS/FAILURE** message is displayed if the configuration is installed/not installed click the Download link at the bottom of the section to learn more about the errors that occurred when applying the configuration.
4. Click **Browse** and select the JSON file that you want to restore.
5. Click **Upload Now** to upload the JSON file.

- The validation of the configuration can be performed only on stand-alone WAFs.
- Restoration of the configurations can be performed on stand-alone WAFs, and JSON configuration bootstrapping can be performed while launching autoscaling WAFs in a cloud environment.
- Unlike conventional Backups and Restore functionality, the JSON configuration import operation does not require reboot of WAF unit.

© 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.