Configuration Tool for Barracuda WSA Windows Client 5.0 and Above

https://campus.barracuda.com/doc/70584314/

This article applies to Windows laptops and desktops running version 5.0 and higher of the Barracuda Web Security Agent with version 12.x and higher of the Barracuda Web Security Gateway.

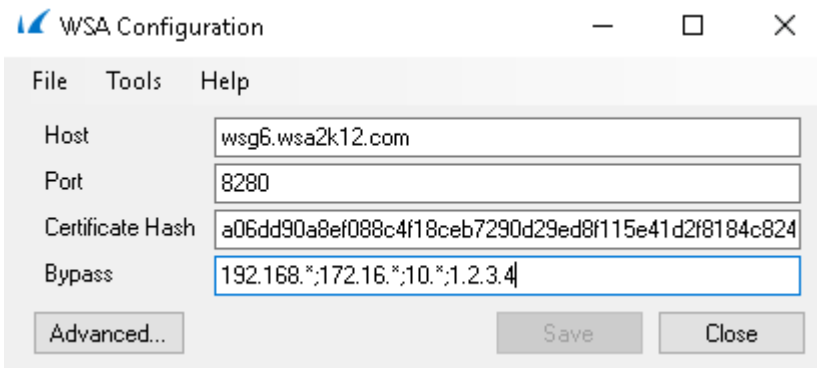
The Configuration Tool makes it easy for the administrator to change settings for the Barracuda WSA from the client. The tool exposes the same settings that are configured from the administrative web interface t he Barracuda Web Security Gateway **ADVANCED > Remote Filtering** page. The tool can optionally be password protected in the administrative web interface.

To run the tool, type **Configuration** in the Windows Startup menu. Click on **Configuration** next to the Barracuda icon in the menu. You then see the Configuration window (see Figure 1 below) showing the following settings:

- Host: The IP address of the Barracuda Web Security Gateway
- Port
- Certificate Hash: This value enables the Barracuda WSA to validate the identity of the Barracuda Web Security Gateway and encrypt all administrative traffic. Available from the **ADVANCED > Remote Filtering** page. See Authentication with the Barracuda Web Security Gateway and the Barracuda WSA.
- Bypass IP addresses - IP addresses/ranges you want the Barracuda WSA to bypass when filtering

Click **Save**. You will be prompted for the administrator password in order to save the changes; the password is required.

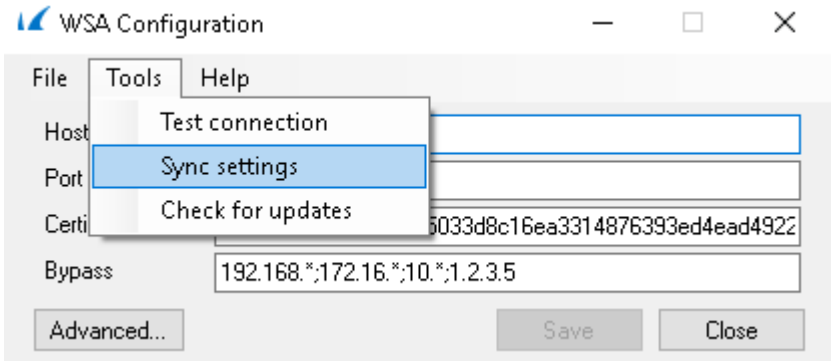
Figure 1. Configuration Tool showing the current host Barracuda Web Security Gateway.



The settings shown are those based on the last sync event between the Barracuda WSA and the Barracuda Web Security Gateway. A sync event is triggered by any of the following:

- User logging into Barracuda WSA
- A network change
- Clicking on the Barracuda WSA icon in the task tray and selecting **Sync**

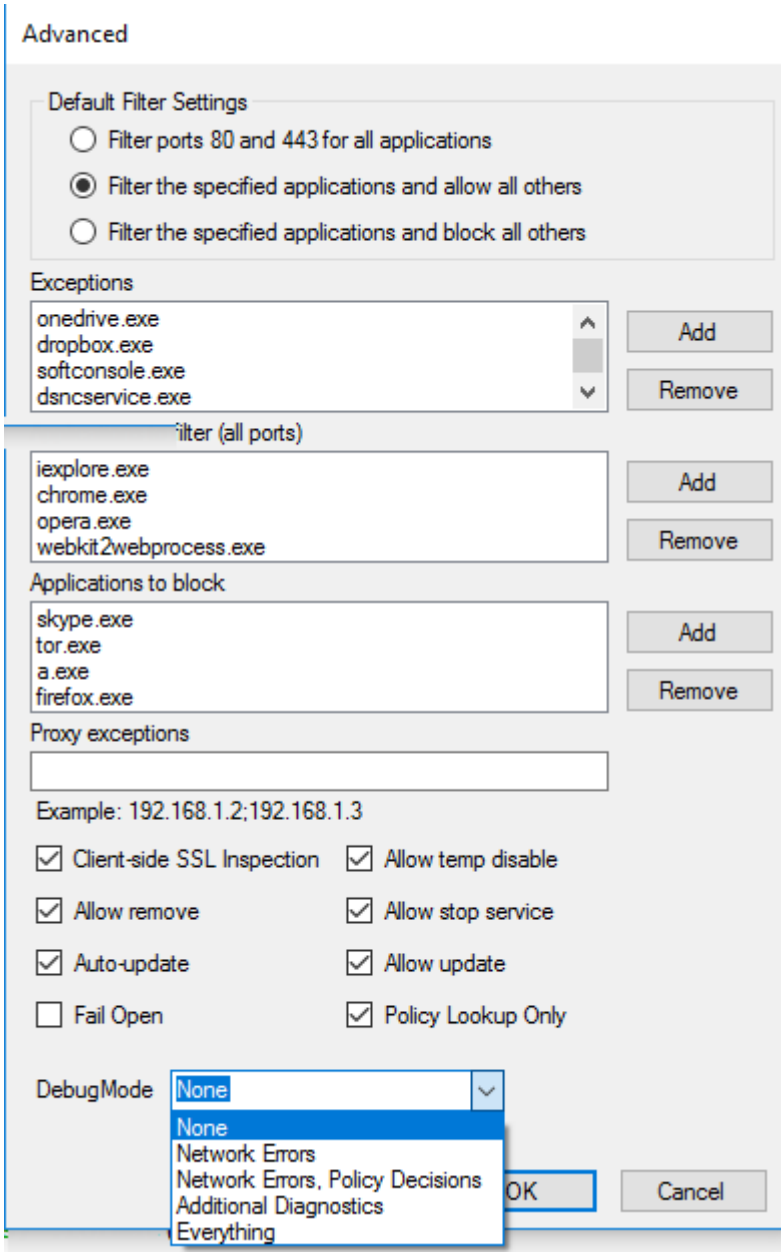
The sync event also updates the client with browse policies configured on the Barracuda Web Security Gateway. **Note that only the administrator can sync settings between the Barracuda WSA and the host from the configuration tool, or to check for updates with the tool:**



Barracuda WSA Settings on the Client

Click on the **Advanced** button in the Configuration tool window to see and modify the settings that are configured on the Barracuda Web Security Gateway **ADVANCED > Remote Filtering** page.

Figure 2. Advanced Configuration Tool Window



Configuration options are described in detail on the **ADVANCED > Remote Filtering** page of the Barracuda Web Security Gateway. Note the following:

- **Fail Open**: see Fail Open and Fail Closed Modes with the Barracuda WSA for more information.
- **Client-side SSL Inspection**: Enabling client-side SSL Inspection on the client computer offloads resource-intensive processing from the Barracuda Web Security Gateway. See Client-side SSL inspection with the Barracuda WSA for details.
- **Debug Mode** is set to **1** by default. This setting can be configured from the tool with these levels. The higher the level, the more that is being logged.

0: Disable logging

1: Log network errors – Basic logging level with the least amount of information.

2: Log network errors, policy decisions – Use this level If you are troubleshooting policy decisions that come from the Barracuda Web Security Gateway.

3: Log additional diagnostics – Use logging level 3 or 4 if you want to know more about what is happening on the Barracuda WSA agent side.

4: Log everything – This level is quite verbose (returns a lot of information).

Debug Mode can also be set at installation using command line options. For example, if you prefer a logging level other than the default (1):

BarracudaWSASetup.exe /v"/qb- /lvmo setup.log SERVICE_URL="my.serviceHost.com" SERVICE_PORT=8280 **DEBUG=<debug level>**

where **<debug level>** can be 0, 1, 2, 3, or 4.

Figures

1. Config_Tool_main.png
2. Config_tool_Sync_Settings.png
3. ConfigToolSettings5.0.PNG