

Configuration Tool for Barracuda WSA Windows Client 4.x

<https://campus.barracuda.com/doc/41101678/>

This article applies to the Barracuda WSA version 4.x. For version 5.0 and above, see [Configuration Tool for Barracuda WSA Windows Client 5.0 and Above](#).

The Configuration Tool makes it easy for the administrator to change settings for the Barracuda WSA from the client. The tool exposes the settings that are configured from the web interface of the Barracuda Web Security Gateway **ADVANCED > Remote Filtering** page. You can optionally password protect the tool from that page.

To run the tool, type **Configuration** in the Windows Startup menu. Click on **Configuration** next to the Barracuda icon in the menu. When you run the Configuration tool you are prompted for the Barracuda WSA Password if one was configured in the web interface. You then see the Configuration window showing the following settings:

- Host: The IP address of the Barracuda Web Security Gateway
- Port
- Bypass IP addresses - IP addresses/ranges you want the Barracuda WSA to bypass when filtering

The settings shown are those based on the last sync event between the Barracuda WSA and the service host. 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.

Barracuda WSA Settings on the Client

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

Figure 1. Advanced Configuration Tool Window Using the Barracuda Web Security Gateway

Advanced

Default Filter Settings

☐ Filter ports 80 and 443 for all applications
☒ Filter the specified applications and allow all others
☐ Filter the specified applications and block all others

Exceptions

dsncservice.exe
 dsnetworkconnect.exe
 junipersetupclient.exe
 mmc.exe

Add Remove

Applications to filter (all ports)

iexplore.exe
 firefox.exe
 chrome.exe
 safari.app

Add Remove

Applications to block

Add Remove

Proxy exceptions

Example: 192.168.1.2;192.168.1.3

☐ Debug mode ☐ Allow temp disable
☐ Allow remove ☐ Allow stop service
☒ Auto-update ☒ Allow update
☐ Fail Open ☐ Policy Lookup Only
☐ Disable Tamper Protection ☒ Use WFP for traffic interception

OK Cancel

Note the following exceptions:

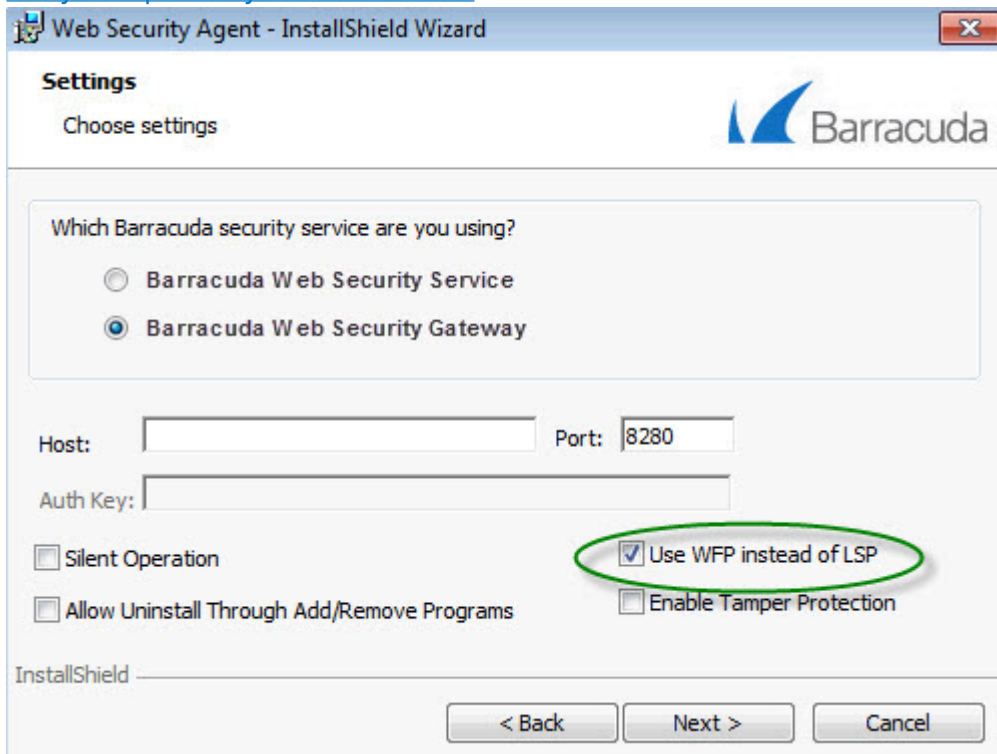
- If the **Auto update** and **Allow User to Check for Update** settings on the **ADVANCED > Remote Filtering** page of the Barracuda Web Security Gateway web interface are not enabled, users will not see the those settings in the configuration tool **Advanced** window shown above.
- The **Policy Lookup Only Mode** check box only appears for users who are remote filtered by the Barracuda Web Security Gateway. When **Policy Lookup Only Mode** is enabled, the Barracuda WSA client on the remote user's machine looks up policies configured on the Barracuda Web Security Gateway for that user/client, applies the policies, then routes allowed web traffic from the user's machine via its usual path to the Internet. In this mode, because traffic is not routed through the Barracuda Web Security Gateway, **SSL Inspection** cannot be applied to HTTPS traffic from remote computers when **Policy Lookup Only Mode** is enabled.
- **Disable Tamper Protection** - (*Tamper Protection is not available on version 5.x and above*)

You should disable Tamper Protection:

- When installing a new Windows Service Pack
- When installing a new AV software version.

The feature will remain disabled until it is re-enabled by unchecking the checkbox or by the next reboot of the machine.

- **Use WFP for traffic interception** will only show if you checked **Use WFP instead of LSP** option at installation. This feature only applies for Windows 7 users. See [Troubleshooting Third Party Compatibility Issues With LSP](#) for details.



The screenshot shows the 'Settings' window of the 'Web Security Agent - InstallShield Wizard'. The window has a title bar with the Barracuda logo and the text 'Web Security Agent - InstallShield Wizard'. Below the title bar, there is a 'Settings' section with a 'Choose settings' link. The main content area contains a question: 'Which Barracuda security service are you using?'. There are two radio button options: 'Barracuda Web Security Service' and 'Barracuda Web Security Gateway'. Below this, there are input fields for 'Host:' and 'Port:' (with '8280' entered). There is also an 'Auth Key:' input field. At the bottom, there are four checkboxes: 'Silent Operation', 'Allow Uninstall Through Add/Remove Programs', 'Use WFP instead of LSP' (which is checked and circled in green), and 'Enable Tamper Protection'. At the very bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

- **Fail Open** setting: see [Fail Open and Fail Closed Modes with the Barracuda WSA](#) for more information about this setting.

Figures

1. ConfigTool4.4.6.jpg
2. InstallerWSSWSGwithWFPchecked.jpg

© 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.