Configuration Options for the Barracuda Web Security Agent

https://campus.barracuda.com/doc/68354116/

The following options can be used when installing the Barracuda WSA from the command line or with a GPO. See also:

- Command Line Examples For Installation of the Barracuda WSA With EXE Installer
- Command Line Examples For Installation of the Barracuda WSA With MSI Installer

Option	Description
ADS (Allow Disable Service)	**1** – Users are allowed to disable the Barracuda WSA. **0** – Users are NOT allowed to disable the Barracuda WSA.
ALLOW_REMOVE	**1** – Users are allowed to remove the Barracuda WSA. **0** – Users are NOT allowed to remove the Barracuda WSA.
ALLOW_UPDATE	**1** (Default) – Allow users to manually update through the Barracuda WSA Monitor and Configuration Tool. **0** – Do not allow users to manually update. Note: This setting has no effect on automatic updates.
APPLICATIONS	Type a pipe-delimited list of applications to be filtered on all ports. Example: APPLICATIONS= iexplore.exe|firefox.exe
BLOCKS	A pipe-delimited list of applications to block. Example: BLOCKS=block1.exe | block2.exe
CERT_HASH	*Available with version 5.0 and above* This value enables the Barracuda WSA to validate the identity of the Barracuda Web Security Gateway and encrypt all administrative traffic. Configure at install time or from the **ADVANCED > Remote Filtering** page. See Authentication with the Barracuda Web Security Gateway and the Barracuda WSA for details.
CLIENT_SSL	*Available with version 5.0 and above* **1** – Client-side SSL Inspection is ENABLED. **0** – Client-side SSL Inspection is DISABLED (default). 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	*These specific settings available with version 5.0 and above* **0** – Disable logging **1** – Log network errors **(default)** **2** – Log network errors, policy decisions **3** – Log additional diagnostics **4** – Log everything

DEFAULT_BEHAVIOR	**1** – All application traffic is forwarded to ports 80 and 443 by default. **2** – No application traffic is forwarded by default and you specify only the applications to filter. **3** – All applications are blocked by default and only applications you specify for filtering are forwarded.
DISABLE_AUTOMATIC_UPDATES	**1** – Updates are DISABLED. **0** – Updates are ENABLED.
EXCEPTIONS	A pipe-delimited list of specific applications from which you don't want to capture any traffic.
FAIL_OPEN	*Available with version 5.0 and above* **1** – Fail Open feature is ENABLED. **0** – Fail Open feature is DISABLED (default). See Fail Open and Fail Closed Modes with the Barracuda WSA for more information about this setting.
LANG	Specifies the language that the Barracuda WSA uses on English operating systems. German: de-DE Japanese: ja-JP Dutch: nl-NL Chinese: zh-CN Chinese Traditional: zh-TW Portuguese: pt-BR Spanish: es-ES
PASSWORD	The password that users must know to stop or configure the Barracuda WSA. Barracuda Networks strongly recommends using a password. Leaving the password field blank allows the user to modify most of the Barracuda WSA settings.
PLO	*Available with version 5.0 and above* **1** – Policy Lookup feature is ENABLED. **0** – Policy Lookup feature is DISABLED (default). Enabling this feature means that 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. See Policy Lookup Only Mode With the Barracuda Web Security Agent for more information.
PROXY_EXCEPTIONS	A semicolon delimited list of network addresses to specify proxy exceptions for internal proxies that should be reachable by Barracuda WSA clients for internal proxying and filtering. Guidelines: Use a * in any octet (except the first) to indicate "any". Entries that begin with a dot (.) include any URL that matches the dot and subsequent string(s). For example, if you use *.example.com as a proxy exception entry, any URL that ends with .example.com will bypass the proxy. URL names that begin with a string (and not a dot) must match the string exactly.

SERVICE_MODE	**For the Barracuda Web Security Agent version 4.x and below:** **2** – Use for the Barracuda Web Security Gateway. **For the Barracuda Web Security Agent 5.0 and above: (The Barracuda Web Security Service is not supported)** **1** – Use for the Barracuda Web Security Gateway. **Example**: SERVICE_MODE=1
SERVICE_PORT	The port number through which the Barracuda WSA communicates to the Barracuda Web Security Gateway. This parameter follows SERVICE_URL. Example: SERVICE _PORT=8280
SERVICE_URL	The URL of the Barracuda Web Security Gateway, followed by SERVICE_PORT and port number. The URL can be a domain name or IP address. Example: SERVICE_PORT=8280
USER_MODE	0 – (Default) Indicates ordinary operation. The Barracuda WSA Monitor appears in the task tray and the Configuration Tool appears in the Program Files menu. 1 – Runs the Barracuda WSA in Silent Mode.
WD	*Not available on version 5.x and above* 1 – Enables the watchdog feature, preventing the removal of Barracuda WSA through tampering with registry settings or network settings. 0 – (Default) Disables the watchdog feature. Warning: Test this setting before deploying into your environment, as locking down network settings and the registry can produce unwanted side effects in your system.
WFP	To choose WFP drivers instead of LSP, set the **WFP** flag to **1**. This option only applies for Windows 7. For all other Windows versions, this flag is ignored. See Troubleshooting Third Party Compatibility Issues With LSP for details about this option.