# Automated Installation of the Barracuda WSA

https://campus.barracuda.com/doc/49058812/

This article applies to using the Barracuda Web Security Agent (WSA) with the Barracuda Web Security Gateway.

## Automated Installation

The Barracuda WSA is designed to support automated installation processes in place in many organizations for managing software deployments. The Barracuda WSA installation program is available as an MSI or an EXE file for flexibility in deployment methods. This article explains a method for creating a self-executing zip file using free tools. You can use this file to automatically pass installation parameters to the Barracuda WSA setup program. Similar processes support MSI installation methods. Consult the documentation for your software deployment solution for details on how to use a typical MSI or EXE installation program.

### Requirement for Automated Installation

- You must have a file archiving utility capable of creating a self-extracting .exe file.
- You must have Microsoft .NET framework installed before you install the Barracuda WSA using the MSI installation method. The MSI file does not install the.NET framework for you. If you do not install the .NET framework before you begin installation with the .MSI file, a message appears prompting you to download and install the .NET framework and then install the Barracuda WSA. For Microsoft .NET Framework and Windows version compatibility, see Requirements for the Barracuda Web Security Agent With Windows.

### Set Up the Directory

To set up the installation directory:

1. Create a directory for the setup program (For example: c:\BarracudaWSA).
2. Copy the Barracuda WSA setup file to the directory.
3. Create a setup.bat file to execute the setup program.
   **Example** (type all on one line): “C:\barracudawsasetup.msi" /v" /qb! /lvmo c:\setup.log SERVICE_URL=10.1.0.51 SERVICE_MODE=2 SERVICE_PORT=8280
4. Put the setup.bat file in your setup program directory.

### Arguments and Options

Use the following arguments and options to control the configuration of the Barracuda WSA.

Arguments:

- **v** passes the **/qn** (no UI) parameter to the installer, which runs the executable in silent mode.

You can set the **USER_MODE** switch to **1** for silent operation (the end user will not see the Barracuda WSA icon in the System Tray or Start Menu).

**Example using various options:**

See Table 1 for a full list of options.

BarracudaWSASetup.exe /s /v"/lvemo \setup.log /qn

ALLOW_REMOVE=1

EXCEPTIONS=chrome.exe|safari.exe

APPLICATIONS=explorer.exe|firefox.exe

BYPASS=11.11.11.0 ADS=1 PASSWORD=pass"

The above example also writes a log file to the setup directory called **setup.log**.

**Table 1. Installation/Configuration options**

| Option | Description |
|---|---|
| ADS | **1** indicates that users are allowed to disable the Barracuda WSA.<br>**0** indicates that users are NOT allowed to disable the Barracuda WSA. |
| ALLOW_REMOVE | **1** indicates that users are allowed to remove the Barracuda WSA.<br>**0** indicates that users are NOT allowed to remove the Barracuda WSA. |
| ALLOW_UPDATE | **1** allows seamless updates to the Barracuda WSA. The Check for Update menu option does not appear in the Configuration Tool (default).<br>**0** disables seamless updates. The Check for Update menu option appears in the Configuration Tool. |
| APPLICATIONS | Type a pipe-delimited list of applications to be filtered on all ports to the Barracuda Web Security Gateway.<br>Example:<br>APPLICATIONS= iexplore.exe\|firefox.exe |

| | |
|---|---|
| BLOCKS | Type a pipe-delimited list of applications to block. Example: BLOCKS=block1.exe \| block2.exe |
| BYPASS | Type a semi-colon-delimited list of network addresses that you want to bypass the Barracuda Web Security Gateway, such as trusted internal networks. Guidelines:<br>Use a * in any octet (except the first) to indicate “any”.<br>Bypass entries that begin with a dot (.) will include any URL that matches the dot and subsequent string(s). For example, if you use *.example.com as a bypass entry, any URL that ends with .example.com will bypass the proxy.<br>URL names that begin with a string (and not a dot) must match the string exactly. |
| DEBUG | **1** indicates that the Debug mode is ENABLED.<br>**0** indicates that the Debug mode is DISABLED (default). |
| DEFAULT_BEHAVIOR | **1** indicates that all application traffic is forwarded to ports 80 and 443 by default.<br>**2** indicates that no application traffic is forwarded by default and you specify only the applications to filter.<br>**3** indicates all applications are blocked by default and only applications you specify for filtering are forwarded. |
| DISABLE_AUTOMATIC_UPDATES | **1** indicates that updates are DISABLED.<br>**0** indicates that updates are ENABLED. |
| EXCEPTIONS | If there are specific applications from which you don’t want to capture any traffic, type them in as a pipe-delimited list. |
| LANG | Specifies the language that the Barracuda WSA uses on English operating systems.<br>German: de-DE<br>Japanese: ja-JP<br>Dutch: nl-NL<br>Chinese: zh-CN<br>Chinese Traditional: zh-TW<br>Portuguese: pt-BR<br>Spanish: es-ES |
| PASSWORD | Type the password users must know to configure, stop or start the Barracuda WSA. |
| PROXY_EXCEPTIONS | Type a semi-colon-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.<br>Guidelines:<br>Use a * in any octet (except the first) to indicate “any”. Entries that begin with a dot (.) will 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 | **2** indicates that you are using the Barracuda Web Security Gateway.<br>**Example**: SERVICE_MODE=2 |
| SERVICE_PORT | Type the port number of the Barracuda Web Security Gateway, which is<br>8280 by default. This parameter follows the SERVICE_URL.<br>**Example**: SERVICE_URL=myWebFilter.com SERVICE_PORT=8280 |
| SERVICE_URL | Type the value of the **ExternalIP address** defined on the **ADVANCED** > **Remote Filtering** page from within the Barracuda Web Security Gateway interface, followed by SERVICE_PORT and the port number (**Destination Port** on the same page). Do not use the hostname; this parameter must use an IP address. See the example syntax at the top of this article. |
| USER_MODE | **0** indicates ordinary operation.<br>**1** indicates silent operation. |
| WD | **1** enables the watchdog feature.<br>**0** disables the watchdog feature (default). |

### Create a Compressed File

Use Windows Explorer to create a compressed file from the setup program directory that contains the Barracuda WSA setup program and your setup.bat file.

### Create a Self-Extracting Archive

Use the file archive utility EXE creator to create a self-extracting file of the compressed directory.

### Deployment

The self-extracting installation program may now be distributed via login script, network share, or other means for automated installation of the Barracuda WSA.