How to Install the Barracuda WSA with the Barracuda Web Security Gateway

https://campus.barracuda.com/doc/42047058/

Barracuda Networks recommends reading this entire article and associated release notes (see links below) before installing the Barracuda Web Security Agent (WSA). After the Barracuda WSA is installed and configured, your web traffic is protected by the Barracuda Web Security Gateway automatically.

The Barracuda WSA directs all traffic from web browsers, and other application traffic on ports 80 and 443, to the Barracuda Web Security Gateway. See also:

- Release Notes for the Barracuda Web Security Agent for Windows OR
- Release Notes for the Barracuda WSA for Macintosh
- Requirements for the Barracuda Web Security Agent With Windows

After installation, continue with How to Configure the Barracuda WSA With the Barracuda Web Security Gateway.

Step 1. Download the Barracuda Web Security Agent (WSA)

Download either the MSI or EXE installer for the Barracuda WSA for Windows, or the DMG file for Mac from the **ADVANCED > Remote Filtering** page of the Barracuda Web Security Gateway. See Windows Installer (MSI) and Windows InstallShield (EXE) documentation for information about Windows command line options. If you download the Barracuda WSA installation file for MS Windows, you have the choice to either load the installer onto each remote client and install directly through the Windows interface, or to push it to client machines using a GPO. Either the .exe or.msi installer can be used to install through GPO or manual installation.

- **Using the Windows EXE** – Installer EXE files can contain any kind of executable code to run, such as a batch file. The Barracuda WSA EXE (bootstrapper) installer runs a check for requirements before installation. You can use the Barracuda WSA EXE installer inside a batch file to install on a Windows PC from the command line, or to install automatically using a GPO.
- **Using the Windows MSI Installer –** MSI files are database files, used by Windows Installer and contain information about an application. MSI files are executed by an EXE file that is part of Windows, called msiexec.exe. The Barracuda WSA .msi file does NOT run a check for requirements before installation.

  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.

1. Log into the Barracuda Web Security Gateway as **admin**.
2. Go to the **ADVANCED > Remote Filtering** page.
3. Download the Barracuda WSA installation files for MS Windows or for the Macintosh.

Step 2. Understand Prerequisites for Installation or Upgrade

- The remote user must have an LDAP record in the domain.
- Because the Barracuda Web Security Gateway will listen on port 8280 (by default) for Barracuda WSA requests, you must make this port available for incoming and outgoing traffic to the Barracuda Web Security Gateway. The Barracuda WSA cannot forward traffic properly if personal firewalls or other devices block non-standard ports. Create a port forward on your network firewall on port 8280 to the local IP address of your Barracuda Web Security Gateway (as specified in the External Hostname/IP Address field on the **ADVANCED > Remote Filtering** page).
- The Barracuda WSA operates on network traffic at a low level within the operating systems, so some anti-virus applications may flag the Barracuda WSA as suspicious during installation or operation. Ensure that your anti-virus client does not block or has an exception for any Barracuda WSA files that the anti-virus client flags as suspicious.
- For Windows installations:
  - The client PC must have Windows installed on the C:\ drive for successful installation of the Barracuda WSA. The Barracuda WSA will not install successfully when Windows is installed on the D:\ drive.
  - 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 system requirements for Windows installations, see Requirements for the Barracuda Web Security Agent With Windows.
- For system requirements for Macintosh installations, see How to Install the Barracuda Web Security Agent on Mac OS.

The Barracuda WSA is now localized for the following languages:

- German
- Japanese
- Dutch
- Chinese
- Chinese Traditional
- Portuguese

- Spanish

Step 3. Understand and Select Key Options Before Installation

Password Protection and User Privileges

During installation, you have an option to specify a password to protect configuration options and control user privileges. Alternatively, you can specify a password for the Barracuda WSA on the **ADVANCED > Remote Filtering** page of the Barracuda Web Security Gateway If you specify a password during installation, that password is required for any user to:

- Change configuration settings using the Configuration Tool
- Temporarily disable the Barracuda WSA (to allow a user to connect to a public network, such as at a captive portal in a hotel or coffee shop, before the Barracuda WSA starts again automatically after two minutes)
- Stop the Barracuda WSA service
- Uninstall Barracuda WSA on the client

Barracuda Networks strongly recommends using a password. Leaving the password field blank on the WSG allows the user to modify most of the WSA settings.

Important! There is no password reset; if the password is lost, the administrator must reinstall the Barracuda WSA.

Allow Uninstall Option

During installation, you can choose the **Allow Uninstall Through Add/Remove** Programs option to allow Windows users to remove the Barracuda WSA from a PC or laptop using the Microsoft Windows Add or Remove Programs utility. Use the password protection feature to ensure that unauthorized users cannot uninstall the Barracuda WSA. Note that the Barracuda WSA does not, by default, appear in the Windows Add or Remove Programs list.

Stop/Start Service Option

During installation, you can choose the option to let users stop the Barracuda WSA from the task tray. This is sometimes helpful with troubleshooting network or performance issues, or when the user needs to connect with their VPN (see below). You can use the password protection feature to ensure that only authorized users can stop the Barracuda WSA.

VPN Interoperability

The Barracuda WSA will forward all web traffic to the Barracuda Web Security Gateway, so virtual

private network (VPN) clients that rely on web browser settings to forward traffic to private networks may interfere with the Barracuda WSA's operation.

In order to use a VPN client on a PC that is running the Barracuda WSA, the end user may either have to:

- Stop the Barracuda WSA when connecting with the VPN,
- Use the VPN in split tunnel mode, or
- Have the Barracuda Web Security Gateway enter bypasses for the VPN server IP address in the Bypass Filter text box on the **ADVANCED > Remote Filtering** page of the Barracuda Web Security Gateway web interface. You can also specify bypass exception network addresses in the Bypass field during manual local installation or by using the BYPASS option in a GPO installation.

If you install and configure the Barracuda WSA so that end users may not stop it, then only bypasses or split tunnel mode will work simultaneously with the Barracuda WSA. You can use the password protection feature, available during installation, to ensure that only authorized users can stop the Barracuda WSA.

Automatic Software Updates

The Barracuda WSA periodically checks the Barracuda Web Security Gateway for available software updates. When an upgrade is available, the Barracuda WSA automatically and silently downloads and installs it, preserving any configuration information you have in place. The automatic updater works whether the Barracuda WSA is installed in regular mode or **Silent Operation** mode. Automatic updates may be disabled at installation for those networks for which the admin prefers to manage upgrade deployments manually.

Step 4. Select a Method For Installing the Barracuda WSA

- Installation on the Remote Windows Client – Load the Barracuda WSA installer on each remote Windows machine and use the Windows InstallShield.
- Installation Using a Windows GPO From the Windows Interface – push the Barracuda WSA to a group of remote computers using a Windows tool to create a template for the GPO.
- Installation using a Windows GPO from the Command Line– push the Barracuda WSA to a group of remote computers from a batch (.bat) file on the server.
- Manual Local Installation from the Command Line
- Installation on a Macintosh

Caution Behavior in the Microsoft Small Business Server (SBS) 2008 breaks the server-client

trust relationship when using GPO deployment. The client has to be rejoined to the server, manually. See GPO Installation of the Barracuda WSA With Microsoft SBS 2008 Server for instructions.

Step 5. Configure the WSA Installation

After you have installed the Barracuda WSA on your client machines, continue with How to Configure the Barracuda WSA With the Barracuda Web Security Gateway.

Uninstalling the Barracuda WSA

- With Windows: See Uninstalling the Barracuda Web Security Agent for Win2K8 Server or Uninstalling the Barracuda Web Security Agent for Win2K3 Server, depending on your Windows server version.
- With the Macintosh: see How to Install the Barracuda Web Security Agent on Mac OS.