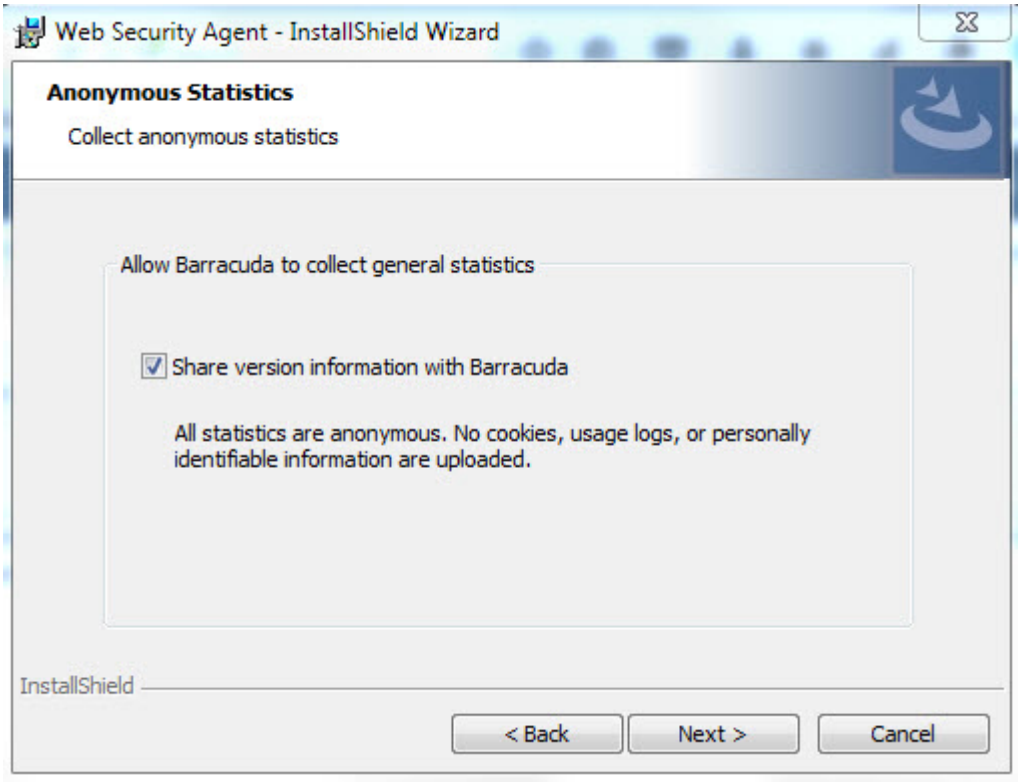
Manual Local Installation of the Barracuda WSA With Windows

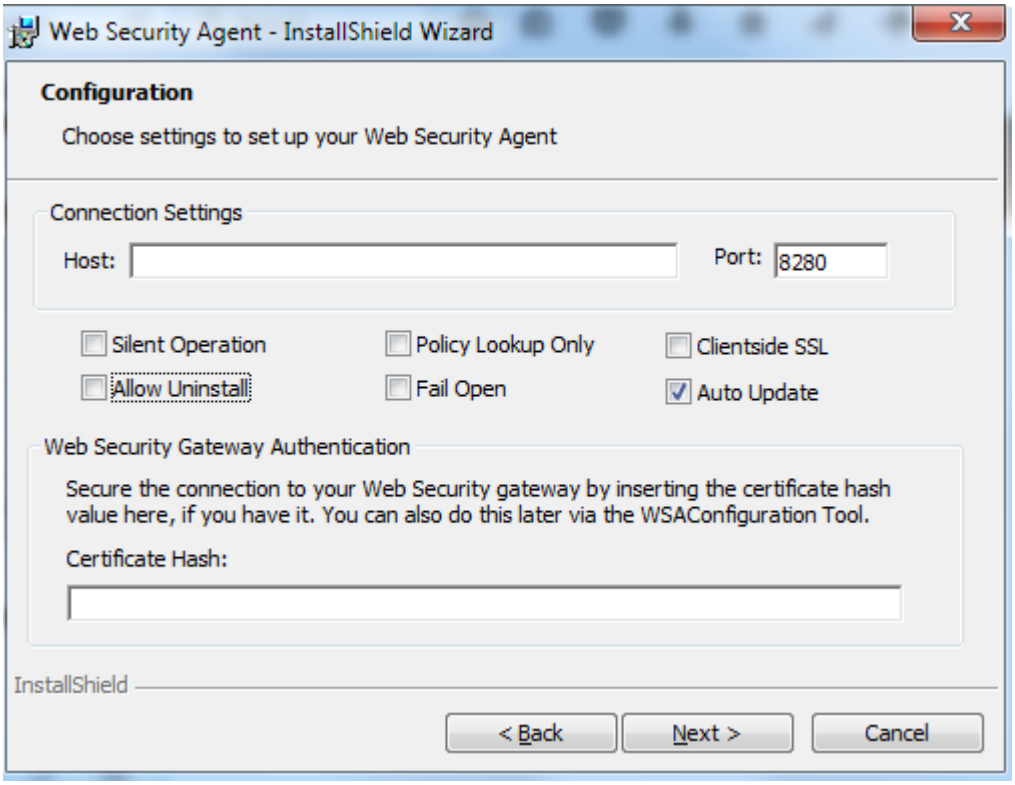
https://campus.barracuda.com/doc/48201968/

Before installation, it is recommended to read How to Install the Barracuda WSA with the Barracuda Web Security Gateway and understand the installation requirements for Windows.

1. Download the Barracuda WSA installer per instructions in How to Install the Barracuda WSA with the Barracuda Web Security Gateway.
2. Log into the remote client Windows machine as administrator.
3. Copy the Barracuda WSA installer onto the machine.
4. Run the installer and accept the license agreement, and then, in the Anonymous Statistics window, decide if you want to allow the Barracuda WSA to share version information with Barracuda. Checking this box allows the Barracuda WSA to collect and share general statistics with Barracuda, all of which are anonymous. Click Next.



5. In the Configuration window, select Barracuda Web Security Gateway and configure options as described below:



Click Next, and then click Install.

- **Host** - Enter the **External IP address** as defined on the **ADVANCED** > **Remote Filtering** page from within the Barracuda Web Security Gateway interface. The default **Port** is 8280 and should match the **Destination Port** on the same page.
- **Silent Operation** - If checked, the end user will not see the Barracuda WSA icon in the System Tray or Start Menu. Note that 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.
- **Allow Uninstall** - If checked, this option allows 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.
- **Policy Lookup Only -** By default, the Barracuda WSA routes client web traffic through the Barracuda Web Security Gateway, which monitors traffic and applies policies before routing the traffic. When **Policy Lookup Only** mode is enabled, the Barracuda WSA deployed on the remote 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 remote machine via the usual path to the Internet. *Traffic is not routed through the Barracuda Web Security Gateway.* For more information, see Policy Lookup Only Mode With the Barracuda Web Security Agent.
- **Fail Open** - Applies only when using the Barracuda Web Security Service. If connectivity

from the Barracuda Web Security Agent (WSA) to a service host cannot be established (i.e. Fallback to another Barracuda Web Security Service host, or connectivity to the Barracuda Web Security Gateway, was unsuccessful), the admin must configure the Barracuda WSA to either Fail Open or Fail Closed. See Fail Open and Fail Closed Modes with the Barracuda WSA.

- **Client-side SSL Inspection** - *Available for Barracuda WSA version 5.0 and above.* Enabling client-side SSL Inspection on the client computer offloads resource-intensive processing from the Barracuda Web Security Gateway. This configuration is highly scalable in terms of number of users, consuming fewer resources on the Barracuda Web Security Gateway and improving system performance.See Client-side SSL inspection with the Barracuda WSA for details and version requirements.
- **Auto Update** - If **Auto-update** and **Allow User to Check for Update** settings on the Barracuda Web Security Gateway **ADVANCED > Remote Filtering** page are not set to **Yes** (enabled), the user will not see the **Auto-update** check box in the configuration tool.
- **Certificate Hash** - *Available for Barracuda WSA 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. For more information and version requirements, see Authentication with the Barracuda Web Security Gateway and the Barracuda WSA. You can either follow instructions below to get the certificate hash and input it in the Configuration window as shown above, or input it later, after installation, using the Configuration Tool for Barracuda WSA Windows Client 5.0 and Above.
  To get the certificate hash:

  1. Log into the Barracuda Web Security Gateway web interface as *admin.*
  2. Go to the **ADVANCED > Remote Filtering** page.
  3. In the **Saved Certificates** section, click **Help** and follow instructions to either create a private (self-signed) certificate, or to upload a certificate purchased from a trusted CA.
  4. After you create or upload the certificate, it will appear in the **Saved Certificates** table. Click **Activate** in the **Actions** column.
     The certificate hash can now be shared with the Barracuda WSA on each Windows machine.

The Barracuda Web Security Gateway certificate hash is the SHA-256 of the admin certificate and, with version 11.0 and higher, can be copied to the clipboard from the **Saved Certificates** table on the **ADVANCED > Remote Filtering** page. Paste this value into the **Certificate Hash** field.

Figures