Configuring Preferences for Barracuda WSA Mac OS Clients

https://campus.barracuda.com/doc/41102749/

The administrator can access the Barracuda **WSA Preferences** from the context menu or from the System Preferences interface to change settings for the Barracuda WSA from the client. The tool exposes the same settings that are configured from the administrative web interface of the Barracuda Web Security Gateway **ADVANCED > Remote Filtering** page.

If you want to configure client-side SSL inspection on the Barracuda WSA, this must be configured in the Barracuda Web Security Gateway web interface. See Client-side SSL inspection with the Barracuda WSA for version requirements and instructions to configure.

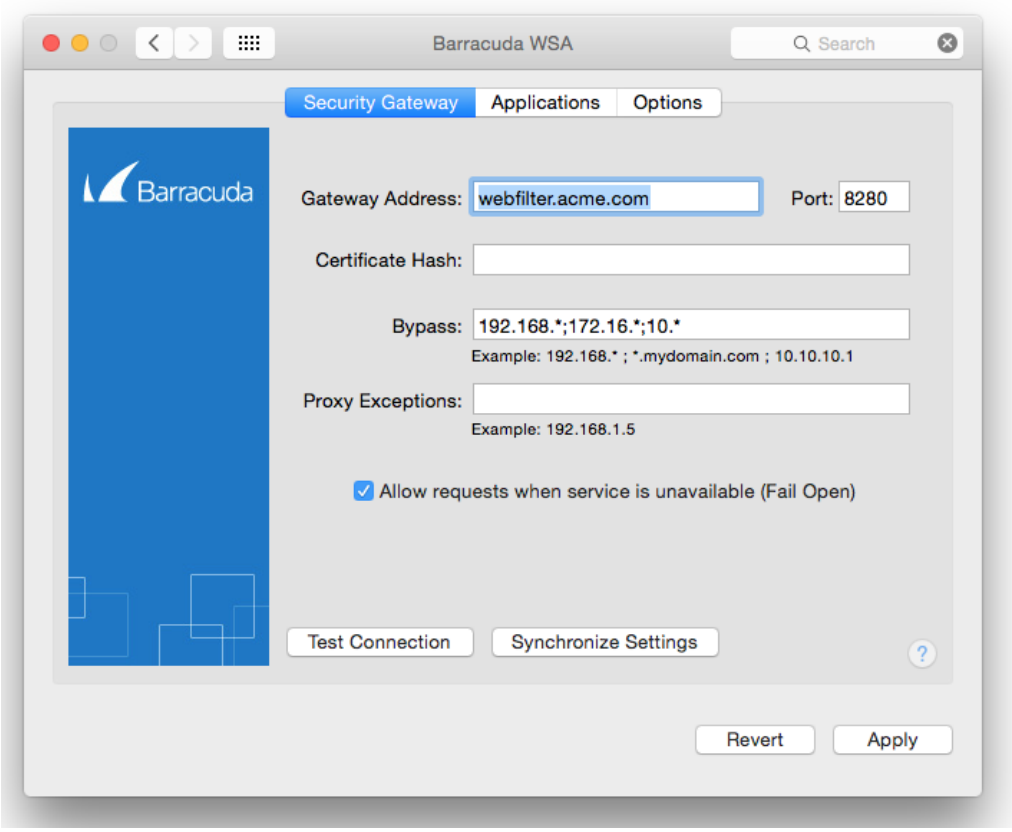
Barracuda WSA Preferences can optionally be password protected on the **ADVANCED > Remote Filtering** page of the Barracuda Web Security Gateway. **Important**: Leaving the password field blank allows the user to modify most of the Barracuda WSA settings.

Barracuda WSA preferences with the Barracuda Web Security Gateway include the following settings (see Figure 1):

- Gateway Address and Port - The external IP address and port to reach the Barracuda Web Security Gateway. See the **External Hostname/IP** and **Destination Port** fields on the **ADVANCED > Remote Filtering** page in the Barracuda Web Security Gateway web interface. The Barracuda WSA directs user web traffic to this IP address. **Note**: It is recommended that you enter the *hostname* of your Barracuda Web Security Gateway in case the IP address of the appliance changes. See also How to Configure the Barracuda WSA With the Barracuda Web Security Gateway.
- Port - the network port at which to contact the Barracuda Web Security Gateway.
- Certificate hash - With version 2.0 or higher of the Barracuda WSA for Mac OS . This value enables the Barracuda WSA to validate the identity of the Barracuda Web Security Gateway and encrypt all administrative traffic. For more information, see Authentication with the Barracuda Web Security Gateway and the Barracuda WSA.
- Bypass - IP addresses/ranges you want the Barracuda WSA to bypass when filtering.
- Proxy Exceptions - The hostname(s) or IP address(es) of these existing proxies on the client's LAN will bypass filtering of traffic. If you have a PAC or WPAD driven proxy setup, ensure that the proxy hosts are listed here.
- Allow requests when service is unavailable (Fail Open) - Behavior you want to configure for the client when the service host is unavailable. See Fail Open and Fail Closed Modes with the Barracuda WSA.

Also see Using the Barracuda WSA With the Barracuda Web Security Gateway.

Figure 1. Barracuda WSA Preferences window showing the current service host with the Barracuda Web Security Gateway.



Synchronizing Settings With the Service Host

The settings shown are those based on the last sync event between the Barracuda WSA and the service host (the Barracuda Web Security Gateway). A sync event is triggered by any of the following:

- Restarting or waking the Mac from sleep
- Logging in to another user account on the Mac
- Changing network connections or WiFi access points
- Clicking **Synchronize Settings** button in the Barracuda WSA Preferences as shown in Figure 1. **Note that you must be logged into the Mac as administrator to perform this action or to check for updates using this tool.**

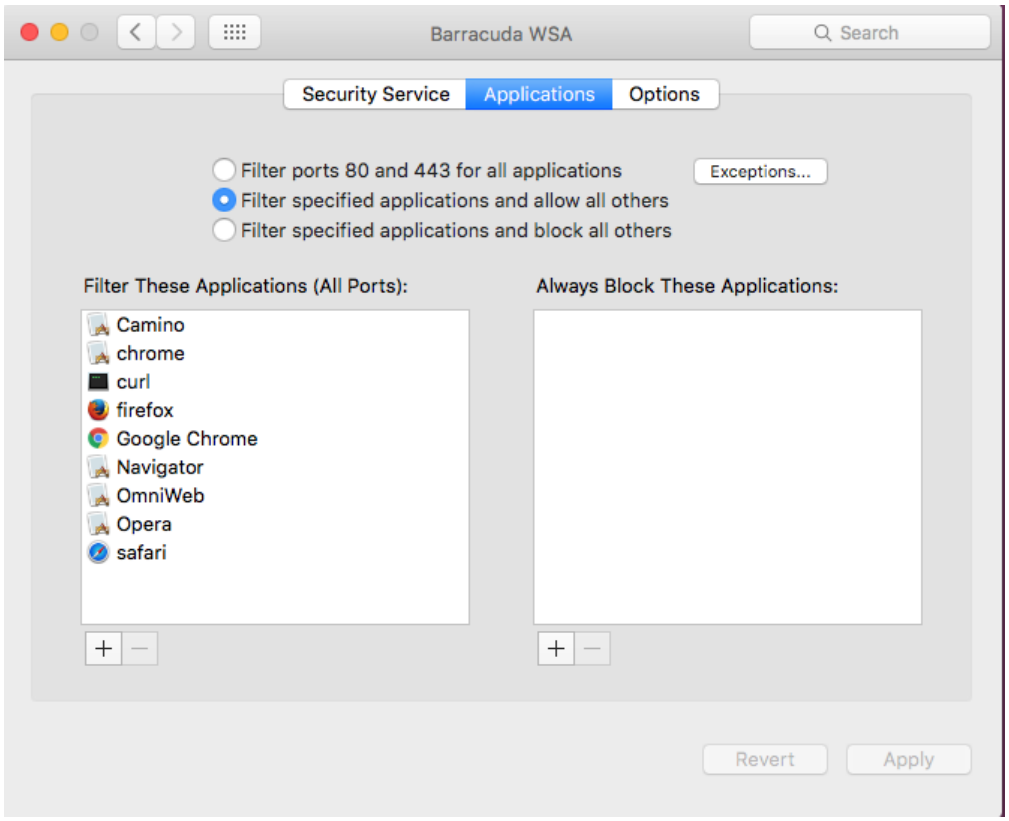
The sync event also updates the client with the following:

- Browse policies configured on the Barracuda Web Security Gateway.
- Certificate hash (see above).

Barracuda WSA Preferences

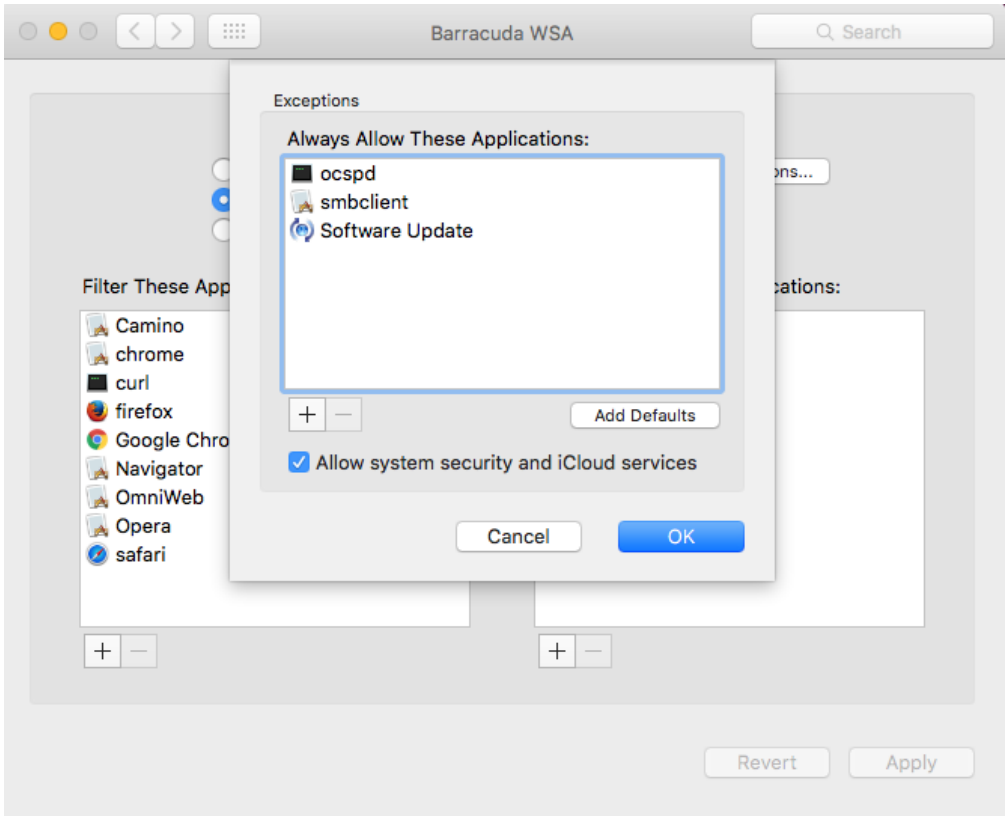
When you select **WSA Preferences** from the context menu, you see the window shown in Figure 1. Click the **Security Gateway** tab to view the current Host, Port and Bypass settings. Click the **Applications** tab to see and change filtering settings that are configured on the Barracuda Web Security Gateway **ADVANCED > Remote Filtering** page, as shown in Figure 3.

Figure 3. Barracuda WSA Applications tab.



To create exceptions to filtering policies, click the **Exceptions** button.

Figure 4. Setting exceptions to filtering policies.



To configure settings for allowing updates, click on the **Options** tab, and note the following:

Log:

The **Log** setting, by default, is set to *Nothing*. The available options are self-descriptive:

- Nothing
- Network Errors Only
- Network Errors, Policy Decisions
- Additional Diagnostics
- Everything

Allow user to Check for Updates:

- If **Allow User to Check for Update** is set to *Yes* on the **Web Security Agent** tab of the Barracuda Web Security Gateway **ADVANCED > Remote Filtering** page, then the administrator will see this option in the preferences and can manually check for updates on the Barracuda WSA client as shown in Figure 5.

Auto-update:

If **Auto-update** is set to *Yes* on the **Web Security Agent** tab of the **ADVANCED > Remote**

Filtering page, the Barracuda WSA checks daily for updates and automatically *installs them* in the background without user interaction. If the Barracuda WSA is installed on the client in *Silent Mode*, no dialog is displayed during an update; however, the log file shows that the Barracuda WSA checked for updates and whether an attempt was made to install an update. Recommended setting is setting **Auto-update** to *Yes* to ensure that the Barracuda WSA client is updated as soon as updates are available.

Check for Updates Automatically:

- This setting only applies with the Barracuda WSA and is configured on the local Mac. Check this option in the Barracuda WSA preferences (on the **Options** tab as shown in Figure 5) if you want the Barracuda WSA check for updates automatically each day on a 24 hour interval. This option does not automatically install updates.

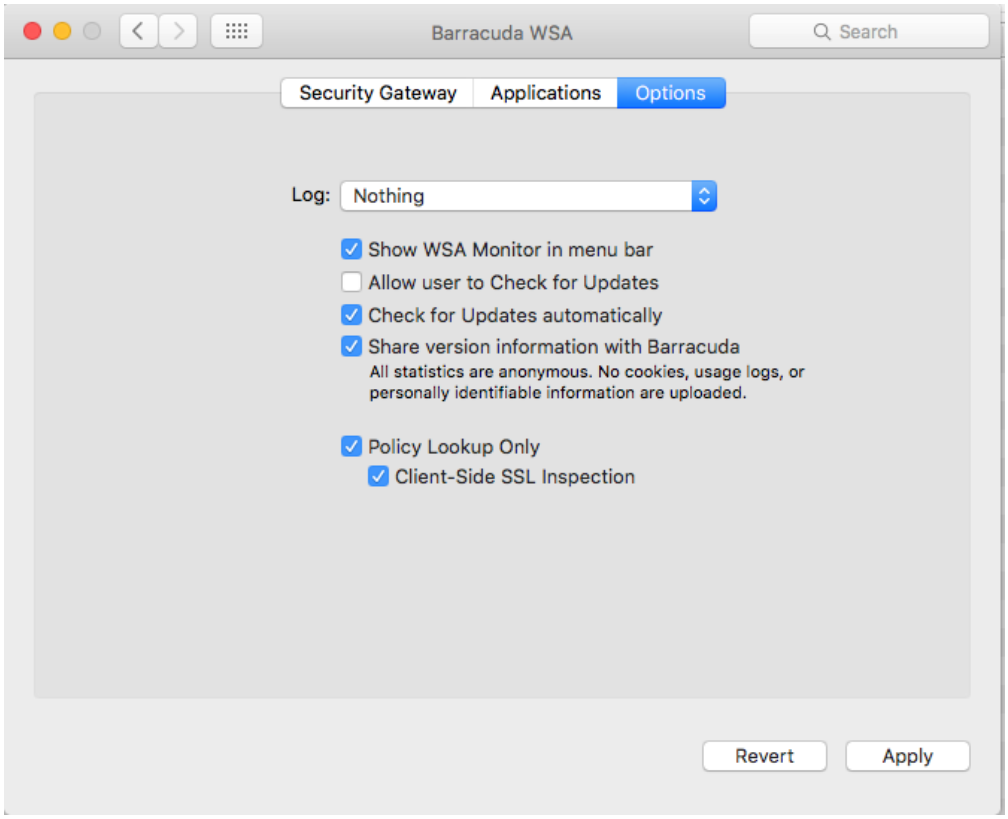
How Automatic Updates Work

- If either **Auto-update** or **Check for Updates Automatically** are enabled, then the Barracuda WSA checks for updates daily.
- If **Auto-update** is enabled on the Barracuda Web Security Gateway and an update is available, it will be installed in the background without user interaction.
- If **Auto-update** is NOT enabled and **Check for Updates Automatically** in the Barracuda WSA preferences is enabled (see Figure 5), then an "update available" dialog is displayed and the user can enter a password to install the update.

Policy Lookup Only:

When checked, the Barracuda WSA deployed on the Mac looks up policies configured on the Barracuda Web Security Gateway for that user/client, applies the policies, then routes allowed web traffic from the Mac via the usual path to the Internet. *Traffic is not routed through the Barracuda Web Security Gateway.* For more information on this feature, see Policy Lookup Only Mode With the Barracuda Web Security Agent.

Figure 5. Options tab.


Barracuda WSA
Search
Security Gateway
Applications
Options
Log:
Nothing
Show WSA Monitor in menu bar
Allow user to Check for Updates
Check for Updates automatically
Share version information with Barracuda
All statistics are anonymous. No cookies, usage logs, or personally identifiable information are uploaded.
Policy Lookup Only
Client-Side SSL Inspection
Revert
Apply

Figures