Release Notes - Barracuda Web Security Agent for Windows

https://campus.barracuda.com/doc/39815304/

What's New in Version 6.0

- Currently supported OS versions are Windows 10, Windows Server 2016, and higher. For agents running on OS versions earlier than Windows 10 or 32 bit, the Barracuda WSA will continue working on those systems, but cannot receive further updates, and installations of the new agent version will fail. T he last version to support 32 bit was 5.0.3.4.
- Improved compatibility with Cisco VPNs using UDP 443.
- No longer modifies Firefox trust store, only system trust store.
- Replaced weak password hashing algorithm (SHA1) with a stronger encryption mechanism. [BNSEC-6248]

What's New in Version 5.0

Barracuda WSA version 5 introduced exciting improvements and features to bring remote filtering into the next generation. Windows supports client side SSL inspection in PLO mode. This means no need to backhaul traffic to the Barracuda Web Security Gateway for SSL traffic control. To utilize these advanced features you must run either version 11.x or 12.x of the Barracuda Web Security Gateway. The Barracuda WSA for Windows supports Windows versions 7 and above.

Upgrading to 5.x

To use version 5.x of the Barracuda WSA for windows, there are two options for installation:

- Manually double click on the Barracuda WSA 5.x installer in Windows on the client machine, and proceed with the installation.
  - OR -
- Use the GPO installation process to install.

Important*:* Beginning with Barracuda WSA version 5.x, there are separate installers for x86 and x64 platforms. If you are running a Windows 32-bit installation, you need to download the 32-bit installer. For a Windows 64-bit installation, download the 64-bit installer. These two installers are available at https://login.barracudanetworks.com/support/downloads/ with the Barracuda WSA software as specified below.

- To get version 5.x of the Barracuda WSA, you must visit https://login.barracudanetworks.com/support/downloads/. Select **Barracuda Web Security** from the drop-down section, and download the Barracuda Web Security Agent.

- If you are upgrading from version 5.0.0.16 to a later version, you must first uninstall the Barracuda WSA, and then install the newer version.

- **Client-side SSL inspection** - Configured on the Barracuda Web Security Gateway, client-side SSL inspection offloads this processing-intensive feature to the client machine, resulting in improved overall performance of the Barracuda Web Security Gateway. See Client-side SSL inspection with the Barracuda WSA for details. This feature requires running the Barracuda Web Security Gateway version 12.0 or higher.
- **Enhanced authentication mechanism with the Barracuda Web Security Gateway** - The Barracuda WSA can use certificates you create on, or upload to, the Barracuda Web Security Gateway to verify the identity of the Barracuda Web Security Gateway and ensure that administrative traffic (configuration, policy requests, and logging) is encrypted, both on the local intranet and when roaming on untrusted networks. See Authentication with the Barracuda Web Security Gateway and the Barracuda WSA for details. This feature requires running the Barracuda Web Security Gateway version 12.0 or higher.
- The Barracuda Web Security Service is not supported for the Barracuda WSA 5.x and above.
- The SERVICE_MODE parameter for the Barracuda Web Security Gateway is now "1" instead of "2", and is now optional for command line installations (by default set to "1").
- The Tamper Protection/Watchdog feature is not supported with the Barracuda WSA 5.x and above.

Version 5.0.3.4

- Fixed issue where Win7/Win8 users saw unsigned driver system errors. [BNWSA-2769]

Version 5.0.3

- The signing certificate of the current agent expires on Jan 21, 2019. This can cause issues with installation or possibly with the agent's ability to enforce policy. This new version contains the updated certificate. [BNWSA-2762]
- In the Barracuda Web Security Gateway web interface, on the **BASIC > Remote Devices** page, there are two entries displayed with same username when **Sync** is requested from the Barracuda Web Security Agent. [BNYF-14766]. This issue has been partially resolved where there are still two entries, but one shows SYSTEM and the other shows the proper username. The final fix is pending on a fix to the Barracuda Web Security Gateway to only show one entry. [BNWSA-2465].
- Improvements on memory consumption caused by service monitoring using WMI. [BNYF-15256]
- Improvements in network monitoring for conditions where the laptop moved between networks. [BNYF-13889]

Version 5.0.2

This patch includes all fixes since the release of Barracuda WSA 5.0.0.26, and is ONLY available via https://login.barracudanetworks.com/support/downloads/. Select **Barracuda Web Security** from the drop-down section, and download the Barracuda Web Security Agent. This patch is not available via the Barracuda WSA Auto-update feature.

Known Issue in version 5.0.2: As observed *only* on Windows 7 machines: If Policy Lookup Mode (PLO) is ON with Client-side SSL Inspection enabled and google.com set as an inspected domain, accessing mail.google.com may need a manual reload to show the page content.

- Improved stability and performance.
- Performance improvements with Client-side SSL Inspection enabled.
- Addressed long load times/ parts of sites not loaded for busy pages like msn.com, espn.com, cnn.com, etc.
- Fixed application errors while the Barracuda WSA is active.
- Fixed Skype For Business NOT working in inline mode.
- Fixed issue where domain wildcards were ignored for proxy exceptions and packet capture.
- Fixed issue where auto-update was always executed, even when disabled.
- Fixed issue where Google Mail was inaccessible with Policy Lookup and Client-side SSL Inspection enabled, and Google domains set to be SSL inspected.

Version 5.0.0.26

- Fixed upgrade issues to future versions (that currently affects only EA 5.0.0.16)
- Fixes for Barracuda Web Security Gateway Authentication feature:
    - Allow Sync Settings via Barracuda WSA Configuration Tool if Authentication feature is disabled.
    - Certificate Hash is now accepted and sanitized if manually entered with colons.
- Check for Updates option is grayed out if 'Allow update' is disabled.

Version 5.0.0.25

- Improvement: Stability fixes and additions
- Improvement: Security additions around Auto-Update functionality
- Improvement: Configuration Tool fixes and web interface improvements, including configuration of the Barracuda Web Security Gateway authentication feature.
- Improvement: Periodic configuration sync every 24 hours.
- Fixed: HSTS blocked as appropriate in Firefox.
- Fixed: Barracuda Web Security Agent Icon in sys tray (non-silent user mode) now reflects the current proxy state.
- Fixed: 'Allow Remove' option works as expected.
- Fixed: Bypass Filter (Network Exceptions) needs bigger buffer size. [BNWSA-2362]

What's New in Version 4.4.7.11

- Added ability to enable Barracuda Web Security Service customers to transition to using the Barracuda Web Security Gateway.
- Enabled the Barracuda Web Security Agent to upgrade to the next major version 5.0 via the Auto Upgrade feature (Barracuda Web Security Gateway only).

Fixed in Version 4.4.7.11

- Resolved issue with password prompt errors if no password is set for Barracuda Web Security Service customers.
- Stability fixes.

What's New in Version 4.4.6

- **Ability to override use of LSP interception technology with WFP** for Windows 7 users. Choosing WFP over LSP can mitigate compatibility issues between the Barracuda WSA and 3rd party applications such as antivirus applications, resulting in better stability. You can choose WFP at installation time or using the Configuration Tool for Barracuda WSA Windows Client 4.x. Does not apply for Windows 8+, which uses WFP by default.
- Barracuda uses SHA-256 code signing for all Barracuda binaries for all supported platforms and OS versions. If you are running Windows 7 and want to be able to use WFP or Tamper Protection, you must install the Microsoft Security Advisory 3033929 security patch*. S*ome Windows 7 installations may run into difficulties when using Tamper Protection or switching between LSP and WFP drivers for traffic interception. These features will not work as expected, as Windows 7 needs the patch to trust the SHA-256 signed kernel-mode drivers.
- **Fail Open/Fail Closed trigger granularity** - Previously, connectivity (health) checks were triggered by system events including log on, sync, network address changes, etc. This version provides more granular connectivity checking based on internal connection errors, resulting in more accurate triggering of Fail Open and Fail Closed modes as well as recovery from Fail Open / Fail Closed modes.

Fixed in 4.4.6

- Fixed: Updated installer to mitigate issue of IE crashing in some scenarios. [BNWSA-1375]
- Fixed: The Barracuda WSAMonitor icon no longer appears when in silent mode when auto updated from 4.4.5.39. [BNWSA-1685]
- Fixed: Toggling the **Auto Update** state to ON no longer requires a re-login / reboot of the machine in order to be applied. [BNWSA-1799]
- Fixed: In some cases, the Barracuda WSA would go to Inline Mode, even if not behind a Barracuda Web Security Gateway. [BNWSA-1851]

What's New in Version 4.4.5

Important: When auto-upgrading on silent installation, the Barracuda WSA Monitor icon can, in some cases, show on the client after the update is complete. To avoid this issue, Barracuda Networks recommends pushing the upgrade by GPO or doing a manual installation.

- **Fail Open/Fail Closed behavior customization option -** The administrator can override the default behavior of the FailOpen/FailClosed feature in terms of:
    - Retry interval
    - Timeout of connectivity test requests

This customization option is available as an override via registry key only. The override can be pushed out to clients via GPO, and must be applied AFTER an update or installation of the Barracuda WSA has completed and the Barracuda WSA has been started up at least once on the client. For details about using the customization option, please contact Barracuda Networks Technical Support.

Fixed in Version 4.4.5

Barracuda Web Security Service Deployments

- The WSAMonitor icon state does not show as active in FailOpen or FailClose mode. [BNWSA-1635, BNWSA-1603]
- The Barracuda WSA FailOpen function behaves as expected. [BNWSA-1301]
- The Barracuda WSA gets disabled as expected when the user account profile is disabled on the **REMOTE FILTERING > Web Security Agent** page in the **Web Security Agent Central Management Activation** section. [BNWSA-1628]
- The client context menu always shows the current host on the host list. [BNWSA-1639]
- In the Configuration tool, the Service Port setting is disabled since it is configured automatically by the Barracuda Web Security Service. [BNWSA-1627]
- Save-Settings function does not fail on Fallback. [BNWSA-1404]
- High CPU usage mitigated when the Barracuda WSA is connected with the Barracuda Web Security Service. [BNWSA-1623]

Barracuda Web Security Gateway and Barracuda Web Security Service Deployments

- Fixed heap corruption issue in BarracudaWSA service. [BNWSA-1539]
- Fixed compatibility issues with VS2012 Express (WDExpress) when opening "Attach to process" dialog. [BNWSA-1542]
- Chrome.exe is not filtered if it’s not specified in the **Applications to Filter** setting. [BNWSA-1638]
- Fixed issue loading websites on Chrome browser. [BNWSA-1484, BNWSA-1558]
- WSAMonitor icon does not display after system restart when the Barracuda WSA is configured for silent installation. [BNWSA-1511]
- In the Configuration Tool, the **Service Host** field reflects changes as expected. [BNWSA-1368]

Fixed in Version 4.4.4.9

- When Central Management is disabled, WSA clients connected to the Barracuda Web Security Service do not fail open or request synchronization of the configuration every 30 seconds.
- When the WSA is installed on the client, applications connect properly to their web service as expected.