Barracuda SSL VPN Release Notes 2.6

https://campus.barracuda.com/doc/41102819/

Please Read Before Updating

Before installing any firmware version, be sure to make a backup of your configuration and read all release notes that apply to versions more recent than the one currently running on your system.

Do not manually reboot your system at any time during an upgrade, unless otherwise instructed by Barracuda Networks Technical Support. The update process typically takes only a few minutes after the update is applied. The appliance web interface for the administrator will usually be available a minute or two before the SSL VPN user interface. If the process takes longer, please contact Technical Support for further assistance.

Upgrading to Version 2.6.x

- ***When upgrading from version 2.6.1.1 (or earlier) firmware:***
  - Remote Assistance does not work in this version.
- ***When upgrading from version 2.5.0 (or earlier) firmware:***
  - Check any NAC exceptions relating to NAC Hotfix after the upgrade.
  - Backups taken from firmware 2.3.X or earlier will NOT restore properly to firmware 2.4.X and beyond, Make new backups after the firmware update.
  - The recommended size for the Web Interface Image has changed to 350x54. After upgrade existing images may appear skewed.
- ***Mapped Drives:***
  - WebDAV is now the default method for providing Mapped Drives and configuration settings have been changed accordingly. Windows 7 and Vista 64-bit clients will be prompted to uninstall the current Dokan driver and also given the option to increase the maximum file download size to 2GB when launching Mapped Drives.
  - Client Certificates need to be disabled when launching WebDAV Mapped Drives.

Firmware Version 2.6

New Features

- **Google Authenticator Support** – It is now possible to use the Google Authenticator as an authentication module for multi-factor and risked based authentication.
- **Risk Based Authentication** – Risk Based Authentication protects selected Web Forwards, Applications or SSL Tunnels with an additional authentication prompt. You can use PIN, Password or Google Authenticator authentication modules.

- **Standalone Agent** – A standalone agent is now available to download from the user portal under the **RESOURCES > User Downloads** tab. This agent contains its own Java JRE, removing the need to have JRE installed on client systems when using the agent. This also resolves previous Java version dependency issues. Security issues and warnings associated with the Java browser plugin are avoided.

Clients that do not have the Java browser plugin installed will be unable to use Key Authentication or to launch IPsec, PPTP and Network Connector from the **My Resources** page. However it is possible to provision IPsec and PPTP from the Device Configuration page. The Standalone Network Connector can be used as before.

What's new with the Barracuda SSL VPN Version 2.6.2.9

2.6.2.9 contains security vulnerability fixes only. No new features were added.

Version 2.6.2.9 Fixes:

- High severity vulnerability: unauthenticated denial of service and remote code execution [BNVS-6162]
- High severity vulnerability: unauthenticated denial of service [BNVS-6163]
- High severity vulnerability: unauthenticated remote code execution [BNVS-6181]
- Medium severity vulnerability: XSS, authenticated [BNVS-6182]
- Medium severity vulnerability: authenticated remote code execution and file creation [BNVS-6185, BNVS-6176]
- High severity vulnerability: unauthenticated denial of service [BNVS-6069]
- Fix: Updated copyright dates [BNVS-6168]

What's new with the Barracuda SSL VPN Version 2.6.2.8

2.6.2.8 is a maintenance release. No new features were added.

Version 2.6.2.8 Fixes:

- Updated hardware drivers [BNVS-6106]
- Fix: Updated copyright dates [BNVS-6108]

What's new with the Barracuda SSL VPN Version 2.6.2.7

- Improved ActiveSync stability under load [BNVS-6005]
- Updated Signing Certificate for agent [BNVS-6084]

Version 2.6.2.7 Fixes:

- High severity vulnerability: persistent XSS, authenticated [BNSEC-6188 / BNVS-6046]
- High severity vulnerability: Upgraded OpenSSL libraries to the latest versions [BNVS-6063] [BNVS-6069]
- High severity vulnerability: NGINX configuration [BNSEC-6959 / BNVS-6070]

What's new with the Barracuda SSL VPN Version 2.6.2.5

2.6.2.5 is a maintenance release. No new features were added.

Version 2.6.2.5 Fixes:

- High severity vulnerability: persistent XSS, authenticated [BNSEC-6899 / BNVS-6039]

What's new with the Barracuda SSL VPN Version 2.6.2.4

2.6.2.4 is a maintenance release. No new features were added.

Version 2.6.2.4 Fixes:

- High severity vulnerability: Removed ImageMagick from the BVS platform [BNVS-6027]
- High severity vulnerability: Upgraded OpenSSL libraries to the latest versions [BNVS-5827] [BNVS-6020]

What's new with the Barracuda SSL VPN Version 2.6.2.3

2.6.2.3 is a maintenance release. No new features were added.

Version 2.6.2.3 Fixes:

- Fix: Updated copyright dates [BNVS-6002]
- Fix: Network Connector sessions end after 2 minutes on clustered systems (Introduced in previous EA) [BNVS-6004]

What's new with the Barracuda SSL VPN Version 2.6.2.2

2.6.2.2 is a maintenance release. No new features were added.

Version 2.6.2.2 Fixes:

- Fix: Password exposure in logs when launching Mapped Drive to path with empty replacements [BNVS-5899]
- Fix: Password exposure in logs during SMB exception [BNVS-5947]
- Fix: ActiveSync can be used when User is disabled in SSL VPN [BNVS-5912]
- Fix: Multiple NTP servers are ignored [BNVS-5921]
- Fix: Mobile Portal cannot upload multiple files to network share at the same time [BNVS-5923]
- Fix: Standalone NC cannot reconnect to HA IP immediately after it switches [BNVS-5926]
- Fix: Network Connector Server Interface fails to start if a NC config has previously been deleted [BNVS-5932]
- Fix: Internal client certificates not working in IE11 due to incorrect Key Usage field [BNVS-5969]
- Fix: Client cert auth is broken in Safari on iOS 9 [BNVS-5927]
- High severity vulnerability: persistent XSS, authenticated [BNSEC-6270 / BNVS-5918]
- High severity vulnerability: unauthenticated, XSS delivered outside of the web based interface [BNSEC-6048 / BNVS-5829]
- High severity vulnerability: requires local network access, arbitrary command execution, privilege escalation [BNSEC-5160 / BNVS-5811]
- High severity vulnerability: arbitrary command execution, privilege escalation [BNSEC-4693 / BNVS-5878]
- High severity vulnerability: [BNSEC-2012 / BNVS-5942]
- Medium severity vulnerability: non-persistent XSS, authenticated [BNSEC-3880 / BNVS-5832]
- Low severity vulnerability: non-persistent XSS, unauthenticated [BNSEC-5394 / BNVS-5883]

What's new with the Barracuda SSL VPN Version 2.6.2.1

- **Windows 10 Support** – Many fixes were applied for Windows 10, for launching of clients, configuring client configurations and adding extra NAC options.

Version 2.6.2.1 Fixes:

- Fix: 2048 bit DH parameters no longer cause SSL VPN to start too slowly after an upgrade. [BNVS-5924]

What's new with the Barracuda SSL VPN Version 2.6.2.0

- **Windows 10 Support** – Many fixes were applied for Windows 10, for launching of clients, configuring client configurations and adding extra NAC options.
- **Enhanced Cryptography** – Barracuda SSL VPN now supports large Diffie-Hellman parameters and allows unlimited strength cryptography and Perfect Forward Secrecy.

Version 2.6.2.0 Features:

- **Windows 10 support**
  - Feature: Windows 10 Mobile has been added to NAC [BNVS-5871]
  - Feature: Edge/Edge Mobile browsers have been added to NAC [BNVS-5857]
  - Feature: Admin is now allowed to block IE11 [BNVS-5858]
- **Enhance cryptography**
  - Feature: Updated Java to 1.8 to support large Diffie-Hellman parameters (Logjam)[BNVS-5120] [BNVS-5886]
  - Feature: Diffie-Hellman parameters were changed from 768 to 2048 bit [BNVS-5185]
  - Feature: Unlimited strength crypto is now allowed by default [BNVS-5819]
  - Feature: Added Elliptic Curve ciphers to allow Perfect Forward Secrecy [BNVS-5885]

Version 2.6.2.0 Fixes:

- **Windows 10 support**
  - Fix: Remote assistance does now work [BNVS-5848]
  - Fix: Web launch configuration of PPTP does now work [BNVS-5849]
  - Fix: Web launch configuration of IPSec does now work [BNVS-5850]

- Fix: Device config of PPTP does now work [BNVS-5851]
  - Fix: Device config of IPSec does now work [BNVS-5852]
  - Fix: NetworkConnector web launch is now possible [BNVS-5853]
  - Fix: Mapped Drives via NetworkConnector does now work [BNVS-5855]
  - Fix: Admin agent messages are not truncated any longer [BNVS-5890]
  - Fix: Agent notifications not truncated any longer [BNVS-5896]
  - Fix: Server Agent installer is not blocked by SmartScreen any longer [BNVS-5893]
  - Fix: NetworkConnector Install Client Config does now work [BNVS-5891]
- **Enhance cryptography**
  - Fix: DH parameters for NetworkConnector were updated [BNVS-5820]
  - Fix: Web Forward to service using 2048+ bit dhparams is now possible [BNVS-5607]
  - Fix: Certificates can now be synced when TLSv1/SSLv3 is disabled [BNVS-4212]
  - Fix: Updated default cipher list to work with Firefox 39 and Chrome 45 [BNVS-5835]
- **Other**
  - Fix: Vulnerability: Allowed creating SSL tunnels to localhost [BNVS-5842]
  - Fix: Vulnerability: Access to certain server files was not restricted [BNVS-5879]
  - Fix: Windows PPP VPN configurator has been updated [BNVS-5884]
  - Fix: Device Config has been updated to work with new PPP configurator [BNVS-5898]
  - Fix: Resources did not launch with unset user attributes [BNVS-5888]
  - Fix: VPN profiles were displayed incorrectly on Windows mobile devices [BNVS-5895]

Version 2.6.1.9:

- Fix: Medium severity vulnerability: Persistent XSS in header logo URL link [BNVS-5828]
- Fix: High severity vulnerability: OpenSSL CVE-2015-1793 alternate chains certificate forgery [BNVS-5827]

Version 2.6.1.8:

- Fix: Medium severity vulnerability: Updated OpenSSL to 1.0.1m to address FREAK (CVE-2015-0204) [BNVS-2955]
- Fix: Low severity vulnerability: Persistent XSS in your Barracuda SSL VPN Firmware - Username Field. [BNVS-5792]
- Fix: Removed NTP daemon as no longer required
- Fix: Threading issue with RADIUS challenge authentication [BNVS-5783]

Version 2.6.1.1:

- Feature: New Standalone Agent.
- Fix: NAC HotFix checking is only performed if required [BNVS-5470]

- Fix: Low severity vulnerability: SSLVPN no longer uses insecure JQuery UI Library [BNVS-5390]
- Fix: Network Connector client launches correctly when client name contains non ASCII characters [BNVS-5422]
- Fix: RADIUS Access-Challenge response is interpreted correctly [BNVS-4002]
- Fix: Server Agent and ActivSync now appear on the Session Types graph when French language is selected [BNVS-4640]

Version 2.6.0.2 Fixes:

- Fix: Notifications are not emailed to users in disabled user databases [BNVS-5281]
- Fix: Improvements to UI [BNVS-5400, BNVS-5386]
- Fix: Improvements to Operating System NAC checking [BNVS-5409]

What's new with the Barracuda SSL VPN Version 2.6.0.1

- Improvements to available NAC OS detection.
- Option added to allow Desktop or Mobile UI on mobile devices.

Version 2.6.0.1 Fixes:

- **Mobile Portal**
  - Fix: Clearer indication of required input fields on Mobile Portal for PIN logon [BNVS-5250]
  - Fix: Mobile Portal login page is displayed correctly when Site Name contains an apostrophe [BNVS-5250]
  - Fix: Usernames are not case-sensitive with OTP authentication on Mobile Portal [BNVS-5200]
  - Fix: Network Places to hidden shares can now be accessed from Mobile Portal [BNVS-5247]
  - Fix: Login screen Message Text is not displayed when Message Type is set to None [BNVS-5213]
- **WebDAV**
  - Fix: Failed WebDAV client login attempts cause account to be locked [BNVS-5262]
  - Fix: Improved WebDAV privacy issues [BNVS-5268]
  - Fix: WebDAV shares can be launched in Windows 7 Explorer [BNVS-4384]
- **NAC**
  - Fix: The Reset Password button now disables NAC checking for the Administrator instead of generating NAC exceptions [BNVS-5133, BNVS-4988]
  - Fix: MAC Address, IP Address and Microsoft Knowledge Base NAC Exceptions can be created with a wildcard type [BNVS-5258, BNVS-5259]
  - Fix: Cancel button closes the NAC Exception Lookup window [BNVS-5199]

- ○ Fix: NAC checking now works with Java 1.6 and 1.7 [BNVS-5304]
  - ○ Fix: When launching a Network Place, the number of sessions are now correctly shown in ACCESS CONTROL > Sessions. [BNVS-5068]
- **IPsec**
  - ○ Fix: IPsec connection is created for usernames containing whitespace [BNVS-5211]
  - ○ Fix: IPsec and PPTP launches in non-English Windows [BNVS-5260]
- **Other**
  - ○ Fix: Web Forwards using NTLM authentication launch correctly [BNVS-5251]
  - ○ Fix: Server Agent improvements on macOS. [BNVS-51]