AVAYA

Release Notes
Avaya VPN Gateway

Contents

Chapter 1: Release Notes

This document describes the new features and enhancements introduced in this release. It also provides details on the software installation, upgrade instructions, supported hardware, licenses, and limitations in software for the Avaya Virtual Private Network Gateway.

For a list of related publications, see Related documentation on page 41. The documentation suite for Avaya Virtual Private Network Gateway can be found on the documentation CD included with the software or on the Avaya Web site http://www.avaya.com/support. For more information, see How to get help.

The following topics are discussed in this document:

Chapter 2: Licenses

The following licenses are available to enhance the capabilities of the Avaya VPN Gateway software.

- SSL/IPsec License
- IPsec User License
- Secure Service Partitioning License
- Portal Guard License
- Demo License
- Emergency Recovery Access (ERA) License
- Secure Portable Office License

For information on these licenses see, BBI Application Guide (NN46120-102) and CLI Application Guide (NN46120-101).

Licenses

Chapter 3: New in this release

The following enhancements are included in included in Release 8.0.5.

Port forwarder applets support for IE 64-bit browser on Windows Vista 64-bit, Windows 7 64-bit and Windows XP 64-bit OS (wi00571517).

Nortel Health Agent 64-bit OS support from NHA 5.3.0 version (wi00692331).

Updated with new signing certificate as the current signing certificate is about to expire. (wi00822198 and wi00822209)

New in this release

Chapter 4: Documentation download

Avaya VPN Gateway documentation is available for download from the Customer Support website:

1. Point your browser to: http://support.avaya.com .
2. To download you must do one of the following:

   Click Register and follow the registration instructions.

   Click Sign In and enter your login credentials.

   Once you are registered or signed in the support pane appears.
3. Select Documentation then select Documentation Library.
4. Select the desired document from A-Z list.

Documentation download

Chapter 5: Software installation and upgrade notice

SSL VPN Server software

The SSL VPN server software is delivered in two different forms, as described following:

- **`SSL-8.0.5.0-upgrade_complete.pkg`**

  This package is the preferred method for upgrading an existing SSL VPN cluster, as the upgrade is propagated across the cluster and all current configuration is preserved.

  The upgrade procedure is described in "Performing Minor/Major Release Upgrades" in Chapter 4 in the *VPN Gateway User's Guide*.

  ### ✳ Note:
  TFTP cannot be used when upgrading to version 7.0.1 or later from an earlier version.

- **`SSL-8.0.5.0-boot.img`**

  This image resets the VPN Gateway to its factory default configuration. It must be used when a VPN Gateway with a different software installed is to be added to a cluster, to bring the additional device to the same software version as in the cluster before joining it to the cluster.

  The software reinstall procedure is described in "Reinstalling the Software" in Chapter 3 in the *VPN Gateway User's Guide*.

  ### ✳ Note:
  TFTP cannot be used when installing version 7.0.1 or later through the reinstall procedure.

- **`SSL-8.0.5.0-auto-install.iso`**

  This image resets the VPN Gateway to its factory default configuration. The image is used for CDROM installation. The software tries to detect the hardware automatically, and if the software finds the hardware a supported one, it starts the installation automatically. This software is useful for the Avaya VPN Gateway (AVG) VMware Appliance installation.

Server software download

The server software is available for download from Avaya Customer Support website. The following is the procedure to access the site:

1. Go to the Avaya Technical support website http://www.ayaya.com/support

2. To download software you must do one of the following:

   Click Register and follow the registration instructions.

   Click Sign In and enter your login credentials.

   Once you are signed in or registered the support pane appears.

3. From the list on the left side of the support pane click Downloads

   A dialog box appears.

4. In the dialog box, do one of the following:

   Enter your product name

   Click the A-Z list, click a letter from the selections, and select your product from the list.

   The product support page appears.

5. From the list on the left side of the product support pane, click Downloads.

   The software downloads dialog appears.

6. Click the link that appears beneath the software downloads dialog, for example: VPN Gateway 3050 Downloads.

   The product download page appears.

7. On the product downloads page, click the Downloads tab.

   A list of available downloads software appears.

8. Click a software file to download and follow the instructions on the screen.

Nortel SSL VPN client

The manually installable SSL VPN transparent client software is available on request. Contact Avaya Support.

The SSL VPN client comes in two versions (for limitations, see Nortel SSL VPN Client on page 27):

- Version 1.1.0.4 (LSP client): Compatible with Windows 98, ME, NT (with IE 5 or later) 2000 and XP

- Version 1.5.0.16 (TDI client): Compatible with Windows 2000 and XP

Nortel VPN client (formerly Contivity)

The VPN client software can be downloaded from Avaya's Customer Support website. Nortel VPN Client 10.0x supports both IPSec and SSL.

Nortel Net Direct installable client

The Net Direct SSL VPN installable client software can be downloaded from AVG server when an internal link pointing to the server is created by the administrator. For example, https://VIP/ nortel_cacheable/NetDirect_Setup.zip.

Disk repartitioning for upgrade or downgrade from Release 7.x to 8.0.5

To support the disk repartitioning for upgrade or downgrade from Release 7.x to 8.0.5 on AVG 3050 and 3070, the following commands are used:

- `/boot/repartition`

  Initiates repartitioning for the local host.

- `/cfg/sys/host <id>/repartition`

  `/cfg/sys/cluster/host <id>/repartition`

  Initiates repartitioning for the given host (which must be running).

These commands are hidden and are not shown in the menu or considered for auto-completion through <TAB>, they cannot be used in normal operation. Repartition includes two automatic reboots, the host is effectively out of service. The time required for the repartition is approximately 5 to 7 minutes.

Upgrading from versions earlier than 2.0.11.15

If you are currently running a software version earlier than 2.0.11.15, upgrade to version 2.0.11.15 (or a later 2.0.11.x version) prior to upgrading to version 6.x. The "intermediate" upgrade to version 2.0.11.15 is necessary to maintain your current configuration, and to provide reliable fallback in case the upgrade should fail.

Downgrading to versions prior to 5.1.5.4

AVG clusters running software version 7.0 or later cannot be downgraded directly to software versions prior to 5.1.5.4. This is due to changes in the internal database format. To downgrade such a cluster to a version lower than 5.1.5.4, first perform an intermediate downgrade to 5.1.5.4 (or later 5.x).

Downgrading to 5.1.5.4 or later

- If a ClearTrust authentication scheme has been configured, downgrading to a version prior to 6.x will fail. Delete the ClearTrust authentication scheme before downgrading.

- In version 6.x, several IP pools may exist for a VPN. In version 5.x, only one IP pool per VPN may exist in the configuration. On downgrading from 6.x or later to 5.1.5.4 or later 5.x, the settings for the default IP pool in the 6.x configuration will be kept in the 5.x configuration, provided the default IP pool is of the type `local`. The Net Direct and IPsec network attributes are configured accordingly. If the default IP pool in the 6.x configuration is not of the type `local`, the first found local IP pool (lowest number) is selected to form the IP pool in the 5.x configuration. If no local IP pool is found, the IP pool will be disabled in the 5.x configuration.

- The Tunnel Guard features introduced in 6.0.1 will be filtered out during the downgrade.

- If Net Direct, IE Wiper and/or Citrix Metaframe support is set to `group`, the setting is changed to the respective default value.

- The Tunnel Guard predefined SRS entries will be lost, if the software is downgraded from 7.0.x release to 6.0.x or 5.1.x release. The predefined SRS is introduced for the first time in 7.0.x as OPSWAT feature. It is recommended to delete the predefined SRS entries from TG SRS rule definitions before downgrade.

- During upgrade and downgrade, the cached version of TG admin applet can be invoked. It is recommended to delete the browser cache.

• Single Tunnel Guard SRS data cannot have more than 255 predefined software entries.

• Due to changes in RADIUS accounting server information in the configuration. Downgrade to 6.0.x and 5.0.x release and upgrade to 7.0.x causes RADIUS server information inconsistency. Administrator must re-configure the RADIUS account server again once upgrade back to 8.0.5 again.

Reload license after upgrade

In version 6.0.1, the default license has been increased from 10 to 50 concurrent users, for SSL and IPsec connections. On upgrades from earlier versions where additional licenses (besides the default license) have been loaded to the devices, the additional license must be reloaded to make use of the extra 40 number of users in the default license.

Downgrade IE Cache Wiper Cab, Net Direct Cab, and SODP ActiveX files

If the server is downgraded, the upgraded version will not be cleaned up. That is, the object files, the IE cache wiper, Net Direct and SODP files are the original upgraded version. You have to manually delete the IE Wiper Control cab, Net Direct cab and SODP activeX files. Follow these steps to delete the files:

1. Open Internet explorer.

2. From the **Tools** menu, select **Internet Options**.

3. Click **Settings**.

4. Click **View Objects**.

5. Select the files and remove.

Chapter 6: Supported hardware platforms

The AVG 8.0.5 server software is supported on the following hardware platforms:

- VPN Gateway 3050
- VPN Gateway 3070

Supported hardware platforms

Chapter 7: Resolved issues

This section lists the CRs/WIs resolved in release 8.0.5:

- Heart Restart Due to ESP4_NSP Crypto Driver Lock (wi00728718)

- Generic server sync_nodes_server terminating (wi00822127)

- Release of the client IP back to the corresponding IP Pool whenever the user logs out is optimized (wi00700829)

- AAA session migration code block profiling and optimization (wi00700832)

- Incorrect parsing of the HTTP header field in case of IF header on PUT requests leading to insertion of extra "<" sign (wi00595398) (Q01994974-01)

- All non-IE browsers (Chrome, Firefox, Safari, Opera, etc) fail to evaluate the rewrite of 'windows.location.href'. (wi00595412) (Q02158861)

- [BBI] Cluster >> Host menu heading shows VPN Gateway 7.0 Host(s) instead of actual Host (wi00568376) (Q02133796)

- Q02112506 (wi00568356) breaks AJAX-SCRIPT re-write (wi00729593)

- Attempting to Edit/Save Bookmarks Corrupts Stored URLs (wi00732494)

- WTS screensize does not work when hidepf on (wi00568120) (Q01957891-01)

- New Cluster Members CLI Accts Not Synced (wi00595404) (Q02155585)

- TG SRS Default Rulesets Do Not Detect Varying NOD32 Antivirus Installations (wi00570495) (Q01793501)

- Adminstrative authentication fails after upgrade (wi00571485) (Q02110403)

- Not able to download Net Direct setup file from BBI VPN Gateways >> VPN-# >> VPN Client >> Net Direct. (Q01848065)

- MSCHAP session setup failure with L2TP and LDAP. (Q02117163) (wi00568371)

- Administrative authentication fails after upgrade. (Q02110403)

- JavaRDP WTS "License Error" Dialog w/ Windows Server 2008. A new CLI /cfg/vpn #/linkset #/ link #/wts/winostype is added to start the corresponding javaRDP client. It takes one of the following options – Windows and Windows 2008. The default value is Windows. (wi00571525) (Q02130505)

- Domino Web Access WARNING pop-up (wi00568231) (Q02053509)

Resolved issues

Chapter 8: Known limitations

VPN limitation

VPN Gateway Release 8.0.5 supports 256 VPNs, even though the CLI and Web UI allows you to create 1024 VPNs. Therefore, the user should create up to 256 VPNs only.

Avaya VPN Gateway can support up to 300,000 CRL retrievals per host at any given time. No multiple retrieval schedules or manual actions can run concurrently.

Browser requirements

The following browsers are recommended while using theAVG software for basic Portal access, that is when not using the applets:

Basic Portal Access (no applets)

When using the AVG software for basic Portal access, that is when not using the applets, the following browsers are recommended:

- Internet Explorer 5 or later
- Mozilla 1.1 or later
- Netscape 4 or later
- Firefox 2.0
- Safari 2.0

Applet support

To support the Telnet/SSH Access, HTTP Proxy, FTP Proxy, Port forwarder applets (available on the Portal's Advanced tab) and the Citrix Metaframe applet, the following browser and Java combinations are recommended:

- Windows

    - Internet Explorer 5 or later with Sun's JRE 1.4.2 or later
    - Internet Explorer 64-bit on Widows Vista, Windows 7 and Windows XP 64-bit OS for port forwarders.
    - Mozilla 1.5 or later with Sun's JRE 1.4.2 or later
    - Firefox with Sun's JRE 1.4.2 or later

- Unix/Linux

    - Mozilla 1.5 or later with Sun's JRE 1.4.2 or later
    - Firefox with Sun's JRE 1.4.2 or later

- Mac OS X

    Safari 2.0 with Sun's JRE 1.4.2 or later

Nortel Health Agent Applet support

To support the Nortel Health Agent SSL applet (used for checking the client machine), Internet Explorer 5.5 or later is recommended.

The following browsers support the Tunnel Guard management applet (used for configuring SRS rules):

Windows

    - Internet Explorer 5.5 or later
    - Netscape Navigator 7.1 or later
    - Mozilla 1.5 or later
    - Firefox 2.0

- Java 1.4.2 or later is required

BBI support

Configuration through the Browser-Based Management Interface (BBI) is supported when the following browsers are used:

• Windows

    - Internet Explorer 5.5 or later

    - Netscape Navigator 7.1 or later

    - Mozilla 1.5 or later

    - Firefox 2.0

• Unix/Linux

    - Netscape Navigator 7.1 or later

    - Mozilla 1.5 or later

Secure Portable Office client

• The Secure Portable Office (SPO) client is supported on the following browser and platform combinations:

    - Windows (2000, XP, Vista, and 7) 32 bit operating system in virtualized and native environment.

    - Windows (XP and Vista) 64 bit operating system in native environment.

• The SPO application Virtualization mode supports SmartCard based certificate management using Virtualized Aladdin PKI Client software only when E-Token NG-FLASH 72 KB (Java Virtual Machine) is used. The E-Token NG-FLASH 64 KB (Siemens CardOS) cannot be used to manage client certificates from SmartCard using Virtualized PKI Client software. This is due to the incompatibility with generic USB CCID driver (usbccid.sys). The E-Token NG-FLASH 64 KB. It can work only with proprietary SmartCard reader driver and they are not available in Windows operating systems. Application virtualization does not support virtualization of drivers. Hence, Aladdin PKI client must be installed in the host PC to manage the client certificates if E-Token NG-FLASH 64 KB is used for SPO Client. (Q02030468)

• In FireFox browser, the E-Token keeps prompting for password input even if the client certification is disabled.

• A maximum delay of 30 seconds can be set after the idle timeout is over to log out an SPO client.

Net Direct client

The Net Direct client is supported using the following browser and platform combinations:

- Internet Explorer on Windows (XP, Vista, and 7) 32 bit OS
- Firefox on Windows (XP, Vista, and 7) 32 bit
- Internet Explorer 32 bit version on Windows (XP and Vista) 64 bit OS
- Firefox 32 bit version on Windows XP 64 bit
- Safari 2.0 on Mac OS version 10.4 and 10.5

The following Linux distributions have been verified to support Net Direct and Firefox:

- RedHat 7.3, Kernel 2.4.18
- RedHat 9.0, Kernel 2.4.20
- Knoppix 4.0.2, Kernel 2.6.12.4
- Fedora Core 2, Kernel 2.6.5
- Fedora Core 3, Kernel 2.6.2
- Fedora Core 4, Kernel 2.6.11
- SUSE 10.0, Kernel 2.6.16

✳ **Note:**
Other distributions work if they have a tun driver.

Other limitations

- The installable Net Direct client is not available for Linux and Mac OS X
- Caching of Net Direct components is not supported for Linux and Mac OS X
- Mobility Feature is not supported for MAC and Linux platforms
- If Net Direct is disconnected in improper way, restoration of DNS will fail. Few improper ways of disconnecting the Net Direct that a user should avoid are:
  - Closing the portal browser when Net Direct is On.
  - Clicking the Close (X) button in the title bar of the applet when Net Direct is On.

Nortel Health Agent

Version TG_1.1.2.0_001 of the installed Tunnel Guard agent is the minimum requirement for use with the VPN Gateway. Nortel Health Agent is the suggested product upgrade path for the Tunnel guard agent.

Special notice for customers using both Nortel VPN Gateway Release 7.0 or later and NSNA Release 1.6.1 products

The installable Nortel Health Agent 4.0 client shipped with this release does not have all of the functionality contained in Nortel Health Agent 3.5 that was shipped with NSNA 1.6.1 Customers who need complete NSNA 1.6.1 and AVG 7.0 functionality should use version 4.5 of Nortel Health Agent which includes the full functionality of both releases. Customer can get the software through their normal support channels.

Nortel VPN Client (formerly Contivity VPN Client)

Nortel VPN client versions 5.x, 6.x, 7.x, and 10.x are supported.

Nortel SSL VPN Client

- The installable SSL VPN client comes in two versions:

    - Version 1.1.0.4 (LSP client): Compatible with Windows 98, ME, NT (with IE 5 or later), and XP. This client does not support UDP.

    - Version 1.5.0.9 (TDI client): Compatible with Windows 2000 and XP. This client supports UDP as well as TCP. Native Microsoft Outlook is not supported because not fully qualified domain names cannot be resolved.

- The AVG software includes commands for allowing/rejecting access for certain SSL VPN clients, based on client version and which operating system the client currently runs on. These commands have been added as a preparation for future releases of the TDI/LSP clients, where the clients will be capable of sending version number and OS version to

the AVG. Until the new TDI/LSP clients are released, existing TDI/LSP clients will be regarded as "old clients".

- CLI path:

    `/cfg/vpn #/sslclient/tdiclient` and `lspclient` (these commands currently have no effect) and `cfg/vpn #/sslclient/oldclients`

- BBI path:

    VPN Gateways >>VPN Client >>TDI Client and LSP Client (these options currently have no effect) and **VPN Gateways >>VPN Client >> Old Clients**.

Portal

- Proxy chaining (option to specify an intermediate HTTP Proxy host and port, for example for the Portal's Telnet/SSH and Custom Port forwarder features) is only supported if SSL is enabled on the portal server.

- Proxy chaining is not supported for the Outlook Port forwarder feature.

- Microsoft Outlook 2003 is not supported when using the Outlook Port forwarder in combination with Exchange 2003.

- Running the Outlook Port forwarder on a Windows 2000 client requires installing the latest service pack for the operating system.

- Applications using dynamic UDP port number allocation (for example NetMeeting, FTP and all streaming media) are not supported by the Port forwarder feature. Applications using static port number allocation (for example DNS, SNMP) are supported.

- When specifying a URL without a path for an iauto (automatic login) link, for example http://www.example.com, enter the URL as `http://www.example.com/`. This will ensure that the root path is implied in the link. Iauto links are created using the `/cfg/vpn #/linkset #/link #/iauto` command.

- When an iauto link should be used for login to web servers using two-tier basic authentication with domain (that is one field for domain\user and one for password), the `/cfg /vpn #/linkset #/link #/iauto/mode` command must be set to `add_domain`.

- Creating a Port forwarder link for mapping a network drive is not supported on Windows 7, 98, XP, and Vista clients.

- The features available on the Portal's Advanced tab (that is Telnet/SSH access, HTTP Proxy and Port forwarder) are supported only with SSL v3 and cipher type RC4-MD5.

- The features available on the Portal's Advanced tab are not supported for the TLS protocol.

- To create a Port forwarder link for mapping a network drive – and the link is to be used on a Windows 2003 server acting as client – port 445 has to be used instead of the suggested port 139. On the Windows 2003 server, port 445 should be disabled by following these steps:

    - Click Start, select Run and enter `regedit`. The registry editor is started.

    - Locate and select the following key: `HKLM\System\CurrentControlSet \Services\NetBT\Parameters`.

    - On the right panel, double-click the `TransportBindName` entry.

    - In the Edit string dialog, delete the displayed value. No value should be specified.

    - Click OK, exit the registry editor and restart the computer.

- Some SSH versions may not be supported when using the SSH feature on the Portal's Advanced tab, for example Alteon 184 SSH-1.5-1.2.27.

- Some of Microsoft's Telnet server versions may not be supported when using the Telnet feature on the Portal's Advanced tab.

- If a Windows XP system is not upgraded to Service Pack 2, and you want to create a WTS Port forwarder link that works on that system, follow these steps:

    - Configure the Port forwarder to listen on 127.0.0.2 instead of 127.0.0.1 (localhost).

    - Configure the Remote Desktop client to connect to 127.0.0.2.

    In Windows XP SP2 Remote Desktop client, you can connect to 127.0.0.1 (localhost) if the used port is other than the default (3389). Windows XP SP2 Remote Desktop client does not support connections through 127.0.0.2.

- JVM 1.5 and later includes support for using the browser's certificate database. If the AVG is set to ask for client certificates, any Java applet started during a Portal session may display a window asking for a client certificate, even though the user has already logged in to the Portal with a client certificate. The solution is to click Cancel without selecting a certificate.

- Some web applications, if started, takes over existing instances of Internet Explorer, which may cause problems for the Portal session. For example, if the Portal page is reused by a web application and the Net Direct client is running, the client will be shut down. To solve this problem in IE, go to Tools>Internet options. On the Advanced tab, under Browsing, disable the setting "Reuse windows for launching shortcuts".

General

- A maximum of 32000 sessions is allowed on the VPN Gateway 3070 with 2 GB RAM.

- The license is not part of the configuration and is also not included when exporting the configuration using the CLI command `/cfg/ptcfg`. If a configuration is deleted, the license is also deleted.

- When using the IPsec VPN client together with the installed Tunnel Guard agent, the result of the Tunnel Guard check cannot lead to an IP address being allocated from an IP pool that is assigned to an extended profile. This is because the IP address has to be allocated before the Tunnel Guard check is run.

- Multiple clients behind the same NAT device cannot make simultaneous L2TP/IPsec connections.

- If you run Port forwarder from SPO Client, and use Firefox browser, you cannot click the Stop button to close the Port forwarder window; the button is disabled.

- L2TP/IPsec client cannot connect to backend servers which are behind the same NAT device with AVG.

- AVG does not support running multiple virtual desktop in the same end-user PC.

- Siteminder authentication does not act as expected while crossing a realm with a lower protection level to another realm with a higher protection level. (Q01351656-01)

Chapter 9: Known issues

This section lists the known issues with the AVG software. See the following topics:

Net Direct

- When running Net Direct on Knoppix, the tun device node must be set up manually. (Q01281449)

  To set the tun node, run the following commands as root:

  ```
  mkdir /dev/net mknod /dev/net/tun c 10 200
  ```

- When running Net Direct on Linux, root must be enabled on the remote user's machine and the administrator must see to it that the user account is authorized to use the command `su root`. (Q01278965)

- Net Direct on Windows may not be compatible with some internet security software for clients. This is expected to be fixed in the future patch releases.

- On Linux (SUSE 10.0) and Firefox, while starting Net Direct from the Portal, the message "Net Direct already running" appears in the Java applet window although the Net Direct is not started. When this error occurs, the Net Direct cannot be started.

- In Net Direct, if the administrator password configured on the AVG does not match the Windows PC client password, the browser closes sometimes.

- If the remote user runs an old version of installable Net Direct client, there is no message displayed to upgrade or continue the old version. This will be fixed in future releases.

- While using Virtual Desktop, downloadable Net Direct cannot be connected. (Q01546498).

- When using Net Direct in Windows 2000 with 2 NICs and one NIC becomes disabled, there is an issue in reconnection for Net Direct. (Q01619895)

- The Siebel portal does a client check before the application loads but fails if it is run through proxy. The application works correctly if it is connected through Net Direct and

after passing the client check through Net Direct, the site can be used through proxy without any issues. (Q01464430)

- If the Net Direct client is unable to establish a UDP transport session with the VPN Gateway and automatically initiates a fallback to TCP-mode, this mode is unusable on any Linux and Unix based platform (wi00833183)

- If the UDP-mode is unavailable, the Net Direct client will fallback to TCP-mode. However Net Direct client will keep checking for UDP-mode. If UDP connectivity is restored, Net Direct will drop its TCP-mode connection and send traffic via the UDP based tunnel. This fails and results in a non working tunnel. Net Direct must be shut down and reconnected in order to re-establish a working tunnel. (wi00833200)

- The "/cfg/vpn #/sslclient/udpports 0-1" option has no effect on any Unix and Linux based platforms (wi00833202)

- The Net Direct log on MAC OSX and all Unix and Linux based platforms will grow in size over time resulting in a very large log file (wi00833191)

Portal

- When HTTPS is used, Internet Explorer version 7.0.2800.1106.xpsp2_gdr. 040517-1325. does not allow downloading or saving a file in the system (for example, files with extension .txt, .exe, .zip) though the SSL VPN server HTTP setting of **addnostore** is set to **off**.

- Outlook 2003 client does not work through native outlook Port forwarder. (Q00757505)

- maxPwdAge attribute is returned before presenting a password\account expiry message to the portal user. (Q01244929)

- In Windows Vista, if you configure the proxy entry using IP address, the Internet Explorer crashes while launching port forwarders. (Q01852590)

- When a user:

    - creates a OWA link,

    - sets the `cookiedb` to **on** in the AVG, and

    - clicks on the OWA link in the portal

  iauto OWA link is not logged in automatically. The system requests for the user name and password. (Q01889808-01)

- Turn off the `cookiedb` when used with Citrix and OWA. **/cfg/vpn/*/server/ portal/cookiedb off**

Secure Portable Office and Portal

- When the usage time increases, the system tray interface tool tips freeze and do not sync with the Dashboard interface status tab. (Q01848465)

- After starting the SPO client and launching the Virtual Desktop, the connected profile is not shown in the Dashboard status tab in the Virtual Desktop mode. (Q01849156)

- Symantec On Demand Protection (SODP) has an option called Secure Mode. Secure Mode is designed to support the default web browser that comes with SODP and to disallow other applications. Secure Mode provides application isolation from the host PC by preventing any local applications from running inside the virtual desktop. With Secure Mode on, the end user will see error messages when the SPO client starts and when the user clicks on any SPO links. SPO client and SPO links will work but the user experience will interrupted by error messages. Customers may decide to run with Secure Mode off and enable SODP File Separation in order to prevent information from being saved to the PC in this scenario. (Q01885125 and Q01870880)

- The SPO client auto update feature is not compatible with CDROM deployment because CDROM is read only memory. TG may fail to start inside Virtual Desktop on Windows Vista (SPO CD-ROM image only. (Q01886811)

- Some Portable Apps launched from SPO do not close when SPO is logged out/exited. (Q01892159)

- Even though many links are available in the linksets, only the first 16 links are shown in the system tray menu. (Q01833490)

- When using SPO with client certificate based authentication, Net Direct is not available in conjunction with Virtual Desktop. (Q01899418)

- The SPO dashboard does not display the linkset changes in the AVG server. To view the changes, logon to the SPO again. (Q02032747)

- In Virtualized mode, Ceedo exits when the SPO Client exits. After exiting, if user tries to upgrade it, the SPO Client software auto upgrade fails. (Q02034025)

- In Virtualized Mode, error message "Authentication failed due to revoked certificate" does not appear if the selected client certificate is incorrect. (Q02036250)

- While running HTTP proxy or Port forwarder, SPOClient window cannot be closed by clicking on stop http proxy. This happens both in Virtualized and Native mode. Click window terminate to close the SPOClient. (Q02040837)

- In SPOClient, Tunnel Guard check fails, and error error server logout appears when user logs in as Tunnel Guard group user. (Q02033013)

  Workaround:

  Use cache wiper to delete the cached file.

- The E-Token always prompts for token password even when Cert authentication is used and SSO is enabled. The request for password appears whenever BBI is launched using E-Token USB. (Q02042591)

- Net Direct fails to establish connection with AVG when it is launched on CD-ROM SPOClient. An error message Failed to install TAP Adapter for Netdirect Client appears. (Q02042248)

- ActiveX Citrix ICA is not supported with IE8 and SPO Application Virtulization mode. The Firefox with Java Applet Citrix ICA can be used instead. (Q02040046)

- Change Password option is not disabled for client certificate authentication. (Q02050856)

- If IE8 browser is used, and user does not have Administrator privilege in PC, then the internal, http proxy, and portforwarder links do not work in the native SPO.

  workaround

  Use Firefox browser.

- SPO with Application Virtuliazation mode does not support Port forwarder host mapping feature. (Q02040815)

Browser-Based Interface

- The output for command `/maint/starttrace` is not available in WebUI. (Q01475271)

- When the system time in the Minute list box (Cluster>Time) is changed to 15 or a higher value an error message appears and the BBI hangs. This issue is expected to be fixed in the future patch releases. (Q01341831)

- After checking AVG configuration using, Diagnostics » Maintenance » error in test is displayed. (Q01688298)

- Monitor takes long time to load data when more number of users are logged into the VPN. (Q01819115)

- The license usage excel sheet created through Cluster Manager does not include the Virtual Desktop license usage count. (Q01846455)

  To view the Virtual Desktop license usage, enter the following:

    - BBI path

      Monitor >> License Usage

    - CLI command:

      info/licenses

- CLI validates the integer in the Net Direct banner/license but BBI does not. (Q01447773)

- urlobscure breaks Citrix Java client connection through web interface. (Q01692215-01)

- When a certificate is created as Other (UPN) with email option and Subject Alternative Name is configured to fetch the General name as email, the AVG always picks the username from the Other. (Q02055990)

- The NOT SRS rules cannot be created with single available expression. (Q02032736)

- The Rule Definition tab does not display newly created rule definitions. To view the definitions, save and close the administration applet and then relaunch the applet. (Q02040320)

- The NHA Rule Definitions menu and tabs behave inconsistently and incorrectly. (Q02040322)

- The NHA trigger command does not accept Windows environment variables. For example, %windir%,%programfiles% and other windows environment variables. (Q02040327)

- The digital signature on trusted certificate is expired. When user opens Config >> Cluster Manager, and launches an applet, a popup appears stating "The application's digital signature has an error. Do you want to run the application?" Click Run to launch the applet. The applet does run, but an error message appears stating "The digital signature was generated with a trusted certificate but has expired." (Q02058170)

- In Tunnel Guard admin applet, the sub tabs of the Rule Expression get disabled when user assigns same rule expression for different rule definitions using the Assign to... option. (Q02062516)

Command Line Interface

- After connecting to AVG using Net Direct for a Tunnel Guard enabled user, recheck does not happen in some cases. Later, when the recheck happens, message NAP unsupported appears. (Q02047291)

- Mac L2TP client fails to establish L2TP session, when `all` or `mschapv2` is set as the primary authentication order using `/cfg/vpn #/l2tp/authorder` . This is due to the compatibility issues of AVG 8.0.3 with non-Microsoft clients. (Q02030476)

  Workaround:

  If non-Microsoft clients are involved, instead of using `all` or `mschapv2` as the primary authentication order, use `pap, chap, mschapv1, mschapv2` .

- The CLI does not display the Encryption/Decryption information of BO Tunnel properly. (Q02083179)

Miscellaneous

- While upgrading the AVG devices in the cluster, some host can reboot continuously and fail to upgrade. This occurs in a cluster configuration when AVG is connected to L2 switch with Spanning Tree Protocol (STP) enabled. (Q01813363)

  Workaround:

While upgrading the cluster, disable the STP in L2 switch.

- AVG does not rewrite URL for addImport function of stylesheet object. (Q01161363)

- The Outlook 2003 version 4.2 client does not work through native outlook Port forwarder. (Q00757505)

- The Virtual Desktop does not support Linux. But, when user tries to logon to the Portal, the Linux tries to load the Virtual Desktop and error Downloading and initializing the applet. Please wait appears on the console. The Portal page does not change after displaying this error message. (Q02051541)

- Tunnel Guard does not work properly if splitnet is enable on the L2TP client for Windows Vista. The Tunnel Guard Connection attempt fails as the default route is modified to route through the L2TP connection (PPP interface). Nortel recommends that disable the splitnet on the client side if Tunnel Guard is enable. (Q02049514)

- AVG software re-image using bootshell causes `/cfg/cert` option to disappear. (Q01800810-01)

- By default, AVG uses unicode for IPsec i18n. This is the default language from Release 6.0.5. The language settings must match with the Contivity client and AVG server. The AVG server side does not require any changes if the Contivity uses version i18n (credentials are unicode). The AVG server requires changes if the default language set is iso-8859-1. The iso-8859-1 consists Latin characters which includes English, French, German, and Swedish. For more information about the Portal Language, see VPN Gateway Command Reference (NN46120-103). (Q02036234)

- Net Direct portal does not work on Windows 7, 64 bit Operating System. (Q02051434)

- While installing NDIC using NetDirectrunner.exe on Windows XP 32 bit Operating System, the NDIC process does not terminate after it receives termination request (idletimeout). (Q02045846)

- If the administrator configures NHA SRS rule from the remote site through the AVG portal, the user needs to access the BBI through tunnel-based client like Net Direct, IPsec, or L2TP. The BBI without NHA admin applet can be accessed through AVG portal. (Q02047301)

- There is problem with Internet Explorer version 7.0.2800.1106.xpsp2_gdr.04051 7-1325. When HTTPS is used, this version of Internet Explorer does not permit download of files that require an external program for processing, or that must be saved in the file system (for example, files with extension .txt, .exe, and .zip), even if the SSL VPN server HTTP setting of `addnostore` is set to `off`. Thus, IE cannot be used to download such files through the Portal.

- On Linux (SUSE 10.0) and Firefox, when Net Direct is started from the Portal, the message "Net Direct already running" is displayed in the Java applet window although the Net Direct is not started. When this message appears, the Net Direct cannot be started.

- Virtual Desktop fails with Kaspersky Internet Security 6.0. Kaspersky prompts for permissions to allow Vdesktop process to run. When it is launched, Vdesktop covers the prompts and the system hangs. (Q01716029). Workaround: Add to trusted zone.

- Cirtix Applet crashes when `urlobscure` is turned on. (Q01692215)

- Change to AAA causes delay in portal traffic. (Q01689436)

- Accessing certain sites can generate java script parse errors in the logs. (Q01926277)
- Triggers of type ip, url, and windowstitle do not work when virtual desktop is launched on Windows Vista and Windows 7 operating systems. (Q02051458)
- In Windows XP 64 bit systems, Net Direct works during the first initiation, but after 5 or 10 seconds it fails and error Forward entry creation failure appears. (Q02037201)
- Net Direct and Tunnel Guard does not get started when NAP is configured in the Windows Vista 32 bit operating system PC. (Q02050586)
- Log message Run Full System Scan Failed appears on NHA client when user connects to AVG using the Net Direct installable client. The predefined rule for the antivirus launches trigger, but does not work. (Q02050561)
- The BWM source IP filter is changed and impacted by another filter or BWM policy. This change impacts the existing traffic. (Q02051061)
- The display message for the NHA SRS failure notification is incorrect. The error message contains Nortel IPsec instead of Nortel SSL. (Q02050864)
- The SRS fail notification message for NHA appears even for the successful Tunnel Guard checks. (Q02053077)
- The NHA client does not respond to the UDP initialization message from server when Windows Firewall is enabled in XP or Vista client PC. When the Windows Firewall is disabled, the NAP autoremediation turns on the Firewall and the NHA client does not respond during the next login. (Q02047308) Workaround: Installing NHA 5.2.2.0_009 automatically adds itself as exception in the Windows firewall, so that UDP packets sent to AVG are not blocked. If NHA is already installed, upgrading NHA to higher version does not add the exception. Hence, user needs to uninstall the NHA, and then reinstall it.
- When NDIC or NVC is used, Tunnel Guard rechecks may not happen in some Windows XP SP3 machines, and consequently the client application exits. This is because if no packets flow through UDP socket, used by the tunnel clients, for about 60 seconds, the UDP socket becomes inactive, and prevents the server messages from reaching the client application. This issue occurs mainly in enabled splittun mode. (Q02047279).

  Workaround:

  Configure `/cfg/vpn #/sslclient/keepalive` to a value less than 60 seconds (for example, 50 seconds).

  The NVC does not support silent keepalives in SSL mode, hence some external application must be used to keep the tunnel alive.
- If two different VPN portals have Tunnel Guard enabled, then both the portals cannot be invoked simultaneously in the same machine using the same type of browser. One portal can be accessed successfully, but the login attempt to the second portal will fail and eventually consume one license. This happens due to the limitations with NHA applet and JRE. (Q01940997)
- The NDIC is not supported in Windows 7 operating system. (Q02059641)
- Virtual Desktop does not work on Windows 7 operating system. (Q02059471)
- During the configuration change, the bandwidth policy is not fully enforced. The user can see brief disruptions in traffic during the configuration change. (Q02050086)

- The group name match fails if user configures the group name using a non-english language, and subsequently changes the portal language to some other language. (Q02032973)

- Adding portal VIP to trusted site does not work with Windows Vista Ultimate, and IE 7 or IE8 browsers.

  workaround:

  Disable the IE protected mode by clearing the Enable Protected Mode check box in Tools, Internet Options, Security, Internet or Local intranet. (Q02026893)

- Pulling out USB drive without closing the SPO application can cause an unexpected behavior due to the limitation in Microsoft Windows. Avaya recommends to remove the USB device in graceful way as recommended by Microsoft. (Q02066043)

- Multiple clients behind the same NAT device cannot make simultaneous L2TP/IPsec connections. (Q02037954)

- Re-write failure for URL strings encapsulated in single quotations. (Q02101556)

  The rewrite engine of 7.x and above does not support single quotes injected inside double quotes. The following work around should fix the issue for all cases:

    - Use URL encoding for URLs containing quotes in user content (eg. %22 or %27 for double, and single quotes respectively).

    - Use HTML encoding for content containing quotes (eg. ' for single quotes).

    - Avoid using single quotes in HTML, javascript or ASP tags (eg. <a href=" "> instead of <a href=' '>).

    - Use proper escape sequences for javascript / asp etc when needing to use double quotes inside double quotes (eg. onscript = "...blah = \"foo\";" instead of onscript = '...blah = "foo";').

    - Use tunnel-based client such as Net Direct or PortForwarder. The use of single quotes in HTML tags seems to work in browsers but the W3C Validator seems to have depreciated it with XHTML 1.1 strict. The industry standard is to use double quotes.

- L2TP based clients on all MAC platforms (iPad, iTouch, iPhone, Mac, etc) works until rekey, but fails after rekey. The user has to disconnect and reconnect to have it working again.

Chapter 10: Known anomalies

This section lists known anomalies with the AVG software.

- In SSL Acceleration mode (type=http), the secure option on the session cookie was introduced in v4.2.1.11 and it can be controlled by /cfg/ssl/server #/http/securecook <on/off>. The old behavior in software versions prior to 4.2.1.11 is OFF. Also, in 4.2.1.11 and later (4.x, 5.1, 6.0), the default value of "securecook" is OFF. But if the software version earlier than 4.2.1.6 to 4.2.x later than 4.2.1.11 or 5.1 or 6.0 is upgraded, the value of "securecook" is set to ON. (Q01452086-01)

- Net Direct is only adding the first dns server in the list, so for example, if the search list containing alteonlab.com, netslab.com, abctest.com, is configured, after connecting, only alteonlab.com is seen against the adapter. In the Winxp registry under the path My computer\HKEY_LOCAL_MACHINE \SYSTEM\ControlSet001\Services\Tcpip\Parameters SearchList value is, alteonlab.com. (Q01731956)

Known anomalies

Chapter 11: Related documentation

- *VPN Gateway 8.0 Users Guide* (NN46120-104)
- *VPN Gateway 8.0 Command Reference* (NN46120-103)
- *VPN Gateway 8.0 Application Guide for SSL Acceleration* (NN46120-100)
- *VPN Gateway 8.0 CLI (Command Line Interface) Application Guide for VPN* (NN46120-101)
- *VPN Gateway 8.0 BBI (Browser-Based Interface) Application Guide for VPN* (NN46120-102)
- *VPN Gateway 8.0 VPN Administrators Guide* (NN46120-105)
- *VPN Gateway 3050/3070 Hardware Installation Guide* (216213-B)
- *VPN Gateway Configuration - Secure Portable Office Client* (NN46120-301)
- *VPN Gateway 8.0 Troubleshooting Guide* (NN46120-700)

Related documentation

Chapter 12: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Appendix A: Compatibility Matrix

This chapter provides you the following compatibility matrixes for Nortel VPN Gateway Release 8.0.5:

Note:

The compatibility matrixes are specified in the following terms:

- Supp—Tested in previous release; not verified in this release
- Cert—Verified in this release
- Unsup—Officially not supported
- x—Not applicable

Compatibility matrix of Avaya VPN Gateway Release 8.0.5

Table 1: AVG 8.0.5 Compatibility Matrix (1)

Client OS	Portal Mode	Port Forwarder	Net Direct	Net Direct installed	NHA	TG/NHA portal	SPO	SODP
Windows 2000 Professional	Supp	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Windows XP Professional	Cert	Cert	Cert	Cert	Cert	Cert	Cert	Supp
Windows XP 64-bit	Cert	Cert	Cert[1]	Unsup	Cert[3]	Cert[1]	Supp	Unsup
Windows Vista	Cert	Cert	Cert	Cert	Cert	Cert	Cert	Supp
Windows Vista 64-bit	Cert	Cert	Cert[1]	Unsup	Cert[3]	Cert[1]	Supp	Unsup

Client OS	Portal Mode	Port Forwarder	Net Direct	Net Direct installed	NHA	TG/NHA portal	SPO	SODP
Windows 7	Cert	Cert	Cert	Unsup	Cert	Cert	Cert	Unsup
Windows 7 64-bit	Cert	Cert	Unsup	Unsup	Cert[3]	Cert[1]	Supp	Unsup
MAC OS – 10.4	Supp	Supp	Supp	x	x	Supp[2]	x	x
MAC OS – 10.5	Cert	Cert	Cert	Unsup	Unsup	Supp[2]	Unsup	Unsup
MAC OS – 10.6	Supp	Supp	Supp	Unsup	Unsup	Supp[2]	Unsup	Unsup
Redhat	Supp	Supp	Supp	Unsup	Unsup	Supp[2]	Unsup	Unsup
Fedora Core	Supp	Supp	Supp	Unsup	Unsup	Supp[2]	Unsup	Unsup
Blackberry	x	x	x	x	x	x	x	x
iPhone – 2.1	x	x	x	x	x	x	x	x
Solaris	Supp	Supp	x	x	x	x	x	x
Windows Mobile – 6.1	x	x	x	x	x	x	x	x

1 — Only for 32-bit browsers. 64-bit browsers are unsupported.

2 — Mac/Linux NHA support is limited to bypass end point security check for the unsupported OS.

3 – NHA 64bit OS is supported from the NHA versions 5.3.0.

Table 2: AVG 8.0.5 Compatibility Matrix (2)

Client OS	L2TP	Application Virtualization	Contivity 6.x 7.x	Contivity 10.01	Contivity 10.04	WTS/ RDP	ICA Client
Windows 2000 Professional	Supp	Supp	Supp	Unsup	Unsup	Supp	Supp
Windows XP Professional	Cert	Supp	Supp	Unsup	Cert	Cert	Supp
Windows XP 64-bit	Cert	Unsup	Unsup	Unsup	Cert	Supp	Supp
Windows Vista	Supp	Supp	Unsup	Supp	Cert	Cert	Supp
Windows Vista 64-bit	Supp	Unsup	Unsup	Supp	Cert	Cert	Supp

Client OS	L2TP	Application Virtualization	Contivity 6.x 7.x	Contivity 10.01	Contivity 10.04	WTS/ RDP	ICA Client
Windows 7	Supp	Supp	Unsup	Unsup	Cert	Cert	Supp[1]
Windows 7 64-bit	Supp	Unsup	Unsup	Unsup	Cert	Cert	Supp[1]
MAC OS – 10.4	Supp[2]	x	x[3]	x	x	Supp[4]	Supp[1]
MAC OS – 10.5	Supp[2]	Unsup	x[3]	x	x	Supp[4]	Supp[1]
MAC OS – 10.6	Supp[2]	Unsup	x[3]	x	x	Supp[4]	Supp[1]
Redhat	Supp	Unsup	x[3]	x	x	Supp[4]	Supp[1]
Fedora Core	Supp	Unsup	x[3]	x	x	Supp[4]	Supp[1]
Blackberry	x	x	x	x	x	x	x
iPhone – 2.1	Supp[2]	x	x	x	x	x	x
Solaris	x	x	x[3]	x	x	Unsup	Unsup
Windows Mobile – 6.1	Supp	x	x	x	x	x	x

1 — ICA client only works in Java mode.

2 — Check Known Issue in the release note for unsupported features.

3 — Contivity Mac/Linux supports are available from 3rd party vendors like Apani.

4 — RDP only works in Java mode.

Compatibility matrix of third party applications with operating systems

Table 3: Third party compatibility matrix with operating systems

Third party applications	Internet Explorer 6	Internet Explorer 7	Internet Explorer 8	Firefox 3.x	Safari 3.0	Safari 4.0
Windows 2000	Supp	x	x	Supp	Supp	Supp

Windows XP	Cert	Cert	Supp	Cert	Supp	Supp
Windows XP 64 bit	Supp	Cert	Supp	Cert	Supp	Supp
Windows Vista	x	Cert	Supp	Cert	Supp	Supp
Windows Vista 64	x	Cert	Supp	Cert	Supp	Supp
MAC	x	x	x	Supp	Cert	Supp
Redhat	x	x	x	Supp	x	x
Fedora	x	x	x	Supp	x	x
Windows 7	x	x	Cert[1]	Cert	Supp	Supp
Windows 7 64 bit	x	x	Cert[1]	Cert	Supp	Supp

1 — Internet Explorer 8 has some compatibility issue with ICA client.

Compatibility matrix of backend servers

Table 4: Backend server matrix

Backend Servers	Portal mode	Port forwarder	SPO
OWA 2003	Cert	Cert	Supp
OWA 2007	Cert	Cert	Supp
OWA 2010	Unsup[1]	Unsup[1]	Unsup[1]
Sharepoint 2003	Cert	Cert	Supp
Sharepoint 2007	Supp	Supp	Supp
Sharepoint 2010	Unsup[1]	Unsup[1]	Unsup[1]
Lotus Domino 7.0	Cert	Cert	Supp
Lotus Domino 8.0	Cert	Cert	Supp
Lotus Domino 8.5	Unsup[1]	Unsup[1]	Unsup[1]
RSA Soft token	Supp	Supp	Supp
Citrix-4.0	Supp	Supp	Supp
Citrix-4.5	Supp	Supp	Supp

Backend Servers	Portal mode	Port forwarder	SPO
Citrix-5.0	Supp	Supp	Supp
Windows 2003 server	Cert	Cert	Supp
Windows 2008 server	Cert	Cert	Supp

1 — Uses Net Direct. or the Contivity client.

Compatibility matrix of AVG VMware Appliance

Table 5: AVG VMware Appliance matrix

VMware Platform	3050-VM	3070-VM
VMware ESX Server 3	Supp	Supp
VMware ESX Server 3.5	Supp	Supp
VMware ESX Server 4.0	Supp	Supp
VMware ESXi Server 3.0	Supp	Supp
VMware ESXi Server 3.5	Supp	Supp
VMware ESXi Server 4.0	Supp	Supp
VMware Workstation	Unsup	Unsup
VMware Server	Unsup	Unsup
VMware Player	Unsup	Unsup
Microsoft Hyper-V	Unsup	Unsup

Compatibility matrix of VPN Branch Office Tunnel

Table 6: VPN Branch Office Tunnel matrix

VPN Branch Office Tunnel	3050	3070
AVG 3050	Supp	Supp
AVG 3070	Supp	Supp
Contivity 1100 and above	Supp	Supp

VPN Branch Office Tunnel	3050	3070
Cisco[1]	Supp	Supp
CheckPoint[1]	Unsup	Unsup
BSR 222[1]	Unsup	Unsup

1 — The BO tunnel does not work properly if DPD is not enabled or DPD is not supported.

Index