Release Notes
Avaya VPN Gateway

8.0.9.0
NN46120-400, 05.01
June 2011

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your Product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://support.avaya.com.

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 35. 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. For more information, see Customer service on page 37.

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).

Chapter 3: New in this release

The following enhancements are included in Release 8.0.9.0:

- Avaya Health Agent is renamed as Avaya Endpoint Access Control Agent (EACA).
- Erlang/OTP support of SMP.

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** and then select **Documentation Library**.
4. Select the desired document from the A-Z list.

Chapter 5: Software installation and upgrade notice

SSL VPN Server software

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

- **`SSL-8.0.9.0-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 *Avaya VPN Gateway User's Guide (NN46120–104)*.

  Note:

  TFTP cannot be used when upgrading to version 7.0.1 or later from an earlier version.

- **`SSL-8.0.9.0-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 *Avaya VPN Gateway User's Guide (NN46120–104)*.

  Note:

  TFTP cannot be used when installing version 7.0.1 or later through the reinstall procedure.

- **`SSL-8.0.9.0-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.

Avaya 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 Avaya SSL VPN Client on page 28):

- 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

Avaya VPN client (formerly Contivity)

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

Avaya Net Direct installable client

The Net Direct SSL VPN installable client software can be downloaded from the AVG server when an external 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 8.0.9.0

To support the disk repartitioning for upgrade or downgrade from Release 7.x to 8.0.9.0 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 8.0.9.0 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 8.0.9.0 server software is supported on the following hardware platforms:

- VPN Gateway 3050
- VPN Gateway 3070

Chapter 7: Resolved issues

This section lists the WIs resolved in release 8.0.9.0:

Work item	Description
wi00822716	Incorrect DNS server chosen with Netdirect client on a Windows client.
wi00853259	The password change feature for Active Directory (AD) LDAP authentication is introduced in and after AVG 8.0.1.0 releases. Before the 8.0.x release, users whose passwords have expired are moved to the password expired group configured on the AVG; the portal then displays the corresponding links configured for that group, allowing the customer the flexibility of doing any remediation work. After the 8.0.1.0 release, this behaviour is changed. When a user whose password has expired logs into the portal, the AVG will present the password change page and will interact with the configured secured LDAP server to change the password and then place the user in the corresponding group returned by the AD server.
wi00853860	The password change feature for the LDAP AD server will work only when the LDAPS server is configured. The Microsoft AD server will allow the change password only when the connection is secured.
wi00861922	The SPO client is unable to connect properly to AVG if EACA is enabled.
wi00858996	The LDAP Browser has been removed..
wi00595618	URLs in the OWA message body are not displayed properly. They are rewritten and cause problems when clicked to view the pages.
wi00854997	Portal rewrite first pass truncates response.
wi00851662	Apple IOS devices fail using L2TP/IPSEC clients over NAT-T UDP port 4500.
wi00851256	Absolute URLs that do not explicitly specify the http or https method are not rewritten properly.
wi00884449	The VPN Gateway may sporadically restart simpleproxy with XASSERT Internal Error 125 when cookies are set by the web server and cookiedb is enabled (by default).
wi00877368	The VPN service restarts during the IP pool deallocation if the redundant IP was assigned. This result from the IP pool table causes the IP pool server to crash and restart.
wi00833905	All SSL licenses are consumed if digital certificates auth is used and TG is enabled.
wi00700833	Erlang/OTP must be upgraded support SMP

wi00821869	NetDirect applet should be supported on32 bit browsers by Win7 and Vista 64 bit
wi00874985	Using a two armed AVG with SSP enabled and specifying an alternative backend interface via the /cfg/vpn x/adv/interface (default = 0) command results in a failure to establish an active L2TP connection.
wi00822264	Microsoft Internet Explorer 9 Testing
wi00865922	simpleproxy may crash or fail to pass cookie data in its entirety (or at all) if the Set-Cookie header exceeds 4096 bytes.
wi00863842	The properjavaRDP open source client can not connect to a Windows Server 2008 Terminal Server w/ Device or Per-User licensing enabled w/ SSO disabled. Any connection attempt results in "Memory Accessed Out of Bounds" error response.
wi00863847	When SSO is enabled and if a WTS link's /cfg/vpn x/linkset y/link z/wts/ domain is specified the username should be formatted DOMAIN \USERNAME. No support was previously added for the properjavaRDP client in wts_java_forwarder to permit this.
wi00893422	With the removal of the ,xct1 tagging system in 8.0.3.0 sites that return a Content-Type: text/x-js (javascript) are not intercepted and rewritten by the AVG rewrite parser and are delivered to clients unchanged. This results in inconsistent client behavior.
wi00825878	The VPN Gateway's default cipher string will automatically trigger a PCI Compliancy exception as it supports weak/low cipher strengths.
wi00890360	As a likely result of changes for Q01834353/wi00567734 in 7.1.1.0 it is now possible to configure a group name (/cfg/vpn x/aaa/group y/name) to exceed 25 characters.
wi00853139	The "VPN Gateways » VPN-# » Traffic Trace » Traceroute" feature in the BBI is not working for unreachable hosts.
wi00704735	/stats/ssl and /stats/vpn Renegotiation Counter Does Not Increment. The renegotiation counter has been removed.
wi00866258	The certificate presented by the Cluster Manager applet has Nortel Networks as it's publisher.

Chapter 8: Known limitations

VPN limitation

VPN Gateway Release 8.0.9.0 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 the AVG software for basic Portal access, that is when not using the applets:

- Firefox 2.0 or later.
- Safari 2.0 or later.

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

Avaya Endpoint Access Control Agent Applet support

To support the Avaya Endpoint Access Control Agent (EACA) SSL applet that is 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, Vista, and Windows 7) 64 bit OS
  - Firefox 32 bit version on Windows (XP, Vista, and Windows 7) 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.
- When running Net Direct on Knoppix, the tun device node must be set up manually.

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

  `mkdir /dev/net mknod /dev/net/tun c 10 200`. No fix planned. wi00569568 (Q01281449)
- 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`**. No fix planned. wi00569565 (Q01278965)
- When using Net Direct in Windows 2000 with 2 NICs and one NIC becomes disabled, there is an issue in reconnection for Net Direct. No fix planned. wi00566645 (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. No fix planned. wi00569762, wi00570450, wi00570451, wi00574096 (Q01464430)

- Outlook 2003 client does not work through native outlook Port forwarder. No fix planned. wi00569342 (Q00757505)
- The maxPwdAge attribute is returned before presenting a password\account expiry message to the portal user. No fix planned. wi00569539 (Q01244929)

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.

Avaya Endpoint Access Control Agent

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

Special notice for customers using both Avaya VPN Gateway Release 7.0 or later and SNA Release 1.6.1 products

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

Avaya VPN Client (formerly Contivity VPN Client)

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

Avaya 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. wi00571215 (Q01351656-01)

Chapter 9: Known issues

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

Net Direct

NetDirect in UDP mode is not working on MAC OS X platforms. (wi00849974)

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

Secure Portable Office and Portal

- ActiveX Citrix ICA is not supported with IE8 and SPO Application Virtulization mode. The Firefox with Java Applet Citrix ICA can be used instead. wi00571435 (Q02040046)
- 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. wi00568280 (Q02040815)

Browser-Based Interface

- The Avaya Endpoint Access Control Agent (formerly Avaya Health Agent) Rule Definitions menu and tabs behave inconsistently and incorrectly. wi00571326 (Q02040322)
- The Avaya Endpoint Access Control Agent trigger command does not accept Windows environment variables. For example, %windir%,%programfiles% and other windows environment variables. wi00568194 (Q02040327)
- 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. wi00571284 (Q02062516)

Miscellaneous

- 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.
- Log message Run Full System Scan Failed appears on the EACA client when user connects to AVG using the Net Direct installable client. The predefined rule for the antivirus launches trigger, but does not work. wi00571411 (Q02050561)
- The BWM source IP filter is changed and impacted by another filter or BWM policy. This change impacts the existing traffic. wi00568267 (Q02051061)
- The display message for the EACA SRS failure notification is incorrect. The error message contains Avaya IPsec instead of Avaya SSL. wi00571350 (Q02050864)
- The SRS fail notification message for EACA appears even for the successful Tunnel Guard checks. wi00571437 (Q02053077)
- The EACA minimum version feature is currently not working. (wi00863201)
- Customer specific application rewrite fails with the error “xnet is undefined.” (wi00852869)
- The inclusion of the "" declaration in the 30x redirects generated by the VPN Gateway breaks application functionality in pure SSL offload mode.

  The SSL offload is intended to provide a front end HTTPS solution to a backend HTTP network. It is not intended to modify or introduce any changes such that applications break

or fail as a result -- aside from applications that are not certified or intended for use via HTTPS.

The SSL offload uses redirects when upstream clients 'ignorantly' request HTTP URLs on what is an HTTPS enabled connection. Such redirects should only provide the required "Location:" header and omit any body, especially considering the fact the body does not itself contain a link to the new location.

You can continue responding with a body, however, the DOCTYPE declaration should not be included OR should only be included as to avoid any conflict with client/server applications. (wi00843497)

- The L2TP/IPSec Windows XP client disconnects after the ISAKMP rekey occurs. (wi00859968)
- Auditing using RADIUS is not working. (wi00882722)
- Error for sequential authentication using LDAPS with expired account password. (wi00883807)
- Installing either AVC 10.04.109 (latest) or NDIC 8.0.8.7 (pre-8.0.9.0 release) on a Windows 7 64-bit (as tested) AND setting the /cfg/vpn x/sslclient/oslist to restrict users to "win7" yields unexpected results. These clients are not properly identified as Windows 7. For AVC, the client is detected as "client type = 2, client version = 0.0.0.2, os type = 9, os desc = vista" and rejected. For NDIC, the client is detected as "client type = 2, client version = 8.0.8.7, os type = 1, os desc = windows xp" and rejected. (wi00889545)
- After resolving the page trunctation issue via wi00854997 a doublemac against the customer application revealed a pre-existing re-write / display issue on the same page previous truncated by the AVG. (wi00891135)
- User session syslog logging for Portal works only for messages of type login-logout. (wi00891638)
- When access an OWA 2007 Internal Auto login URL the following error appears:

  An error occured while Automatic login: "got unsupported response '{undef,[{ssl,connect,\n [{11,126,8,75},\n 443,\n [binary,{packet,raw},{nodelay,true},{active,true}],\n 15000]},\n {url,get,4},\n {portal,auto_login_follow,7},\n {yaws_server,deliver_dyn_part,8},\n {yaws_server,aloop,3},\n {yaws_server,acceptor0,2},\n {proc_lib,init_p,5}]}' when talking to server". (wi00893144)
- Custom Port Forwarding link doesn't start from SPO. (wi00893695)
- When you configure NetDirect with a banner in rich text text format and you start NetDirect Instalable Client (on Windows Vista), the Interactive Services Detection starts. (wi00875067)
- The group name is not validated when adding a user to LOCAL database (wi00884712)
- Drop down menus cannot be accessed for a rewritten SharePoint 2007 site. (wi00884859)
- Authentication to SharePoint 2007 doesn't work if the IP address is used to connect to Sharepoint server. (wi00884905)

- Unable to login to OWA 2007 using an auto link from MF (wi00892516)
- DOCTYPE Declaration in 30x redirect breaks Customer Applications. No fix planned. (wi00843497)

Chapter 10: 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)

Chapter 11: 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 B: Compatibility Matrix

This chapter provides you the following compatibility matrixes for Avaya VPN Gateway Release 8.0.9.0:

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 8.0.9.0

Table 1: AVG 8.0.9.0 Compatibility Matrix (1)

Client OS	Portal Mode	Port Forwarder	Net Direct	Net Direct installed	EACA	TG/ EACA 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

Client OS	Portal Mode	Port Forwarder	Net Direct	Net Direct installed	EACA	TG/ EACA portal	SPO	SODP
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
Windows 7	Cert	Cert	Cert	Cert	Cert	Cert	Cert	Unsup
Windows 7 64-bit	Cert	Cert	Cert[1]	Unsup	Cert[3]	Cert[1]	Supp	Unsup
MAC OS – 10.4	Supp	Supp	Supp	x	x	Supp[2]	x	x
MAC OS – 10.5	Supp	Supp	Supp	Unsup	Unsup	Supp[2]	Unsup	Unsup
MAC OS – 10.6	Supp	Supp	Supp	Unsup	Unsup	Supp[2]	Unsup	Unsup
Redhat	Supp	Supp	Cert	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 EACA support is limited to bypass end point security check for the unsupported OS.

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

Table 2: AVG 8.0.9.0 Compatibility Matrix (2)

Client OS	L2TP	Application Virtualization	Contivity 6.x 7.x	Contivity 10.0.1	Contivity 10.0.4	Contivity 10.0.5	WTS/ RDP	ICA Client
Windows 2000 Pro	Supp	Supp	Supp	Unsup	Unsup	Unsup	Supp	Supp
Windows XP Pro	Cert	Cert	Supp	Unsup	Supp	Cert	Supp	Supp
Windows XP 64-bit	Cert	Unsup	Unsup	Unsup	Supp	Cert	Supp	Supp
Windows Vista	Cert	Cert	Unsup	Supp	Supp	Cert	Cert	Supp
Windows Vista 64-bit	Cert	Unsup	Unsup	Supp	Supp	Cert	Supp	Supp
Windows 7	Cert	Supp	Unsup	Unsup	Supp	Cert	Cert	Supp[1]
Windows 7 64-bit	Cert	Unsupp	Unsupp	Unsupp	Supp	Cert	Supp	Supp
MAC OS – 10.4	Supp[2]	x	x[3]	x	x	x	Supp[4]	Supp[1]
MAC OS – 10.5	Supp[2]	Unsup	x[3]	x	x	x	Supp[4]	Supp[1]
MAC OS – 10.6	Cert[2]	Unsup	x[3]	x	x	x	Supp[4]	Supp[1]
Redhat	Supp	Unsup	x[3]	x	x	x	Supp[4]	Supp[1]
Fedora Core	Supp	Unsup	x[3]	x	x	x	Supp[4]	Supp[1]
Blackberry	x	x	x	x	x	x	x	x

Client OS	L2TP	Application Virtualization	Contivity 6.x 7.x	Contivity 10.0.1	Contivity 10.0.4	Contivity 10.0.5	WTS/ RDP	ICA Client
iPhone – 2.1	Supp [2]	x	x	x	x	x	x	x
iPhone and iPad – iOS 4.2.1	Supp [2]	x	x	x	x	x	x	x
Solaris	x	x	x[3]	x	x	x	Unsup	Unsup
Windows Mobile – 6.1	Supp	x	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	IE 6	IE 7	IE 8	IE 9	Firefox 3.x	Firefox 4.x	Safari 3.0	Safari 4.0
Windows 2000	Supp	x	x	x	Supp	Supp	Supp	Supp
Windows XP	Supp	Supp	Supp	Unsupp	Supp	Cert	Supp	Supp
Windows XP 64 bit	Supp	Supp	Supp	Cert	Supp	Cert	Supp	Supp
Windows Vista	x	Supp	Cert	Cert	Supp	Cert	Supp	Supp

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

1 — Internet Explorer 8 and 9 have 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	Supp	Cert
OWA 2007	Cert	Supp	Cert
OWA 2010	Unsup[1]	Unsup[1]	Unsup[1]
Sharepoint 2003	Cert	Supp	Supp
Sharepoint 2007	Cert	Supp	Supp
Sharepoint 2010	Unsup[1]	Unsup[1]	Unsup[1]
Lotus Domino 7.0	Cert	Supp	Supp
Lotus Domino 8.0	Cert	Supp	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
Citrix-5.0	Supp	Supp	Supp
Windows 2003 server	Supp	Supp	Supp
Windows 2008 server	Supp	Supp	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 4.1	Cert	Cert
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
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