Release Notes
Avaya VPN Gateway

8.0.13.0
NN46120-400, 07.01
January 2012

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.This document also provides details on the software installation, upgrade instructions, supported hardware, licenses, and limitations in software for the Avaya Virtual Private Network Gateway (VPN Gateway).

For a list of related publications, seeRelated documentation on page 33. You can find the documentation suite for Avaya VPN Gateway on the documentation CD included with the software or on the Avaya Web site. For more information, see Customer service on page 35.

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 User License
- Secure Service Partitioning License
- Portal Guard License
- Demo License
- Emergency Recovery Access (ERA) License
- Secure Portable Office License
  - Existing SSL customers can add an SPO feature license to their existing license to enable SPO user access.
  - New customers must purchase the SSL and SPO licenses together.
  - The SSL license is a volume license, and therefore is applied in the cluster.
  - The SPO license is a feature license that must be purchased per node in the cluster.

For more information about SPO licenses, see Known issues on page 29 For more information on all license types see, *BBI Application Guide for VPN* (NN46120-102) and *CLI Application Guide for VPN* (NN46120-101).

Chapter 3: New in this release

There are no new features 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** 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 the following three different forms:

- **`SSL-8.0.13.0-upgrade_complete.pkg`**

  This package is the preferred method for upgrading an existing SSL VPN cluster because 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:

  You cannot use TFTP when upgrading to version 7.0.1 or later from an earlier version.

- **`SSL-8.0.13.0-boot.img`**

  The SSL-8.0.13.0-boot image file resets the VPN Gateway to its factory default configuration. You must use this image file when you add to a cluster a VPN Gateway that uses a different software. The current image file aligns the added VPN Gateway to the same software version as in the cluster before joining the gateway to the cluster.

  The software reinstall procedure is described in "Reinstalling the Software" in Chapter 3 of the *Avaya VPN Gateway User Guide* (NN46120–104).

  Note:

  You cannot use TFTP when installing version 7.0.1 or later through the reinstall procedure.

- **`SSL-8.0.13.0-auto-install.iso`**

  The SSL-8.0.13.0-auto-install.iso image resets the VPN Gateway to its factory default configuration. Use this image for a CD ROM 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://support.avaya.com
2. To download the software you must do one of the following:

   Click **Register** and follow the registration instructions.

   Click **Sign In** and enter your login credentials.

   After 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 then 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 box appears.
6. Click the link that appears beneath the software downloads dialog box, 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 25):

- 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)

You can download the VPN client software from theAvaya Customer Support website. Avaya VPN Client 10.0x supports both IPSec and SSL.

Avaya Net Direct installable client

You can download the Net Direct SSL VPN installable client software from the AVG server when you create an external link pointing to the server: for example, https://VIP/nortel_cacheable/NetDirect_Setup.zip.

Disk repartitioning for upgrade or downgrade from Release 7.x to 8.0.13.0

To support disk repartitioning for an upgrade or downgrade from Release 7.x to 8.0.13.0 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, during which time 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 ofTG 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 data model in the configuration, downgrade to 6.x and below or upgrade to 7.x and above causes RADIUS accounting server information inconsistency. The administrator must re-configure the RADIUS account server during this upgrade/downgrade process.
- Due to change in RADIUS auditing server data model in the configuration, downgrade to 8.0.11.x and below from 8.0.13.0 and above causes RADIUS auditing server information inconsistency. The administrator must re-configure the RADIUS auditing server during this upgrade/downgrade process.

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 platforms

The AVG 8.0.13.0 server software is supported on the following platforms:

- VPN Gateway 3050
- VPN Gateway 3070
- VMware ESX server

Chapter 7: Resolved issues

This section lists the WIs resolved in release 8.0.13.0:

Work item	Description
wi00947953	IKE daemon restarts unexpectedly and results in IPSEC client disconnection. The internal IKE table qmInboundSpiIndexTable is not updated after ISAKMP re-key for IPSEC clients behind a NAT device. The entries in this table incorrectly reference the deleted ISAKMP SA. This reference is used when handling new port mappings for these NAT'd clients.
wi00961868	Client browsers accessing websites via the portal may report a javascript exception after upgrading from AVG 8.0.7.1 or earlier and malfunction. The exception reported is "anObject.document is null or not an object".
wi00956484	Client certificates containing multiple OU (Organizational Unit) objects were parsed in reverse order in all prior 8.x releases and were inconsistent with 7.x and earlier behavior. This issue has been corrected.
wi00945498	The "nortelxnetch" challenge cookie is sent during secondary authentication (RSA + another authentication method). This cookie is marked secure, but it cannot be marked httpOnly (httpOnly is not supported by Yaws server). This cookie is not an actual security threat as it retains only the state that the PIN has to be changed. Logging into the portal is not based on this cookie, and it is immediately expired is expired when you log in to the portal.
wi00929780 wi00956623	Yaws error while accessing portal; Yaws process died: {error,closed}.
wi00965049 wi00966183	Introduce BBI Support for DOMAIN for WTS Linksets.

Chapter 8: Known limitations

VPN limitations

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

Secure Portable Office client

The Secure Portable Office (SPO) client virtualization mode supports SmartCard-based certificate management using Virtualized Aladdin PKI Client software only when you use an E-Token NG-FLASH 72 KB (Java Virtual Machine). You cannot use the E-Token NG-FLASH 64 KB (Siemens CardOS) to manage client certificates from SmartCard using Virtualized PKI Client software because this software is incompatibility with the generic USB CCID driver (usbccid.sys). The E-Token NG-FLASH 64 KB can only work with the proprietary SmartCard reader driver, which is not available in Windows operating systems. Application virtualization does not support the virtualization of drivers, therefore, you must install theAladdin PKI client on the host PC to manage the client certificates if you use an E-Token NG-FLASH 64 KB as the SPO client. (Q02030468)

In FireFox, the E-Token keeps prompting you to enter a password even if the client certification is disabled.

You can configure a maximum delay of 30 seconds to log out of an SPO client after the idle timeout is over.

Net Direct client

When running Net Direct client on Knoppix, you must configure the tun device node manually.

Run the following command as root to configure the tun node:

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

No fix planned. wi00569568 (Q01281449)

When running Net Direct on Linux, you must enable root on the remote user's machine and authorize the user account to use the command **`su root`**. No fix planned. wi00569565 (Q01278965)

When using the Net Direct client in Windows 2000 with two 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, however the check fails if it is run through a proxyThe application works correctly if it is connected through the Net Direct client. After passing the client check through Net Direct, the site can be used through a 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

You cannot install the Avaya VPN Client (AVC) and Net Direct Installable Client (NDIC) on the same device. You must uninstall the NDIC before you install the AVC, or vice-versa.

Caching of Net Direct components is not supported for Linux and Mac OS X.

The Mobility feature is not supported for MAC and Linux platforms.

If you improperly disconnect Net Direct, DNS restoration fails. Avoid the following improper ways of disconnecting the Net Direct client:

- 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.

The system does not save any users to local database if the add bulk option is used for more than 3000 entries. (wi00936281)

NDIC Linux ICMP reply with PID 0000. (wi00909159)

Custom App Re-write Failure reports "xnet is undefined". (wi00852869)

Issue with common host mappings for multiple port forwarder applets running at the same time on Windows XP. (wi00937551)

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 Endpoint Access Control 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 Endpoint Access Control 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 SSLVPN 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 HTTPProxy 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.
- 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)
- SSL VPN portal mode to handle JSON that contains JavaScript string enclosed with single quotation mark is failing. (wi00891135)
- Microstrategy custom application re-write failure. (wi00946181) See also wi00891135 (above) for more detail.

Chapter 9: Known issues

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

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 SSLVPN 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 SPOApplication Virtulization mode. The Firefox with Java Applet Citrix ICA can be used instead. wi00571435 (Q02040046)
- SPO with Application Virtualization mode does not support Port forwarder host mapping feature. wi00568280 (Q02040815)
- In Windows 7 with IE9, you cannot drag the SPO window with single-click and hold but double-click and hold. In order to drag the window again, you have to do a single-click first and then the double-click and hold. (wi00946776)

Browser-Based Interface

- The Avaya Endpoint Access Control Agent (formerly Avaya Health Agent and Nortel 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)

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 the 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)
- User session syslog logging for Portal works only for messages of type login-logout. (wi00891638)
- 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)
- Two redundant IPs can be allocated from the IP pool table. (wi00877371)
- VPN BO tunnel is not stable. The 3rd party VPN device is SonicWALL NSA 240. The tunnel can stop working randomly. (wi00871926)
- EACA 5.x cannot use the Memory Snapshot feature on MS Windows Vista or Windows 7 with UAC enabled. Windows 7 Enterprise version does not have the issue with UAC enabled. The work-around is to disable the UAC. (wi00942037)

- A MAC OSX/iOS L2TP/IPsec client connection issue exists when the Avaya VPN Gateway is in SSP mode and when the assigned backend interface is not the same as the management network interface. (wi00952899, wi00928313, wi00952901)
- When you install an SSLlicense, the license information menu does not display the IPsec license number, which is implicitly included in the SSL license.
- There is a limitation within the EACA Memory Snapshot functionality on machines with UAC (User Account Control) enabled. Most Windows OS' from Vista through Windows 7 Professional -- not including Windows 7 Enterprise and Ultimate -- are limited in the output of the embedded memory snapshot functionalityThe limitation only shows user-spawned processes. No local/network/system processes can be detected. This renders the EACA applet memory snapshot functionality via the portal inefective for the broadest category of client machines -- most presumed to have UAC enabled by default or forced enabled by company policy. The current workaround for this issue is to permanently disable UAC. (wi00942037)
- Third-party PeopleSoft application not usable via portal rewrite. (wi00943849)
- Split Tunnel Mode "Disabled" does not work with Net Direct. (wi00967990, wi00967989)
- You cannot view host IP pool allocations in BBI. (wi00968428)
- Uninstalling NDIC requires a mandatory system restart,even though this option is not selected during the uninstall process. (wi00961745)
- You cannot delete user tunnel profiles that have been created automatically using the QUICK wizard. (wi00965415)
- You cannot unset the L2TP or IPsec certificate from the BBI menu. (wi00960623)
- Net Direct in UDP mode is not working on MAC OS X platforms. (wi00849974)

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 http://support.avaya.com.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at http://support.avaya.com. From this Web site, you can locate theTraining 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 http://support.avaya.com.

Appendix A: Compatibility Matrix

This chapter provides you the following compatibility matrixes forAvaya VPN Gateway Release 8.0.13.0:

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 matrices for Avaya VPN Gateway Release 8.0.13.0

Table 1: Compatibility matrix[1] — Windows

Applications	Windows operating systems						
	2000 Pro	XP Pro	XP 64-bit	Vista	Vista 64-bit	7	7 64-bit
Portal Mode	Supp	Cert	Supp	Cert	Supp	Cert	Cert
Port Forwarder	Supp	Supp	Supp	Supp	Supp	Cert	Cert
Net Direct	Supp	Cert	Supp[1]	Cert	Supp[1]	Cert	Cert[1]
Net Direct installed	Supp	Supp	Unsup	Supp	Unsup	Cert	Unsup
EACA	Supp	Supp	Supp[2]	Supp	Supp[2]	Cert	Cert[2]

Applications	Windows operating systems						
	2000 Pro	XP Pro	XP 64-bit	Vista	Vista 64-bit	7	7 64-bit
TG/EACA portal	Supp	Supp	Supp[1]	Supp	Supp[1]	Cert	Cert[1]
SODP	Supp	Supp	Unsup	Supp	Unsup	Unsup	Unsup

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

2 — EACA 64bit OS is supported from the EACA versions 5.3.0.

Table 2: Compatibility matrix[1] — MAC

Applications	MAC OS – 10.4	MAC OS – 10.5	MAC OS – 10.6
Portal Mode	Supp	Supp	Cert
Port Forwarder	Supp	Supp	Cert
Net Direct	Cert	Cert	Cert
Net Direct installed	x	Unsup	Unsup
EACA	x	Unsup	Unsup
TG/EACA portal	Supp[1]	Supp[1]	Supp[1]
SODP	x	Unsup	Unsup

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

Table 3: Compatibility matrix[1] — other operating systems

Applications	Redhat	Fedora Core	Solaris
Portal Mode	Supp	Supp	Supp
Port Forwarder	Supp	Supp	Supp
Net Direct	Cert	Supp	x
Net Direct installed	Unsup	Unsup	x
EACA	Unsup	Unsup	x
TG/EACA portal	Supp[1]	Supp[1]	x
SODP	Unsup	Unsup	x

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

Table 4: Compatibility matrix[1] — mobile

Applications	Blackberry	iPhone – 2.1	Windows Mobile – 6.1
Portal Mode	x	x	x
Port Forwarder	x	x	x
Net Direct	x	x	x
Net Direct installed	x	x	x
EACA	x	x	x
TG/EACA portal	x	x	x
SPO	x	x	x
SODP	x	x	x

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

Table 5: Compatibility matrix[2] — Windows

Applications	Windows operating systems						
	2000 Pro	XP Pro	XP 64-bit	Vista	Vista 64-bit	7	7 64-bit
L2TP	Supp	Cert	Supp	Cert	Supp	Cert	Cert
SPO[1]	Supp	Cert	Unsup	Supp	Unsup	Cert	Unsup
Contivity 6.x 7.x	Supp	Supp	Unsup	Unsup	Unsup	Unsup	Unsup
VPN Client 10.1	Unsup	Unsup	Unsup	Supp	Supp	Unsup	Unsup
VPN Client 10.04	Unsup	Supp	Supp	Supp	Supp	Supp	Supp
VPN Client 10.05	Unsup	Cert	Supp	Cert	Supp	Cert	Supp
WTS/ RDP	Supp	Supp	Supp	Supp	Supp	Cert	Supp

1 — SPO refers to both Native and Virtualized modes. See the SPO Compatibility Matrix table for more information.

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

Table 6: Compatibility matrix[2] — MAC

Applications	MAC OS – 10.4	MAC OS – 10.5	MAC OS – 10.6
L2TP	Supp[2]	Supp[2]	Cert[2]
SPO[5]	x	Unsup	Unsup

Applications	MAC OS – 10.4	MAC OS – 10.5	MAC OS – 10.6
Contivity 6.x 7.x	x[3]	x[3]	x[3]
VPN Client 10.1	x	x	x
VPN Client 10.04	x	x	x
VPN Client 10.05	x	x	x
WTS/ RDP	Supp[4]	Supp[4]	Cert[4]
ICA Client	Supp[1]	Supp[1]	Supp[1]

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.

5 — SPO refers to both Native and Virtualized modes. See the SPO Compatibility Matrix table for more information.

Table 7: Compatibility matrix — other operating systems

Applications	Redhat	Fedora Core	Solaris
L2TP	Supp	Supp	x
SPO[2]	Unsup	Unsup	x
Contivity 6.x 7.x	x[3]	x[3]	x[3]
VPN Client 10.1	x	x	x
VPN Client 10.04	x	x	x
VPN Client 10.05	x	x	x
WTS/ RDP	Supp[4]	Supp[4]	Unsup
ICA Client	Supp[1]	Supp[1]	Unsup

1 — ICA client only works in Java mode.

2 — SPO refers to both Native and Virtualized modes. See the SPO Compatibility Matrix table for more information.

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

4 — RDP only works in Java mode.

Table 8: Compatibility matrix[1] — mobile

Applications	Blackberry	iPhone – 2.1	iPhone and iPad – iOS 4.2.1	Windows Mobile – 6.1
L2TP	x	Supp[1]	Cert[1]	Supp
SPO[2]	x	x	x	x

Applications	Blackberry	iPhone – 2.1	iPhone and iPad – iOS 4.2.1	Windows Mobile – 6.1
Contivity 6.x 7.x	x	x	x	x
VPN Client 10.1	x	x	x	x
VPN Client 10.04	x	x	x	x
VPN Client 10.05	x	x	x	x
WTS/ RDP	x	x	x	x
ICA Client	x	x	x	x

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

2 — SPO refers to both Native and Virtualized modes. See the SPO Compatibility Matrix table for more information.

Table 9: Compatibility matrix — SPO Native mode[1]

Applications	XP Pro 32-bit	XP 64-bit	Vista 32-bit	Vista 64-bit	Win 7 32-bit	Win 7 64-bit
Net Direct	Cert	Supp	Supp	Cert	Cert	Cert
Firefox 4.5	Cert	Supp	Supp	Supp	Cert	Cert
Firefox 8.0	Cert	Cert	Cert	Cert	Cert	Cert
JRE 1.6.0	Supp	Supp	Supp	Supp	Cert	Cert
IE 8	Cert	Supp	Supp	Supp	Supp	Supp
IE 9	X	X	Supp	Supp	Cert	Cert
Portal Links	Cert	Supp	Supp	Cert	Cert	Cert

1— SPO does not support Mac and Linux operating systems.

Table 10: Compatibility matrix — SPO virtualized mode[1, 2]

Applications	XP Pro 32-bit	XP 64-bit	Vista 32-bit	Vista 64-bit	Win 7 32-bit	Win 7 64-bit
Net Direct	Cert	Unsup	Supp	Unsup	Cert	Unsup
Firefox 3.5.2	Cert	Unsup	Cert	Unsup	Cert	Unsup
JRE 1.6.0	Supp	Unsup	Supp	Unsup	Supp	Unsup
IE 8	Cert	Unsup	Supp	Unsup	Supp	Unsup
IE 9	X	X	Supp	Unsup	Cert	Unsup
Portal Links	Cert	Unsup	Supp	Unsup	Cert	Unsup

Applications	XP Pro 32-bit	XP 64-bit	Vista 32-bit	Vista 64-bit	Win 7 32-bit	Win 7 64-bit
2050 IP softphone	Cert	Unsup	Supp	Unsup	Cert	Unsup

1 — SPO does not support Mac and Linux operating systems.

2 — SPO Virtualized Mode on CDROM is not supported.

Compatibility matrix of third party applications with operating systems

Table 11: Third party compatibility matrix with operating systems — Windows

Applications	Windows operating systems						
	2000	XP	XP 64-bit	Vista	Vista 64	7	7 64-bit
IE 6	Supp	Supp	Supp	x	x	x	x
IE 7	x	Supp	Supp	Supp	Supp	x	x
IE 8	x	Cert	Supp	Supp	Supp	Supp[1]	Supp[1]
IE 9	x	x	x	Cert	Cert	Cert[1]	Cert[1]
Firefox 3.x	Supp	Supp	Supp	Supp	Cert	Cert	Cert
Firefox 4.x	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Firefox 5.x	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Firefox 6.x	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Firefox 8.x	Supp	Cert	Supp	Cert	Supp	Cert	Cert
Safari 3.0	Supp	Supp	Supp	Supp	Supp	Supp	Supp
Safari 4.0	Supp	Supp	Supp	Supp	Supp	Supp	Supp

1 — Internet Explorer 8 and 9 have some compatibility issue with ICA client.

Table 12: Third party compatibility matrix with operating systems — other operating systems

Applications	MAC	Redhat	Fedora
IE 6	x	x	x
IE 7	x	x	x
IE 8	x	x	x

Applications	MAC	Redhat	Fedora
IE 9	x	x	x
Firefox 3.x	Supp	Supp	Supp
Firefox 4.x	Unsup	x	Supp
Firefox 5.x	Supp	x	x
Firefox 6.x	Supp	x	x
Safari 3.0	x	x	x
Safari 4.0	x	x	x

Compatibility matrix of backend servers

Table 13: Backend server matrix

Backend Servers	Portal mode	Port forwarder	SPO
OWA 2003	Cert	Supp	Supp
OWA 2007	Cert	Supp	Supp
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	Supp	Supp	Supp
Lotus Domino 8.0	Supp	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	Cert	Cert	Supp
Citrix-6.5	Cert	Cert	Cert
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 14: 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	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 devices

Table 15: VPN Branch Office Tunnel device matrix

VPN Branch Office Tunnel device	Supported
AVG 3050	Yes
AVG 3070	Yes
Contivity 1100 and above	Yes
Cisco[1]	Yes
CheckPoint[1]	No
BSR 222[1]	No
SonicWALL N240	No

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