Avaya VPN Gateway
Release Notes

Release 10.0.1.0
Issue 29.01
November 2014

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 may generally make available to users of its products and Hosted Services. 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 websites 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 Avaya hardware and software. 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 website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFOARE 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”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Note to Service Provider

The Product or Hosted Service may use Third Party Components subject to Third Party Terms that do not allow hosting and require a Service Provider to be independently licensed for such purpose. It is your responsibility to obtain such licensing.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), 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, Hosted Service(s) 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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 6
Purpose 6
Chapter 2: AVG Release 10.0.1.0 Target Applications 7
Chapter 3: New in this release 8
Features 8
Other changes 8
Chapter 4: Licenses 10
Obtaining a license for VPN Gateway 10
Chapter 5: Software installation and upgrade notice 11
SSL VPN Server software 11
Server software download 12
Avaya VPN Client (formerly Contivity) 12
Downgrade IE Cache Wiper Cab, Net Direct Cab, and SODP ActiveX files 12
VM Appliance Package 13
Chapter 6: Supported platforms 14
Chapter 7: Resolved issues 15
Chapter 8: Known limitations 16
VPN limitations 16
Net Direct 16
Avaya VPN Client (formerly Contivity VPN Client) 17
Portal 17
Other limitations 19
General 19
Chapter 9: Known issues 20
VM Appliance Package 20
OVF Template menu in vSphere Client 4.1 fails to install AVG OVA package 20
Portal 20
Miscellaneous 21
Appendix A: Compatibility Matrix 23
Compatibility matrixes for Avaya VPN Gateway Release 10.0.1.0 23
Compatibility matrix — Windows 23
Compatibility matrix — MAC 24
Compatibility matrix — other operating systems 25
Compatibility matrix — mobile 25
Compatibility matrix — Android 26
Compatibility matrix — IP Phones 26
Compatibility matrix of backend servers 26
Compatibility matrix of AVG VMware Appliance 27

Compatibility matrix of VPN Branch Office Tunnel devices..... 28
Compatibility matrix of third party applications with operating systems..... 28
Appendix B: Related Resources..... 30
Getting technical documentation..... 30
Training..... 30
Viewing Avaya Mentor videos..... 30
Support..... 31

Chapter 1: Introduction

Purpose

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 more information on how to configure the AVG for IP Office applications, refer to *Deploying Avaya IP Office Platform™ SSL VPN Services*.

Chapter 2: AVG Release 10.0.1.0 Target Applications

The following software and virtual appliances are intended to support SSL Management Services for IP Office customers only.

- AVG-10.0.1.0 software
- AVG-10.0.1.0-3050.ova
- AVG-10.0.1.0-3070.ova
- AVG-10.0.1.0-3090.ova

All other customers shall not install or upgrade to AVG 10.0.1.0 software on following platforms:

- Install/Upgrade from AVG 8.x software on virtual appliances
- Install/Upgrade from AVG 9.x software on virtual appliances
- Install/Upgrade from 3050 and 3070 HW appliances

Chapter 3: New in this release

The following sections detail what is new for Release 10.0.1.0.

Features

The following new features have been added to this release.

Security Enhancement

- Introduction of new **ipoffice** group with **novice** user type for added security.
- AVG 10.0.1.0 supports TLS 1.2 by default for added security.
- During initial setup user has possibility to choose between **Generic** parameters or **Alteon** when configuring RADIUS server.
- AVG 10.0.1.0 configures the remote administrative access via HTTPS and SSH by default. For one-armed and two-armed setup, HTTPS default port is 8443 and 443 respectively.

Usability Enhancement

- Easier way to jump start the VPN services for SSL Management Services during the initial deployment.
- AVG 10.0.1.0 default IDLE TTL value is changed to two minutes.
- AVG 10.0.1.0 generates a self-signed certificate with a seven year validity period.
- Easy setup of static route, splitnet and network access configuration in startup wizard. Split tunnel is enabled by default for added security.
- AVG 10.0.1.0 default **IDLE Checking for SSL Clien**t value is changed to disabled.
- AVG 10.0.1.0 default Link URL display mode value is changed to **off** for added security

Other changes

- CVE-2014-7169 bash environment variable code injection.
- CVE-2014-0160 TLS heartbeat read overrun.
- CVE-2014-0224 SSL/TLS MITM Vulnerability and other OpenSSL Security Advisories for June 5, 2014.

- CVE-2014-3566 POODLE.
- The Avaya Endpoint Access Control Agent (AEACA) feature is no longer supported in the 10.0.1.0 release.
- Net Direct Installable Client (NDIC) for Windows is no longer supported in the 10.0.1.0 release.

Chapter 4: Licenses

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

- SSL
- Demo License
- Emergency Recovery Access (ERA) License

Obtaining a license for VPN Gateway

Perform the following procedure to obtain a license for Avaya VPN Gateway.

Procedure

1. Send an E-mail request to: datalicensing@avaya.com.
2. In your E-mail, include the following information:
   a. MAC address of your VPN Gateway; for example, MIP MAC if HA cluster.

      To obtain the MAC address, from Command Line Interface (CLI) enter the following command:

      ```
      /info/local
      ```

   b. List of order codes associated with purchase.
   c. License Authorization Codes (LAC) received with purchase.

Note:

The E-mail account avaya0118@gwsmail.com is no longer active. To request a license, contact datalicensing@avaya.com.

Chapter 5: Software installation and upgrade notice

SSL VPN Server software

The SSL VPN server software is delivered in the following forms:

- **SSL-10.0.1.0-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).

- **SSL-10.0.1.0-boot.img**

  The SSL-10.0.1.0-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).

- **SSL-10.0.1.0-auto-install.iso**

  The SSL-10.0.1.0-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.

- **SSL-10.0.1.0–<platform ID>.ova**

  The SSL-10.0.1.0-<platform ID>.ova image resets the VPN Gateway to its factory default configuration. Use this Virtual Appliance image to install on VMware. The software configures virtual HW based on the platform specification and it starts the installation automatically. For more information, refer to *VMware Getting Started Guide* (NN46120-302).

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. Select **Downloads & Documents** and then enter **VPN Gateway 3050** or **VPN Gateway 3070** in the product field.
4. Select the Release or **Don't Know** if you do not know the release number.
5. Select **Downloads** as the content type and press **Enter**.
6. Click **Download** for the software version you wish to download.

   You are directed to a Downloads & Documents summary page.
7. Click the appropriate software file to download.

Avaya VPN Client (formerly Contivity)

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

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.

Note:

If you are running Windows 8, you need to manually remove the respective cab files from the "%SYSTEMROOT%\Downloaded Program Files" as Internet Explorer on Windows 8 will not remove them with this procedure.

VM Appliance Package

The SSL VPN server software is delivered in the following forms:

- SSL-10.0.1.0-3050.ova
- SSL-10.0.1.0-3070.ova
- SSL-10.0.1.0-3090.ova

These packages contain files used to describe Avaya VPN Gateway virtual machines. They include an .OVF descriptor file, a manifest (.MF) and an Avaya trusted certificate file, and other related files saved in a single archive using .TAR packaging. OVF support allows for simpler and easier AVG virtual appliances deployment.

For information on known issues with VM Appliance Package, see Known issues on page 20. For more information on the AVG OVF deployment procedure, see *VMware Getting Started Guide* (NN46120-101).

Chapter 6: Supported platforms

The AVG 10.0.1.0 server software is supported on the following platforms:

- Avaya VPN Gateway 3050–VM (AVG 3050–VM)
- Avaya VPN Gateway 3070–VM (AVG 3070–VM)
- Avaya VPN Gateway 3090–VM (AVG 3090–VM)
- VMware ESX server

For more information, refer to Compatibility matrixes for Avaya VPN Gateway on page 23.

Chapter 7: Resolved issues

The VPN Gateway 10.0.1.0 software release contains the same corrective content, bug fixes and features as the 9.0.15.0 and 9.1.5.0 software release.

This section lists the WIs resolved in this release.

ID	Summary
wi01190975	CVE-2014-7169 bash environment variable code injection
wi01164288	CVE-2014-0160 TLS Hearbeat read overrun
wi01198801	File upload to Windows Server 2012 through Portal mode failed
wi01163977	OSX/iOS L2TP behind NAT Fails Due To Malfunctioning DPD
wi01179056	CVE-2014-0224 SSL/TLS MITM Vulnerability and other OpenSSL Security Advisories for June 5, 2014

Chapter 8: Known limitations

The following section describes the known limitations in the VPN Gateway that customers should be aware of when designing and implementing network solutions.

VPN limitations

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.

Net Direct

- Before launching Net Direct, you must first install JRE.
- The Siebel portal does a client check before the application loads, however the check fails if it is run through a proxy. The application works correctly if it is connected through the Net Direct. 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. (wi00569539, Q01244929)
- TCP is used instead of UDP when TLS12 protocol is set for the Net Direct connection.

Windows

- Windows operating system supports the running of one instance of a Net Direct.
- When using Net Direct in Windows 2000 with two NICs and one NIC becomes disabled, there is an issue in reconnection for Net Direct. (wi00566645, Q01619895)

MAC OS X

- The Mac OS X modes enabled, enabled_inverse and disabled do not tunnel the local net. The enabled_inverse mode is not supported on the Linux operating system. As a general rule, if the user is running Net Direct and the split tunneling mode is not supported, the enabled_inverse_local mode will be used as fallback. (wi01021792)

- The portalbind=off option is not supported on Mac OS X, and portalbind=on will be used as a fallback.(wi01021794)
- Mac OS X uses 127.0.0.1 by default. To use loopback address other than 127.0.0.1, the Mac user must configure the loopback alias manually.
- Caching of Net Direct components is not supported for Linux and Mac OS X.
- Net Direct in UDP mode is not working on MAC OS X platforms. (wi00849974)
- Net Direct's Mobility feature is not supported on Mac OS X & Linux (wi01022473).

Linux

- 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)
- Net Direct's Mobility feature is not supported on Mac OS X & Linux (wi01022473).

Knoppix

- When running Net Direct 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)

Avaya VPN Client (formerly Contivity VPN Client)

Avaya VPN client versions 5.x, 6.x, 7.x, 8.x, and 10.x are supported.

Note:

Although legacy Avaya VPN Client (AVC) versions 5.x – 8.x may continue to operate with AVG 9.0, Avaya highly recommends upgrading to the latest AVC release in order to stay current with Avaya's most recent software releases.

In the event you experience any issue with legacy versions of AVC, please upgrade to AVC Release 10.06 to take advantage of Avaya's most recent software improvements.

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 98, XP, Vista, 7 and 8 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.
- 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, take 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 Net Direct 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".

- The features available on the Portal as WTS/RDP activeX full screen functionality do not support "Restore Down" sizing. (wi00568359)

Other limitations

- 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 Net Direct:
  - 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)
- IPOffice SSL client ICMP reply with PID 0000. (wi00909159)
- On Android 2.3.6, IPSec and ISAKMP Rekey doesn't take place. On Android 3.1 and 4.x, only the IPsec Rekey is always done correctly. (wi01019594)
- All portal links (except NetDirect) do not support TLSv1 and above. (wi01088305)

General

- A maximum of 5000 SSL or IPSec/L2TP clients generating up to 32000 cumulative concurrent connections are allowed on a 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.
- 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.
- Android, MAC OS X and iOS L2TP/IPsec support: When configuring Authorder tab under L2TP for the VPN gateway, do not select MSCHAPV2 and All. (wi01028212)
- L2TP Android 3.1, 4.0.4 clients are not properly disconnected from VPN. The client session remains blocked until the idle or dpd timer expires. (wi01019073)

Chapter 9: Known issues

This section lists the known issues that have been identified relative to specific features.

VM Appliance Package

- AVG 3090-VM installed from OVA package on ESXi 5.1.0 build 799733 stops functioning after some time since installation. (wi01117152)

  This issue was fixed in VMware ESXi Server 5.1.0 update 1 build 1065491. For more information, refer to Compatibility matrix of AVG VMware Appliance on page 27.

OVF Template menu in vSphere Client 4.1 fails to install AVG OVA package

This is a vSphere Client 4.1 bug. The issue occurs if the OVF .cert file is a multiple of 1024 bytes where AVG OVA cert file is 4096 bytes. The recommended work-around:

- Use ISO image to do legacy installation method.
- Deploy the .ova with the Open Virtualization Format Tool (ovftool).
- Unpack the .ova and deploy the .ovf with the vSphere Client.

More information can be found at http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1032863.

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`**

- Due to an issue with Oracle JRE, to use SSLv3 for AVG Java Applets, users must select the "**Use SSL 3.0**" check-box only in the Java Control Panel (uncheck TLS1.0). JRE does not fallback to lower protocol. (wi01079782)
- AVG Port fowarder and SSH terminal only support SSL 3.0. The Applet will fail to operate if the AVG is configured to use TLS1.0 and above.

Issues specific to OWA2010

- A gray window appears when user tries to establish an appointment in Firefox 27.0.1. No information available for user to establish (no issue with Firefox 20.0.1 and Internet Explorer 9-11). (wi01160020)
- Signature is not automatically placed when open to write a mail from Firefox 27.0.1. Internet Explorer 9-11 and FF 20.0.1 can be used instead. (wi01160012)
- E-mails cannot be sent using OWA 2010 and Firefox 27.0.1. Internet Explorer 9-11 and FF 20.0.1 can be used instead. (wi01159986)
- The option "Check Names" is not available anymore with OWA 2010 and Firefox 27.0.1. No action is taken when you click on this button. Internet Explorer 9-11 and FF 20.0.1 can be used instead. (wi01159992)
- After mails are moved to other folders, they are not available after that (Firefox). (wi01160000)
- VPN xnet javscript rewrite code is displayed in E-mail document body when change format from HTML to Plain text (Firefox). (wi01160008)
- OWA 2010 Forms-based authentication failure due to malformed cookie. (wi01152256)

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.
- The BWM source IP filter is changed and impacted by another filter or BWM policy. This change impacts the existing traffic. (wi00568267, Q02051061)
- 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)
- VPN BO tunnel is not stable. The 3rd party VPN device is SonicWALL NSA 240. The tunnel can stop working randomly. (wi00871926)
- You cannot view host IP pool allocations in BBI. (wi00968428)
- You cannot delete user tunnel profiles that have been created automatically using the QUICK wizard. (wi00965415)
- Net Direct applet does not work on Fedora 14. (wi01015358)
- Multiple clients behind the same NAT device cannot make simultaneous L2TP/IPsec connections. (wi00571477, Q02037954)

- Avaya VPN Gateway Node/Cluster may restart due to underlying kernel BUG in inode.c:1157. See Product Support Note *PSN004039* for more information. (wi01096774)
- When used for IPsec based connections, the Avaya VPN Gateway 3050/3070 NetOctave cryptographic accelerator card used for offloading cryptographic functions from the local CPU is subject to random lockups over time. See Product Support Note PSN004038u for more information. Customers are advised to move to VM appliance 3050-VM/3070-VM/3090-VM. (wi01019295)
- TCP port 3390 will be in Listening mode on a Windows XP, Vista, 7 or 8 machine if Windows Media Center is enabled and Windows Media Center extenders have been configured. As a result RDP WTS port forwarders using the default recommended port 3390 may fail if this condition applies. (wi01150400)
- Users may be unable to launch the Microsoft RDP ActiveX client in Windows 7 and above due to increased security restrictions imposed by Internet Explorer. See http://msdn.microsoft.com/en-us/library/aa382994%28v=vs.85%29.aspx. Work around is to navigate to **IE Tools** > **Internet Options** > **Security** > **Trusted Sites** > **Site** and manually add AVG URL to trusted zone. A restart of your browser is required for changes to take effect. (wi01151431)

Appendix A: Compatibility Matrix

This chapter provides the compatibility matrixes for Avaya VPN Gateway Release 10.0.1.0.

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 matrixes for Avaya VPN Gateway Release 10.0.1.0

The following tables provide compatibility matrixes for the Avaya VPN Gateway Release 10.0.1.0.

Compatibility matrix — Windows

Table 1: Compatibility matrix — Windows 32–bit operating systems

Application	Windows 32–bit Operating System Version			
	Vista	7	8	8.1
Portal Mode	Supp	Cert	Cert	Supp
Port Forwarder	Supp	Cert	Cert	Supp
Net Direct	Supp	Cert	Cert	Supp
L2TP	Supp[1]	Supp[1]	Supp[1]	Supp[1]
Contivity 6.x 7.x	Unsup	Unsup	Unsup	Unsup
VPN Client 10.01	Supp[1]	Unsup	Unsup	Unsup
VPN Client 10.04–10.06	Supp	Cert	Cert	Supp
WTS/ RDP	Supp	Cert	Cert	Supp

1 — Supported but not certified in 10.0.1.0 release.

Table 2: Compatibility matrix — Windows 64–bit operating systems

Application	Windows 64–bit Operating System Version			
	Vista 64-bit	7 64–bit	8 64–bit	8.1 64-bit
Portal Mode	Supp	Supp	Supp	Cert
Port Forwarder	Supp	Supp	Supp	Cert
Net Direct	Supp[1]	Supp[1]	Supp	Cert
L2TP	Supp[2]	Supp[2]	Supp[2]	Supp[2]
Contivity 6.x 7.x	Unsup	Unsup	Unsup	Unsup
VPN Client 10.01	Supp[2]	Unsup	Unsup	Unsup
VPN Client 10.04–10.06	Supp	Supp	Supp	Cert
WTS/ RDP	Supp	Supp	Supp	Cert

1 — Net Direct applet on Windows 64–bit is Supported on 32–bit browsers.

2 — Supported but not certified in 10.0.1.0 release.

Compatibility matrix — MAC

Table 3: Compatibility matrix — MAC

Applications	MAC OS – 10.4	MAC OS – 10.5	MAC OS – 10.6	MAC OS – 10.7	MAC OS – 10.8	MAC OS – 10.9
Portal Mode	Supp[2]	Supp[2]	Supp[2]	Supp[2]	Supp[2]	Supp[2]
Port Forwarder	Supp[2]	Supp[2]	Supp[2]	Supp[2]	Supp[2]	Supp[2]
Net Direct	Supp[1, 2]	Supp[1, 2]	Supp[1, 2]	Supp[1, 2]	Supp[1, 2]	Supp[1, 2]
L2TP	Supp	Supp	Supp	Cert	Cert	Cert
Contivity 6.x 7.x	x[3]	x[3]	x[3]	x[3]	x[3]	x[3]
VPN Client 10.x	x	x	x	x	x	x
WTS/ RDP	Supp[2, 4]	Supp[2, 4]	Supp[2, 4]	Supp[2, 4]	Cert[2, 4]	Cert[2, 4]
ICA Client	Supp[2, 5]	Supp[2, 5]	Supp[2, 5]	Supp[2, 5]	Supp[2, 5]	Supp[2, 5]

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

2 — Supported but not certified in 10.0.1.0 release.

3— MAC / Linux support provided by third party clients where applicable. Mac OS X users should upgrade to Net Direct for future deployments and Linux users may leverage open source clients such as shrew.net. Use of open source clients are solely the responsibility of the customer to test and support.

4— RDP only works in Java mode.

5— ICA client only works in Java mode.

Compatibility matrix — other operating systems

Table 4: Compatibility matrix — other operating systems

Applications	Redhat	Fedora Core	Solaris
Portal Mode	Supp[2]	Supp[2]	Supp[2]
Port Forwarder	Supp[2]	Supp[2]	Supp[2]
Net Direct	Supp[2]	Supp[1, 2]	x
L2TP	Supp	Supp	x
Contivity 6.x 7.x	x[3]	x[3]	x[3]
VPN Client 10.x	x	x	x
WTS/ RDP	Supp[2, 4]	Supp[2, 4]	Unsup
ICA Client	Supp[2, 5]	Supp[2, 5]	Unsup

1— View Known Issues: Net Direct applet does not work in Fedora 14 (wi01015358)

2 — Supported but not certified in 10.0.1.0 release.

3— MAC / Linux support provided by third party clients where applicable. Mac OS X users should upgrade to Net Direct for future deployments and Linux users may leverage open source clients such as shrew.net. Use of open source clients are solely the responsibility of the customer to test and support.

4— RDP only works in Java mode.

5— ICA client only works in Java mode.

Compatibility matrix — mobile

Table 5: Compatibility matrix[1] — mobile

Applications	Blackberry	iPhone – 2.1	iPhone and iPad – iOS 4.2.1	Windows Mobile – 6.1
Portal Mode	x	x	x	x
Port Forwarder	x	x	x	x
Net Direct	x	x	x	x
L2TP	x	Supp[1, 2]	Supp[1, 2]	Supp[1]
Contivity 6.x 7.x	x	x	x	x
VPN Client 10.x	x	x	x	x
WTS/ RDP	x	x	x	x

Applications	Blackberry	iPhone – 2.1	iPhone and iPad – iOS 4.2.1	Windows Mobile – 6.1
ICA Client	x	x	x	x

1 — Supported but not certified in 10.0.1.0 release.

2 — Check Known Issues for unsupported features.

Compatibility matrix — Android

Table 6: Compatibility matrix — Android

Authentication type	2.3.6	3.1	4.0	4.1
Pre-shared key	Supp	Supp[1, 2]	Supp[1, 2]	Supp[1, 2]
Certificate	Supp	Supp	Supp	Supp

1 — Check the Known limitations section in the release notes.

2 — Supported but not certified in 10.0.1.0 release.

Compatibility matrix — IP Phones

Table 7: IP Phones matrix

IPsec Authentication type	Phone models		
	11xx	96x0	96x1
Pre-shared key	Supp	Supp	Unsup
Certificate	Supp	Unsup	Unsup

Compatibility matrix of backend servers

Table 8: Backend server matrix

Backend Servers	Portal mode	Port forwarder
OWA 2003	Supp[3]	Supp[3]
OWA 2007	Supp[3]	Supp[3]
OWA 2010	Cert	Cert
SharePoint 2003	Supp[3]	Supp[3]
SharePoint 2007	Supp[3]	Supp[3]

Backend Servers	Portal mode	Port forwarder
SharePoint 2010	Unsup[1]	Unsup[1]
Lotus Domino 7.0	Supp[3]	Supp[3]
Lotus Domino 8.0	Supp[2, 3]	Supp[2, 3]
Lotus Domino 8.5	Unsup[1, 2]	Unsup[1, 2]
RSA Soft token	Supp[3]	Supp[3]
Citrix-4.0	Supp[3]	Supp[3]
Citrix-4.5	Supp[3]	Supp[3]
Citrix-5.0	Supp[3]	Supp[3]
Citrix-6.5	Cert	Supp
Windows 2003 server	Supp[3]	Supp[3]
Windows 2008 server	Supp[3]	Supp[3]

1 — Uses Net Direct or the Avaya VPN client.

2 — Supported only on IE 6/7/8 http://www-10.lotus.com/ldd/dominowiki.nsf/dx/Supported_Browsers_in_Lotus_iNotes_by_Domino_Release

3 — Supported but not certified in 10.0.1.0 release.

Compatibility matrix of AVG VMware Appliance

Table 9: AVG VMware Appliance matrix

VMware Platform	3050-VM	3070-VM	3090-VM
VMware ESX Server 3	Supp	Supp	x
VMware ESX Server 3.5	Supp	Supp	x
VMware ESX Server 4.0	Supp	Supp	x
VMware ESXi Server 3.0	Supp	Supp	x
VMware ESXi Server 3.5	Supp	Supp	x
VMware ESXi Server 4.1	Supp	Supp	x
VMware ESXi Server 5.0	Supp	Supp	Supp
VMware ESXi Server 5.1*	Cert	Cert	Cert
VMware ESXi Server 5.5**	Cert	Cert	Cert
VMware Workstation	Unsup	Unsup	x
VMware Server	Unsup	Unsup	x
VMware Player	Unsup	Unsup	x
Microsoft Hyper-V	Unsup	Unsup	x

*VMware ESXi Server 5.1.0 update 1 (build 1065491)

**VMware ESXi Server 5.5.0 update 2 (build 1623387)

Compatibility matrix of VPN Branch Office Tunnel devices

Table 10: VPN Branch Office Tunnel device matrix

VPN Branch Office Tunnel device	Supported*
AVG 3050/3050–VM	Yes
AVG 3070/3070–VM	Yes
AVG 3090–VM	Yes
VPN Router (formerly 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.

*Supported but not certified in 10.0.1.0 release.

Compatibility matrix of third party applications with operating systems

Table 11: Third party compatibility matrix with Windows 32–bit operating systems

Browser	Windows 32–bit Operating System Version			
	Vista	7	8	8.1
IE 6	x	x	x	x
IE 7	Supp	x	x	x
IE 8	Supp	Supp	x	x
IE 9	Supp	Cert[1]	x	x
IE 10	x	Supp	Cert	x
IE 11	x	Supp	x	Supp
Firefox 3.x	Supp	Supp	Supp	x
Firefox 4.x and above	Supp	Cert	Cert	Supp

Browser	Windows 32–bit Operating System Version			
	Vista	7	8	8.1
Safari 3.x-5.x	Supp	Supp	Supp	Unsup

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

Table 12: Third party compatibility matrix with Windows 64–bit operating systems

Browser	Windows 64–bit Operating System Version			
	Vista 64–bit	7 64–bit	8 64–bit	8.1 64–bit
IE 6	x	x	x	x
IE 7	Supp	x	x	x
IE 8	Supp	Supp	x	x
IE 9	Supp	Supp[1]	x	x
IE 10	x	Supp	Supp	x
IE 11	x	Cert	x	Cert
Firefox 3.x	Supp	Supp	Supp	Supp
Firefox 4.x and above	Supp	Cert	Supp	Cert
Safari 3.x-5.x	Supp	Supp	Supp	Unsup

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

Table 13: Third party compatibility matrix with operating systems — other operating systems

Applications	MAC	Redhat	Fedora
IE 6.x-11.x	x	x	x
Firefox 3.x	Supp[1]	Supp[1]	Supp[1]
Firefox 4.x and above	Supp[1]	x	x
Safari 3.x-4.x	Supp[1]	x	x
Safari 5.x-7.x	Supp[1]	x	x

1 — Supported but not certified in 10.0.1.0 release.

Appendix B: Related Resources

Getting technical documentation

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

1. Point your browser to http://support.avaya.com.

   To download you must do one of the following:

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

   Enter your login credentials in the **Username** and **Password** fields then click **Log In**.

   Once you are registered or signed in the support pane appears.
2. Select **Downloads & Documents** and then enter **VPN Gateway 3050** or **VPN Gateway 3070** in the product field.
3. Select the Release or **Don't Know** if you do not know the release number.
4. Select **Documents** as the content type and click **Enter**.

Training

Product training is available on the Avaya Learning website. For more information or to register, see http://avaya-learning.com.

Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support web site, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support web site, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

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.