Release Notes
Avaya VPN Gateway

Release 9.0.11.0
NN46120-400
Issue 20.01
November 2013

© 2013 Avaya Inc.

All Rights Reserved.

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 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 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 website: http://support.avaya.com. 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. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

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 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, 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.

CPU License (CP). End User may install and use each copy 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 that 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”). 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. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

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. 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 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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Comments? infodev@avaya.com

Contents

Chapter 1: Introduction 7
- Purpose 7
- Related Resources 7
  - Getting technical documentation 7
  - Training 8
  - Avaya Mentor videos 8
  - Support 8

Chapter 2: New in this release 9
- Features 9
  - Time Format for SMB browser Portal users 9
- Other changes 11

Chapter 3: Licenses 13

Chapter 4: Software installation and upgrade notice 15
- SSL VPN Server software 15
- Server software download 16
- Avaya SSL VPN client 16
- Avaya VPN Client (formerly Contivity) 16
- Avaya Net Direct installable client 17
- Disk repartitioning for upgrade or downgrade from Release 7.x to 9.0 or later 17
- Upgrading from versions earlier than 2.0.11.15 17
- Downgrading to versions prior to 5.1.5.4 17
- Downgrading to 5.1.5.4 or later 18
- Reload license after upgrade 19
- Downgrade IE Cache Wiper Cab, Net Direct Cab, and SODP ActiveX files 19
- VM Appliance Package 20

Chapter 5: Supported platforms 21

Chapter 6: Resolved issues 23

Chapter 7: Known limitations 25
- VPN limitations 25
- Secure Portable Office client 25
- Net Direct client 25
- Avaya Endpoint Access Control Agent 27
- Avaya VPN Client (formerly Contivity VPN Client) 27
- Avaya SSL VPN Client 27
- Portal 28
- Other limitations 30
- General 31

Chapter 8: Known issues 33
- VM Appliance Package 33
- OVF Template menu in vSphere Client 4.1 fails to install AVG OVA package 33
- Portal 33
- Secure Portable Office and Portal 34
- Browser-Based Interface 36
- Miscellaneous 36

Appendix A: Compatibility Matrix **39**
Compatibility matrixes for Avaya VPN Gateway Release 9.0.11.0 ..... **39**
Compatibility matrix — Windows **39**
Compatibility matrix — MAC **41**
Compatibility matrix — other operating systems **42**
Compatibility matrix — mobile **43**
Compatibility matrix — Android **44**
Compatibility matrix — IP Phones **44**
Compatibility matrix — SPO Native mode **45**
Compatibility matrix — SPO virtualized mode **45**
Compatibility matrix of backend servers **46**
Compatibility matrix of AVG VMware Appliance **47**
Compatibility matrix of VPN Branch Office Tunnel devices **47**
Compatibility matrix of third party applications with operating systems **48**

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).

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

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com.

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

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.

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.

Ceedo Enterprise (CE) application is used in conjunction with the Avaya Secure Portable Office (SPO) solution. Ceedo Enterprise user documentation should be consulted as part of the use of SPO. Ceedo's technical support should be contacted for any issues involving CE application virtualization. http://www.ceedo.com/company/ceedo-support-center.html

Chapter 2: New in this release

The following sections detail what is new in *Avaya VPN Gateway – Release Notes* for Release 9.0.11.0.

Features

See the following sections for information about feature changes.

Time Format for SMB browser Portal users

In earlier releases, the VPN Gateway portal “SMB browser” feature displayed file or directory date and time in UTC (Coordinated Universal Time) regardless of the VPN Gateway's configured time zone. Release 9.0.11.0 introduces the option to display time stamp information based on the VPN Gateway's configured time zone in lieu of UTC format.

Time Format for SMB browser Portal users is configured using CLI or BBI.

Configuring Time Format for SMB browser Portal using CLI

In CLI, use the following command to configure time format:

1. At the prompt, enter: `cfg/vpn VPN-1/portal/`
2. At the `>>Portal#` prompt, enter: `smbtimefmt local`
3. At the `>>Portal#` prompt, enter: `diff`

   The system will display:

   ```
   Configuration/
     VPN 1/
      Portal/
       Time format display for SMB browse network: utc -> local
   ```

4. At the `>>Portal#` prompt, enter: `apply`

   The system will display:

   ```
   Changes applied successfully.
   ```

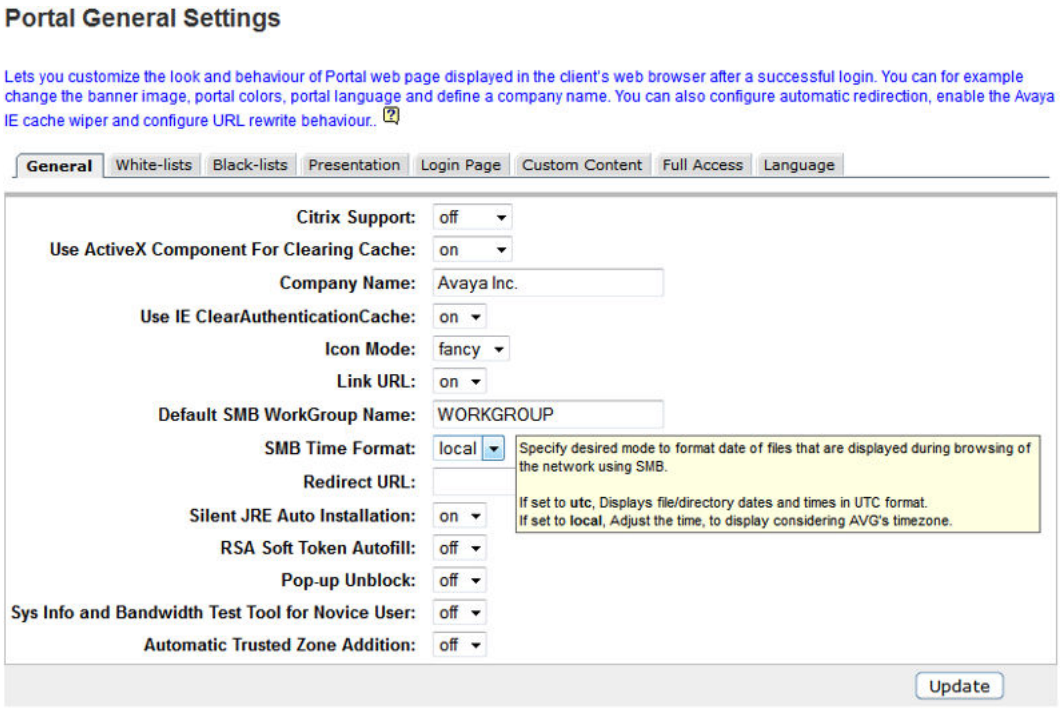
Configuring Time Format for SMB browser Portal using BBI

You can configure the time format using the **Portal General Settings** page in BBI.

To access **Portal General Settings** , use the following path:

1. Click **Config** > **VPN Gateways** > **VPN x** > **Portal** > **General**.
2. Click the arrow in the drop-down box next to **SMB Time Format** and choose **local** to show local time, or **utc** to use UTC .
3. Click **Update** to apply your selection.

The following figure shows the **Portal General Settings** screen in BBI.

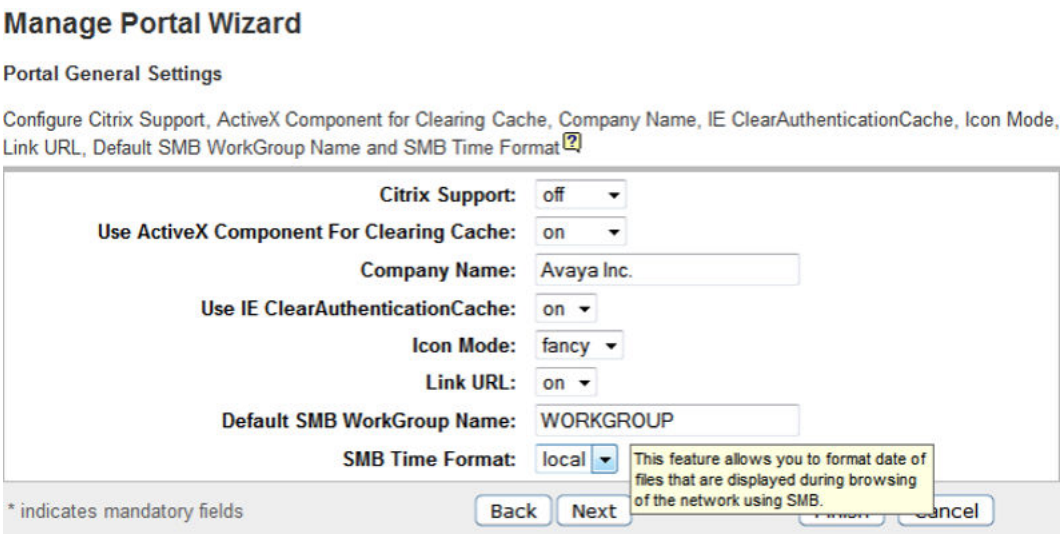


Alternately, you can configure the time format using the **Manage Portal Wizard**.

To access the **Manage Portal Wizard**, use the following path:

1. Click **Config** > **Wizards** > **Manage Portal Wizard**.
2. On the **VPN Selection** page, select the desired VPN from the existing list then click **Next**.

   The **Portal General Settings** page opens.



3. Click the arrow in the drop-down box next to **SMB Time Format** and choose **local** to show local time, or **utc** to use UTC .
4. Click **Next** to continue with the wizard, or **Finish** to save the configuration and end the wizard.

Other changes

See the following sections for information about changes that are not feature-related.

Local storage of /cfg/dump or /cfg/ptcfg for recovery

In order to facilitate recovery, each time a configuration change is applied through either CLI or BBI, a backup copy of the current configuration (/cfg/ptcfg equivalent) is saved in /tmp.

A maximum of 10 backup files are saved in /tmp (only on master nodes). The system stores the most recent 10 backup files in /tmp, with the oldest file overridden if the user attempts to save more than 10 backups.

Increased Number of Non-Debug SSL.LOG.x/IKE.LOG.x

Non-Debug SSL.LOG.x/IKE.LOG.x logs have been changed to log 10 iterations at 500kb each.

Comments? infodev@avaya.com

Chapter 3: 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 known issues with SPO licenses, see Known issues on page 33 . For more information on all license types see, *BBI Application Guide for VPN* (NN46120-102) and *CLI Application Guide for VPN* (NN46120-101).

Obtaining a license for VPN Gateway

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

Procedure

1. Send and 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 4: Software installation and upgrade notice

SSL VPN Server software

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

- **SSL-9.0.11.0-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-9.0.11.0-boot.img**

  The SSL-9.0.11.0-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-9.0.11.0-auto-install.iso**

  The SSL-9.0.11.0-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-9.0.11.0-<platform ID>.ova**

  The SSL-9.0.11.0-<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 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 27):

- Version 1.1.0.4 (LSP client): Compatible with Windows 98, ME, NT (with IE 5 or later) 2000 and XP
- Version 1.5.0.16 (TDI client): Compatible with Windows 2000 and XP

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.

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 9.0 or later

To support disk repartitioning for an upgrade or downgrade from Release 7.x to 9.0 or later 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 9.0 or later. 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 9.0 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 9.0 or later, 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 9.0 or later to 5.1.5.4 or later 5.x, the settings for the default IP pool in the 9.0 or later 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 9.0 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 Avaya EACA (as Tunnel Guard introduced in 6.0.1) feature 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 Avaya EACA (Tunnel Guard) predefined SRS entries will be lost, if the software is downgraded from 9.0 or later 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 Avaya EACA (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 causes RADIUS accounting server information inconsistency. The administrator must re-configure the RADIUS account server during this 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.

- Due to addition of AES 256 support in the 9.0.1.0 version, while downgrading to 8.0.19.0 and below, from 9.0.3.0 and above some configuration changes will be automatically done. The current behavior for downgrade to 8.0.X is as follows:
  - AES 256 values for *Diffie Hellman Groups* and *Auth and Encryption* configuration are reset after downgrade.
  - In case AES 256 was the only setting for the IKE profile, the default values will be used: 3DES with SHA for *Auth and Encryption* and Diffie Hellman group 2 for *Diffie Hellman Groups*.

Reload license after upgrade

In version 6.0.1.0, 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.

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-9.0.11.0-3050.ova
- SSL-9.0.11.0-3070.ova
- SSL-9.0.11.0-3090.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 33. For more information on the AVG OVF deployment procedure, see *VMware Getting Started Guide* (NN46120-101).

Chapter 5: Supported platforms

The AVG 9.0 server software is supported on the following platforms:

- VPN Gateway 3050
- VPN Gateway 3070
- 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 matrix of AVG VMware Appliance on page 47.

Comments? infodev@avaya.com

Chapter 6: Resolved issues

This section lists the WIs resolved in release 9.0.11.0:

Work item	Description
wi01038597	Local storage of /cfg/dump or /cfg/ptcfg for recovery.
wi01117450 wi01126149	IPsec, L2TP/IPsec and in some cases NetDirect SSL-based services become unstable when there is a large number of IPsec clients coming from same NAT device.
wi01118923	In OVID web application, when navigating between different application sections, users receive "Session Timeout" pop-up message and redirect to login page.
wi01123878	When the AVC SSL client connects to VPN Gateway, VPN Gateway delivers all AAA authentication methods in AVG instead of what is configured to the clients.
wi01127460	Portal SMB Browser shows timestamp in UTC instead of local time.

Comments? infodev@avaya.com

Chapter 7: 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.

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 the Aladdin 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

- 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 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. (wi00569539, Q01244929)

Windows

- Windows operating system supports the running of one instance of a Net Direct client.
- 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. (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 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.
  ```


Comments? infodev@avaya.com

No fix planned. (wi00569568, Q01281449)

Avaya Endpoint Access Control Agent

Version TG_1.1.2.0_001 of the installed Tunnel Guard agent is the minimum requirement to be used with the VPN Gateway. Avaya Endpoint Access Control Agent is the suggested product upgrade path for the Tunnel Guard agent.

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.

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 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

Comments? infodev@avaya.com

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.
- Starting from Windows 8, there is a limitation on sockets listening on loopback addresses 127.0.0.x (x>1) when routing table changes. (wi01109836)

  For users running Portal links with port forwarding on Windows 8 and Windows 8.1, Avaya recommends to configure links to listen on 127.0.0.1.
- 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 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".

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.
- 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)
- Issue with common host mappings for multiple port forwarder applets running at the same time on Windows XP. (wi00937551)
- The NTLM authentication might not work on some Windows XP computers. On Windows Vista and 7 it is working as expected. (wi01033631)
- 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 functionality. The 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 ineffective 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)
- 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)

Comments? infodev@avaya.com

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.
- When using the IPsec VPN client together with the installed EACA agent, the result of the EACA 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 EACA 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.
- 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)
- Deploying the OVA image on a VMware Workstation 7 fails with following error due to VMware Workstation limitation: "OVF descriptor could not be parsed" (wi01019092). The workaround is to upgrade to VMware Workstation 8 or later versions.

Comments? infodev@avaya.com

Chapter 8: 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 47.

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.
- Beginning with Java SE 7 update 10+, Oracle has introduced an auto-update mechanism (details available at http://www.java.com/en/download/faq/expire_date.xml). If the current Java version installed is 7u10+, Java will automatically start a validation against the latest JRE available when an applet is started. When using AVG with EACA enabled, on Internet Explorer, the AVG portal will display a page that requests Java to be installed. On Mozilla Firefox browser, the EACA applet will stop loading and display the message "Loading EACA". From this point, open a new browser tab or window and load the official Oracle Java page at http://www.java.com/verify to automatically update Java. (wi01117577)
- Beginning with Java SE 7 update 21+, Oracle has introduced security restrictions against mixed calls between Javascript and signed applets (details available at http://docs.oracle.com/javase/7/docs/technotes/guides/jweb/mixed_code.html). While using the AVG portal applet, you may receive a pop-up window that states **"Block potentially unsafe components from being run?**" Select "**Don't Block**" in order to continue with current application. (wi01109465)

  Avaya recommends end clients using the Avaya Endpoint Access Control Agent (EACA) upgrade to the latest available Java Runtime Environment (JRE) release provided by Oracle to ensure forward compatibility and end client security.

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)
- SPO with Application Virtualization mode does not support Port forwarder host mapping feature. (wi00568280, Q02040815)
- Authenticating with certificates in SPO virtualized environment does not work on W7/Vista. (wi00947931)
- The same message that appears when SPO Client is running on client machine x64 with no Java installed, is displayed also when Java x64 is only jre installed. (wi00986709)
- SPO: Custom PF link fails to launch the link. (wi00571239)
- No URL bar is displayed in SPO Client when no links are configured for the user group. (wi01021339)
- On clean Windows machines AVG portal fails to install Java Jre when EACA is set. (wi01032012)
- User with expired password can't change password when authenticating against LDAPS server with SPO client. (wi00945369)

- SPO doesn't error when authentication is rejected due to remote LDAP or SiteMinder server being unresponsive. (wi00971227)
- In SPO Virtualized AVG applet links doesn't start if Firefox is used and Java 1.6 is running on client PC . (wi01034058)
- EACA & AVG applet links not running in SPO Virtualized environment if client PC language is set to ASIAN format. (wi01034154)
- SPO:links are not visible in SPO Dashboard when link text is given in quotes. (wi00567976)
- Windows 7 is "unknown Windows version" to SPO. (wi00971222)
- VPN portal does not handle properly UTF-8 chars. (wi00871865)
- Selecting the path for IE x64 to be used when a link from SPO is opened, IE x86 will be used instead. (wi00986739)
- SPO does not display a banner in a rich text format. (wi00989087)
- Drop down menus do no display for a rewritten SharePoint site. (wi00834777)
- Calendar button does not appear in a rewritten SharePoint site. (wi00834781)
- External link from SPO is opened with IE no matter if browser selected to use is IE or Firefox. (wi00940109)
- Invalid profile is obtained if you want to modify an SPOClient.iso profile. (wi01010920)
- SPO downloaded software applications after were deleted from SPOClient->Apps, they still appear in Status->Software. (wi01026876)
- Outlook PF option "Start Outlook Client" from portal is not persistent. (wi01012631)
- An Internet Explorer Script Error appears when SPO is launched in native environment by a non-admin user on Windows XP x86. (wi00993820)
- Applet of port forwarding links opened in SPO with Firefox is not closed when Stop button is pressed. (wi01006146)
- No Firefox new window will be opened for a Portal http proxy link, for which New browser window option is Yes. (wi01006166)
- No Firefox new window will be opened for a SPO http proxy link, for which New browser window option is Yes. (wi01006175)
- Port Forwarder fields values should be checked before port forwarder starts. (wi00986215)
- HTML inline styles for linkset text break SPO linkset display. (wi00570936)
- SPO: The New Software message will not be displayed entirely if the name of software is long. (wi01026826)
- EACA check fails (Failed to Load Required Modules) with SPO in Virtualized environment. (wi01137749)

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)
- 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)
- 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)

Comments? infodev@avaya.com

- 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)
- OSX/iOS L2TP behind NAT fails due to malfunctioning DPD. (wi01132540)

Comments? infodev@avaya.com

Appendix A: Compatibility Matrix

This chapter provides you the following compatibility matrixes for Avaya VPN Gateway Release 9.0.11.0:

- Compatibility matrixes for Avaya VPN Gateway Release 9.0.11.0 on page 39
- Compatibility matrix of third party applications with operating systems on page 48
- Compatibility matrix of backend servers on page 46
- Compatibility matrix of AVG VMware Appliance on page 47
- Compatibility matrix of VPN Branch Office Tunnel devices on page 47

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 9.0.11.0

The following tables provide compatibility matrixes for the Avaya VPN Gateway Release 9.0.11.0.

Compatibility matrix — Windows

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

Application	Windows 32–bit operating systems				
	XP Pro	Vista	7	8	8.1
Portal Mode	Supp	Supp	Cert	Cert	Unsup
Port Forwarder	Supp	Supp	Cert	Supp	Unsup

Application	Windows 32–bit operating systems				
	XP Pro	Vista	7	8	8.1
Net Direct	Cert	Supp	Cert[1]	Supp	Unsup
Net Direct installed	Cert	Supp	Cert	Cert	Unsup
EACA	Supp	Supp	Cert	Supp	Unsup
TG/EACA portal *	Supp	Supp	Cert[2]	Cert	Unsup
SODP	Supp	Supp	Unsup	Unsup	Unsup
L2TP	Supp	Supp	Cert	Unsup	Unsup
SPO[3]	Supp	Supp	Cert	Unsup	Unsup
Contivity 6.x 7.x	Supp	Unsup	Unsup	Unsup	Unsup
VPN Client 10.01	Unsup	Supp	Unsup	Unsup	Unsup
VPN Client 10.04–10.06	Cert	Supp	Cert	Supp	Unsup
WTS/ RDP	Supp	Supp	Cert	Supp	Unsup

* Validate local JRE in the browser at http://www.java.com/verify before starting the application. (wi01117577)

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

2 — AEACA on Windows 64–bit is Supported on 32–bit browsers with 32–bit JRE.

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

Note:

Check the Known Issues section for Unsuported features.

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

Application	Windows 64–bit operating systems				
	XP 64-bit	Vista 64-bit	7 64–bit	8 64–bit	8.1 64-bit
Portal Mode	Supp	Supp	Cert	Cert	Unsup
Port Forwarder	Supp	Supp	Supp	Cert[5]	Unsup
Net Direct	Supp[1]	Supp[1]	Cert[1]	Cert	Unsup
Net Direct installed	Unsup	Unsup	Unsup	Unsup	Unsup
EACA	Supp	Supp	Cert	Cert	Unsup
TG/EACA portal *	Supp[2]	Supp[2]	Cert[2]	Cert	Unsup

Comments? infodev@avaya.com

Application	Windows 64–bit operating systems				
	XP 64-bit	Vista 64-bit	7 64–bit	8 64–bit	8.1 64-bit
SODP	Unsup	Unsup	Unsup	Unsup	Unsup
L2TP	Supp	Supp	Cert	Unsup	Unsup
SPO[3]	Supp	Supp	Cert	Unsup	Unsup
Contivity 6.x 7.x	Unsup	Unsup	Unsup	Unsup	Unsup
VPN Client 10.01	Unsup	Supp	Unsup	Unsup	Unsup
VPN Client 10.04–10.06	Supp	Supp	Supp	Cert[4]	Unsup
WTS/ RDP	Supp	Supp	Supp	Cert	Unsup

* Validate local JRE in the browser at http://www.java.com/verify before starting the application. (wi01117577)

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

2 — AEACA on Windows 64–bit is Supported on 32–bit browsers with 32–bit JRE.

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

4 — Avaya VPN Client is Supported on Windows 8 starting with release 10.06.200.

5 — Port Forwarder on Windows 32/64–bit on 32–bit browsers with minimum JRE 1.7u10 or 1.6u38.

Note:

Check the Known Issues section for Unsuported features.

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	Supp	Supp	Cert	Cert	Unsup
Port Forwarder	Supp	Supp	Supp	Supp	Cert	Unsup
Net Direct	Supp[1]	Supp[1]	Supp[1]	Cert[1]	Cert[1]	Unsup
Net Direct installed	x	x	x	x	x	Unsup
EACA	x	x	x	x	x	Unsup

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
TG/EACA portal	Supp[2]	Supp[2]	Supp[2]	Supp[2]	Cert	Unsup
SODP	x	Unsup	Unsup	Unsup	Unsup	Unsup
SPO[3]	x	x	x	x	x	Unsup
L2TP	Supp	Supp	Supp	Cert	Cert	Unsup
Contivity 6.x 7.x	x[4]	x[4]	x[4]	x[4]	x[4]	Unsup
VPN Client 10.x	x	x	x	x	x	Unsup
WTS/ RDP	Supp[5]	Supp[5]	Supp	Cert[5]	Cert	Unsup
ICA Client	Supp[6]	Supp[6]	Supp[6]	Supp[6]	Cert	Unsup

Note:

MAC OS X 10.9 (Mavericks) has not been tested or certified for use, therefore functionality may vary compared to OS X 10.8 (Mountain Lion).

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

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

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

4 — 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.

5 — RDP only works in Java mode.

6 — 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	Supp	Supp
Port Forwarder	Supp	Supp	Supp
Net Direct	Supp	Supp[1]	x

Comments? infodev@avaya.com

Applications	Redhat	Fedora Core	Solaris
Net Direct installed	x	x	x
EACA	x	x	x
TG/EACA portal	Supp[2]	Supp[2]	x
SODP	Unsup	Unsup	x
L2TP	Supp	Supp	x
SPO[3]	x	x	x
Contivity 6.x 7.x	x[4]	x[4]	x[4]
VPN Client 10.x	x	x	x
WTS/ RDP	Supp[5]	Supp[5]	Unsup
ICA Client	Supp[6]	Supp[6]	Unsup

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

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

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

4— 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.

5— RDP only works in Java mode.

6— 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
Net Direct installed	x	x	x	x
EACA	x	x	x	x
TG/EACA portal	x	x	x	x

Applications	Blackberry	iPhone – 2.1	iPhone and iPad – iOS 4.2.1	Windows Mobile – 6.1
SPO	x	x	x	x
SODP	x	x	x	x
L2TP	x	Supp[2]	Supp[2]	Supp
SPO[3]	x	x	x	x
Contivity 6.x 7.x	x	x	x	x
VPN Client 10.x	x	x	x	x
WTS/ RDP	x	x	x	x
ICA Client	x	x	x	x

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

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

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

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]	Supp[1]	Supp[1]
Certificate	Supp	Supp	Supp	Supp

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

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

Comments? infodev@avaya.com

Compatibility matrix — SPO Native mode

Table 8: Compatibility matrix — SPO Native mode

Applications	XP Pro 32-bit	XP 64-bit	Vista 32-bit	Vista 64-bit	Win 7 32-bit	Win 7 64-bit
Net Direct	Supp	Supp	Supp	Supp	Supp	Supp
Firefox 3.x and above	Supp	Supp	Supp	Supp	Supp	Supp
JRE 1.6	Supp	Supp	Supp	Supp	Supp	Supp
JRE 1.7	Supp[1]	Supp[1]	Supp[1]	Supp[1]	Cert[1]	Supp[1]
IE 8	Supp	Supp[2]	Supp[2]	Supp[2]	Supp	Supp[2]
IE 9	x	x	Supp	Supp[2]	Cert	Supp[2]
Portal Links	Supp	Supp	Supp	Supp	Cert	Supp

1 — AVG applets do not run on IE browser when Windows OS has ASIAN regional settings as system locale.

2 —Only IE 32–bit browser on 64–bit platform.

Compatibility matrix — SPO virtualized mode

Table 9: Compatibility matrix — SPO virtualized 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	Supp	Supp	Supp	Supp	Cert	Cert
Firefox 3.x and above	Supp	Supp	Supp	Supp	Supp	Supp
Java JRE 1.7	Supp[2]	Supp[2]	Supp[2]	Supp[2]	Supp[2]	Supp[2]
IE 8	Supp	Supp[3]	Supp	Supp[3]	Supp	Cert[3]
IE 9	x	x	Supp	Supp[3]	Cert[3]	Supp[3]
Portal Links	Supp	Supp	Supp	Supp	Cert	Supp
2050 IP softphone	Supp	Supp	Supp	Supp	Supp	Supp
One-X Agent	Supp	Supp	Supp	Supp	Supp	Supp

Applications	XP Pro 32-bit	XP 64-bit	Vista 32-bit	Vista 64-bit	Win 7 32-bit	Win 7 64-bit
Contact Center Express Desktop	Supp	Supp	Supp	Supp	Supp	Supp

1— SPO Virtualized Mode on CDROM is not supported.

2— AVG applets do not run on IE browser when Windows OS has ASIAN regional settings as system locale.

3—Only IE 32–bit browser on 64–bit platform.

Compatibility matrix of backend servers

Table 10: Backend server matrix

Backend Servers	Portal mode	Port forwarder	SPO
OWA 2003	Supp	Supp	Supp
OWA 2007	Supp	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	Supp	Supp	Supp
Citrix-6.5	Supp	Supp	Supp
Windows 2003 server	Supp	Supp	Supp
Windows 2008 server	Supp	Supp	Supp

Comments? infodev@avaya.com

1 — Uses Net Direct or the Avaya VPN client.

Compatibility matrix of AVG VMware Appliance

Table 11: 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	Cert	Cert	Cert
VMware ESXi Server 5.1*	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)

Compatibility matrix of VPN Branch Office Tunnel devices

Table 12: 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 Branch Office Tunnel device	Supported
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.

Compatibility matrix of third party applications with operating systems

Table 13: Third party compatibility matrix with Windows 32–bit operating systems

Browser	Windows 32–bit Operating System Version				
	XP	Vista	7	8	8.1
IE 6	Supp	x	x	x	x
IE 7	Supp	Supp	x	x	x
IE 8	Cert	Supp	Cert	x	x
IE 9	x	Supp	Cert[1]	x	x
IE 10	x	x	Cert	Cert	x
IE 11	x	x	Unsup	x	Unsup
Firefox 3.x	Supp	Supp	Supp	Supp	Unsup
Firefox 4.x and above	Supp	Supp	Cert	Cert	Unsup
Safari 3.x-5.x	Supp	Supp	Supp	Supp	Unsup

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

Comments? infodev@avaya.com

Table 14: Third party compatibility matrix with Windows 64–bit operating systems

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

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

Table 15: Third party compatibility matrix with operating systems — other operating systems

Applications	MAC	Redhat	Fedora
IE 6.x-9.x	x	x	x
Firefox 3.x	Supp	Supp	Supp
Firefox 4.x and above	Supp	x	x
Safari 3.x-4.x	Supp	x	x
Safari 5.x-6.x	Cert	x	x

Comments? infodev@avaya.com