Avaya VPN Client for FIPS 140-2 Release Notes – Client Software Release 7.11.101

Avaya VPN Client
Release 7.11.101

Document Status: **Standard**

Document Number: **NN46110-413**

Document Version: **02.01**

Date: **December 2010**

© 2010 Avaya Inc. All Rights Reserved.

Notices
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
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) 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 this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

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

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

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

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(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(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.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

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

Contents

New in this release. 7

Features 7
Other changes 7
Preface 9

Before you begin 9
Text conventions 9
Related publications 11
Overview 13

Supported platforms 13
FIPS 140-2 support 14
New features 14
Issues and considerations 15

Customer issues fixed in this release 15
Avaya VPN Client considerations 17
Avaya VPN Client 7.11 upgrade fails on new Win2000 machine 17
Fast switching on Windows XP 17
Interface selection by Avaya VPN Client 17
Restricted mode operation 18
Windows 2000 delay 19
Windows 2000 or XP running as a service can present a security issue 19

Nonprivileged users can affect system phone book entries 19
Windows 2000 dialup icon in task bar issues 20
Client auto connect limitation 20
Using the comma delimiter in the DOS command line 20
Client policy definition 20
Integrated web browser conflicts 21
WinPOET incompatibility 21
Entrust internal error 21
Log off issue when running as a service 22
Reboot required after uninstalling the Client 22
Version 7.11.101 known anomalies 22
Q01377196-01—Client ISAKMP keepalive mechanism is inconsistent when using NAT Traversal 22
Restricted product—export license requirement 22

Customer service

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

Navigation

- "Getting technical documentation" on page 5
- "Getting product training" on page 5
- "Getting help from a distributor or reseller" on page 6
- "Getting technical support from the Avaya Web site" on page 6

Getting technical documentation

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

Getting product training

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

Getting help from a distributor or reseller

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

Getting technical support from the Avaya Web site

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

New in this release

The following sections details what's new in *Avaya VPN Client for FIPS 140-2 Release Notes — Client Software Release 7.11.101* (NN46110-413) for Release 7.05.100.

- "Features"
- "Other changes"

Features

There are no new features in this release.

Other changes

There are no other changes in this release.

Preface

These release notes contain the latest information about Avaya VPN Client version 7.11.101 for FIPS 140-2 certified.

For more information on FIPS 140-2, see *Avaya VPN Client Configuration — FIPS 140-2*. (NN46110-510).

Before you begin

The *Avaya VPN Client for FIPS 140-2 Release Notes — Client Software Release 7.11.101* are intended for network managers who are responsible for the Avaya VPN Client. It is assumed that you have experience with windowing systems or graphical user interfaces (GUI) and familiarity with network management.

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is **ping** <*ip_address*>, you enter **ping 192.32.10.12**
bold Courier text	Indicates command names and options and text that you need to enter. Example: Use the **show health** command. Example: Enter **terminal paging** {**off** | **on**}.

braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is **`ldap-server source {external | internal}`**, you must enter either **`ldap-server source external`** or **`ldap-server source internal`**, but not both.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is **`show ntp [associations]`**, you can enter either **`show ntp`** or **`show ntp associations`**. Example: If the command syntax is **`default rsvp [token-bucket {depth | rate}]`**, you can enter **`default rsvp`**, **`default rsvp token-bucket depth`**, or **`default rsvp token-bucket rate`**.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is **`ping`** *`<ip_address>`*, *`ip_address`* is one variable and you substitute one value for it.
`plain Courier text`	Indicates system output, for example, prompts and system messages. Example: `File not found.`
separator (>)	Shows menu paths. Example: Choose Status > Health Check.

Related publications

For more information about the Avaya VPN Router, refer to the following publications:

- *Avaya VPN Router Configuration — Client (NN46110-306)* introduces the client product and provides information about initial setup and configuration.
- *Avaya VPN Router Configuration — TunnelGuard (NN46110-307)* provides information about configuring and using the TunnelGuard feature.

Overview

The Avaya VPN Client version 7.11.101 for FIPS 140-2 certified includes software fixes and new features added since version 6.01. The Avaya VPN Client was formerly called the Contivity VPN Client.

For more information on fixes and new features see the following release notes:

- *Contivity VPN Client Release Notes* 311773-P, version 6.01
- *Avaya VPN Router Release Notes — Client Software Release 7.01* NN46110-400 (311773-R Rev 01)

Supported platforms

This client release supports the following Microsoft* operating systems:

- Windows XP Home, Windows XP Professional, and Windows XP Tablet
- Windows 2000.

Note: Version 4.91 is the last release that provides support for the Windows 98 and Windows ME operating systems.

Although you can install the client on older versions of Microsoft operating systems, Avaya provides support only for Windows XP and Windows 2000. The client is supported with all Microsoft supported service packs for each operating system.

FIPS 140-2 support

The client supports FIPS 140-2 Level 1. FIPS 140-2 is a U.S. Government federal standard that enhance the security of information when applied to software and hardware. The FIPS 140-2 publication (“Security Requirements for Cryptographic Modules”) specify requirements for the design and implementation of products that perform cryptography.

For more information on FIPS 140-2 publications and related information, see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm, and do a search on the page for Avaya.

The client also has Common Criteria EAL4+ certification. For more information on Common Criteria, see http://www.niap-ccevs.org/cc-scheme/.

New features

There are no new features with this release.

Issues and considerations

This chapter describes issues resolved since version 6.01 and considerations that apply to version 7.11.101 release of the Avaya VPN Client.

Customer issues fixed in this release

Table 1 lists customer issues from release 6.01 that are fixed in release 7.11.101.

Table 1 Customer issues fixed in version 7.11.100

CR	Description
Q00891058	A pop-up message now appears on the client's PC when the user's Entrust certificate key is updated or renewed.
Q01011549-01	Use of an Entrust certificate no longer results in a delay during logon.The Client now allows selection of a subordinate CA certificate. To avoid errors when a certificate with the same subject DN as the Issuer is present in the Intermediate store (Entrust Event Certificate) or CA certificate rollover, Avaya recommends that customers use the new Certificate Chain Verification Functions.
Q01067139	GinaClientTimeOut maximum allowable value is increased from 120 to 900 to allow a longer time-out.
Q01079047	When you use Autoconnect, you no longer receive an error message saying *Profile specified does not exist*. Autoconnect now works.
Q01190761	After a PC restart, GINA now saves the credential entered in the login window. The user does not have to re-enter the id or the domain.
Q01192465	The text box that collects the SecureID token code in the VPN Client dialog box now appears correctly after you move the Windows XP task bar to either the left or the top of the screen. The location of the text box used to change.
Q01226168	VPN Client is now compatible with the InfoExpress Client.

Table 1 Customer issues fixed in version 7.11.100 (continued)

CR	Description
Q01231046-01	You no longer receive an error message when you create a shortcut for the Client connection profile to your desktop and then click the icon.
Q01257968	The restriction on maximum number of routes for inverse split tunneling is removed. 128 routes was the maximum number allowed. The VPN Client now allows any number of these routes.
Q01297125	There is no longer a filter driver binding check failure for *Windows Mobile-based Device* adapter. The binding check algorithm is improved.
Q01304216	Data now transmits without interruption when applications send bursts of traffic over the VPN tunnel.
Q01308927	The VPN Group Password is now saved.
Q01322574	Fragmented frames are now decrypted properly by the Avaya VPN client when AES encryption is used with no compression.
Q01327368	Packets marked with a DiffServ Code Point (DSCP) value other than zero are now processed correctly. Some of these packets were discarded incorrectly, or corrupted.
Q01399631-01	MS CAPI certificate selection no longer has certificates with an empty subject.
Q01404677-02	A PC can now go to suspended mode with the VPN Client.
Q01415017	There is now a blank username field every time users launch the Client.
Q01419547-02	Entrust ID Guard now works with the V7.01Client.
Q00495667	You can now customize the title bar at the login window.

Avaya VPN Client considerations

The following sections describe Avaya VPN Client considerations. You must have admin privileges to install the VPN Client and you must copy the Client installation files to a local drive.

Note: You can lose network connectivity for a short time during the Client installation, but connectivity should return after the installation. In some instances, this causes problems with running network applications. To avoid any problems, always exit all programs before starting the installation process.

Avaya VPN Client 7.11 upgrade fails on new Win2000 machine

An upgrade may not complete after reboot on a new Win2000 machine. To workaround this issue, restart the installer and it finishes correctly.

Fast switching on Windows XP

Depending on how you install it, the VPN Client behaves differently after installing Fast User Switch in Windows XP. The VPN Client disconnects after a Fast Switch if you install it as an application. The tunnel stays up after a fast switch if you install the VPN Client as a service. As a feature, the status icon does not show up for any user other than the user who started the tunnel.

Some files do not clean up properly if you uninstall the VPN Client after a fast switch while the tunnel is active. If you do run into this situation and want to properly uninstall the Avaya VPN Client, first install it and then uninstall it.

Interface selection by Avaya VPN Client

As a feature of IPsec Mobility, the VPN Client roams to the best interface if multiple interfaces are available. Currently, the VPN Client prioritizes the interface based on its Interface Metric. For example, you can use Interface Metric to notify the VPN Client to use Ethernet over wireless.

On Windows 2000, the Interface Metric is manually set from Interface Properties > Internet Protocol (TCP/IP) Properties > Advanced > Interface Metric. Windows XP automatically sets this value based on the interface speed.

Restricted mode operation

When you start the VPN Client from the NNGINA, it must run in restricted mode. Restricted mode secures and disables some VPN Client dialog buttons and menus. The following VPN Client menu items and dialog buttons are disabled in restricted mode:

Menus:

- File Menu
  - New
  - Connection Wizard
  - Save
  - Delete
  - Create Shortcut
- Options Menu - None
- Help Menu
  - Contents
  - Search…
- Entrust tool menu
  - New
  - Open
  - Open From Smartcard
  - Password Change
  - Recover Profile
- Verisign tool menu
  - Recover
  - View File
  - Change Password

Dialog buttons:

- Challenge Response Token Options
  - *Browse* disabled
- Screen Saver Settings Incorrect
  - *Control Panel >>* disabled

Successful completion of the tunnel connection and the Windows logon restores these controls.

If the tunnel is terminated and you remain logged on to the system, the restricted mode is not restored. You have full control of the VPN Client options when you successfully complete a Windows logon.

Windows 2000 delay

After rebooting a Windows 2000 PC, you may not be able to run the Client immediately because Windows has not completed the startup. If you try to run the Client during this period, there is a delay before you see the Client application.

Windows 2000 or XP running as a service can present a security issue

When installed as a service to provide domain login, the Client runs under the LOCAL SYSTEM account as an interactive service. This means that all dialog boxes presented to you on that system are running under the system account and may provide access to other users' files on that system. If this is an issue, install and run the Client as an application.

Nonprivileged users can affect system phone book entries

On the Windows 2000 platform, you can modify or delete entries from the All Users phone book.

Windows 2000 dialup icon in task bar issues

When installed as a service to provide domain login, the Client remains running when you log off and then log on to the Windows NT domain, reachable on the private side of the switch. When you connect using a dialup connection, those dialup connections created for All Users persist over a logoff/logon sequence, and appear in the task bar when the Client logs back on. Dialup connections created as user dialup connections persist over a logoff/logon sequence, but are not available in the task bar after you log on. This is a problem when trying to disconnect the dialup connection.

Create the dialup connections for All Users if you plan to use the domain login feature. Another option is to invoke the dialup connection by name from the system start menu: Start > Settings > Network and Dialup connections > YourDialupName. By selecting a dialup connection, you activate the application that alerts the Microsoft Dialup application to repaint the icon on the task bar.

Client auto connect limitation

The maximum number of auto connect networks is 32.

Using the comma delimiter in the DOS command line

You cannot enter a comma as a parameter at the DOS command line prompt, because the comma is used as the parameter delimiter.

Client policy definition

Because the password expiration check now uses port 586, you must define TCP client port 586 within your Client policy to ensure that the policy does not fail. When the Client needs to connect to a remote port that is greater than 1024 and, at the same time, the local port number is also greater than 1024, the Client must specify the Client rules separately, as shown in the following example:

```
Tcp: Local (10.44.128.240:1068) Remote (192.10.155.2:8088)
State (Established)
```

or

```
Tcp: Local (10.4.127.102:1068) Remote (192.35.217.195:17027))
State (SYN_Sent)
```

In both cases, the remote ports are greater than 1024. You can no longer define the wildcard policy rules as follows to cover either case:

```
TCP Client 0
UDP Client 0
```

You need separated Client policy rules in this situation.

Integrated web browser conflicts

America Online* V5.0 web browser is not supported. America Online V5.0 includes an integrated web browser that uses a web proxy. The integrated web browser conflicts with the use of IPsec and PPTP tunnels.

With an IPsec or PPTP tunnel running, you cannot access any web sites while using the AOL V5.0 integrated web browser. Do not use the AOL V5.0 integrated web browser. Use another web browser, such as Internet Explorer or Netscape Navigator.

WinPOET incompatibility

Versions 2.1 and earlier of WinPOET are incompatible with intermediate filter drivers, including the VPN Client filter driver. This problem is resolved in later versions of WinPOET.

Entrust internal error

If you use the Connection Wizard to request an Entrust Digital Certificate and log on as a user without administrative privileges, you may see “Error: open of log file failed.” If you see “Error: open of log file failed; error 13 File ....\other\elog.cpp LINE 721,” it indicates that you do not have access rights to certain Entrust files or directories.

Log off issue when running as a service

When you run the VPN Client as a service under Windows 2000 or Windows XP, you may not be able to log off after you log on and log off several times. This is a known Windows issue when using an NT service with an active GUI interface. The workaround for this issue is to first disconnect the VPN Client service and then log off.

Reboot required after uninstalling the Client

You should reboot the PC if you plan to install the VPN Client immediately after uninstalling a previous version. Failing to reboot the PC after uninstalling, and before installing the new version, can cause driver errors.

Version 7.11.101 known anomalies

The following sections describe issues that Avaya has determined need to be corrected in a future release, but are not fixed in the current release.

Q01377196-01—Client ISAKMP keepalive mechanism is inconsistent when using NAT Traversal

When a Client connects, it sends a NAT Traversal keepalive and an ISAKMP keepalive every 18 seconds. If an ISAKMP keepalive response does not respond to the client, the client stops sending the ISAKMP keepalives every 18 seconds and starts sending the ISAKMP keepalives at one-half the failover tuning timer rate (whatever it is set for). This behavior makes it difficult to troubleshoot Client keepalive issues.

Restricted product—export license requirement

This product incorporates encryption technology that is highly restricted and can require an export license from the US Department of Commerce, Bureau of Export Administration, prior to international shipment.

A product that incorporates encryption with a key length up to 56 bits can be eligible for international shipment pursuant to a license exception. However, any product that incorporates encryption technology exceeding 56 bits requires an export license from the US Department of Commerce.

Pursuant to such license, the product can be marketed and sold only to a limited class of international users. Any entity, other than Avaya, that wants to export this product must first obtain license approval from the US Department of Commerce.

Further, the user of this product cannot re-export, transfer, or divert the product to any country to which such re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries, or provide the product to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.