

Version 6.01

Part No. 311773-P Rev 00  
September 2005

600 Technology Park Drive  
Billerica, MA 01821-4130

# **Contivity VPN Client Release Notes**

**NORTEL**

## Copyright © Nortel Networks 2005. All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

## Trademarks

Nortel Networks, the Nortel Networks logo, and Contivity are trademarks of Nortel Networks.

ActivCard is a trademark of ActivCard Incorporated.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

America Online and AOL are trademarks of America Online, Inc.

Datakey is a trademark of Datakey, Inc.

Entrust is a trademark of Entrust Technologies, Inc.

iPlanet, Java, and Sun Microsystems are trademarks of Sun Microsystems, Inc.

Microsoft and Windows are trademarks of Microsoft Corporation.

Netscape, Netscape Communicator, Netscape Directory Server, and Netscape Navigator are trademarks of Netscape Communications Corporation.

Steel-Belted Radius is a trademark of Funk Software, Inc.

The asterisk after a name denotes a trademarked item.

## Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

## Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

---

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

## **Nortel Networks Inc. software license agreement**

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

**1. Licensed Use of Software.** Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

**2. Warranty.** Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

**3. Limitation of Remedies.** IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN

ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

#### **4. General**

- a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).
- b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.
- c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.
- d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
- e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
- f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

---

# Contents

---

## Preface

Before you begin .....	7
Text conventions .....	7
Related publications .....	9
Hard-copy technical manuals .....	9

## Chapter 1 Overview

Supported platforms .....	11
New features .....	11
Differentiated services code point (DSCP) .....	12
CVC coexists with Microsoft Windows IPsec Policy Service .....	12
Banner improvements .....	12
Entrust Roaming Profiles .....	12
Using the 0.0.0.0/0 subnet wildcard with Inverse split tunneling .....	13
Clickable link in TunnelGuard Agent .....	13
No required reboot on fresh installs .....	13

## Chapter 2 Issues and considerations

Customer issues fixed in this release .....	15
Contivity VPN Client known issues .....	18
Q01126528 — CVC6.01: Cannot save as NEW Profile .....	18
Contivity VPN Client considerations .....	18
Fast switching on Windows XP .....	19
Interface selection by Contivity VPN Client .....	19
Restricted mode operation .....	19
Windows 2000 delay .....	20

Windows 2000 or XP running as a service can present a security issue . . . . .	21
Non-privileged users can affect system phone book entries . . . . .	21
Windows 2000 dialup icon in task bar issues . . . . .	21
Client auto-connect limitation . . . . .	21
Using the comma delimiter in the DOS command line . . . . .	22
Client policy definition . . . . .	22
WinPOET incompatibility . . . . .	23
Entrust internal error . . . . .	23
Improper configuration parameter for Dynamic DNS . . . . .	23
Windows XP known problem . . . . .	23
Log off issue when running as a service . . . . .	24
Reboot required after uninstalling the client . . . . .	24

---

## Preface

---

These release notes contain the latest information about Nortel\* VPN Client Version 6.01.

### Before you begin

The *Contivity VPN Client Release Notes* are intended for network managers who are responsible for the Contivity Secure IP Services Gateway. 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.<br>Example: If the command syntax is <b>ping &lt;ip_address&gt;</b> , you enter <b>ping 192.32.10.12</b> |
| <b>bold Courier text</b> | Indicates command names and options and text that you need to enter.<br>Example: Use the <b>show health</b> command.<br>Example: Enter <b>terminal paging {off   on}</b> .  |

braces ({} )	<p>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.</p> <p>Example: If the command syntax is <b>ldap-server source {external   internal}</b>, you must enter either <b>ldap-server source external</b> or <b>ldap-server source internal</b>, but not both.</p>
brackets ([ ] )	<p>Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command.</p> <p>Example: If the command syntax is <b>show ntp [associations]</b>, you can enter either <b>show ntp</b> or <b>show ntp associations</b>.</p> <p>Example: If the command syntax is <b>default rsvp [token-bucket {depth   rate}]</b>, you can enter <b>default rsvp</b>, <b>default rsvp token-bucket depth</b>, or <b>default rsvp token-bucket rate</b>.</p>
<i>italic text</i>	<p>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.</p> <p>Example: If the command syntax is <b>ping &lt;ip_address&gt;</b>, <i>ip_address</i> is one variable and you substitute one value for it.</p>
plain Courier text	<p>Indicates system output, for example, prompts and system messages.</p> <p>Example: File not found.</p>
separator ( > )	<p>Shows menu paths.</p> <p>Example: Choose Status &gt; Health Check.</p>



## Related publications

For more information about the Contivity Secure IP Services Gateway, refer to the following publications:

- *Configuring the Contivity VPN Client* introduces the client product and provides information about initial setup and configuration.
- *Configuring TunnelGuard for the Contivity Secure IP Services Gateway* provides information about configuring and using the TunnelGuard feature.

## Hard-copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to [www.nortel.com/documentation](http://www.nortel.com/documentation), find the product for which you need documentation, and locate the specific category and model, or version, for your hardware or software product. Use Adobe\* Acrobat Reader\* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems website at [www.adobe.com](http://www.adobe.com) to download a free copy of the Adobe Acrobat Reader.

## How to get Help

This section explains how to get help for Nortel products and services.

### Getting Help from the Nortel Web site

The best source of support for Nortel products is the Nortel Support Web site:

<http://www.nortel.com/support>

This site enables customers to:

- download software and related tools
- download technical documents, release notes, and product bulletins
- sign up for automatic notification of new software and documentation
- search the Support Web site and Nortel Knowledge Base
- open and manage technical support cases

## **Getting Help over the phone from a Nortel Solutions Center**

If you have a Nortel support contract and cannot find the information you require on the Nortel Support Web site, you can get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the Web site below and look up the phone number that applies in your region:

<http://www.nortel.com/callus>

When you speak to the phone agent, you can reference an Express Routing Code (ERC) to more quickly route your call to the appropriate support specialist. To locate the ERC for your product or service, go to:

<http://www.nortel.com/erc>

## **Getting Help through a Nortel distributor or reseller**

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

---

# Chapter 1

## Overview

---

The Nortel Contivity VPN Client (CVC) Version 6.01 release includes software fixes and new features added since Version 5.01. These release notes contain the latest information about the client.

### 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 the client may install on older versions of Microsoft operating systems, Nortel provides support only for Windows XP and Windows 2000. The client works with all service packs available for each operating system.

### New features

Version 6.01 provides support for:

- Differentiated services code point (DSCP)
- CVC to coexist with Microsoft IPsec service
- Banner improvements
- Entrust roaming profile support

- Using the 0.0.0.0/0 subnet wildcard in inverse split tunneling
- Clickable link in TunnelGuard Agent
- No required reboot on fresh installs

## Differentiated services code point (DSCP)

DSCP is a 6-bit field in an IP header that identifies the priority of service a packet receives in the network. The client copies the inner IP header DSCP to the outer IP header in the tunnel. DSCP is aware that the network can now prioritize the IPsec stream.

## CVC coexists with Microsoft Windows IPsec Policy Service

The CVC does not disable Microsoft IPsec automatically. If the CVC detects that IPsec service is active, it tries to bring up a UDP tunnel. In order for this to work, you must enable NAT traversal on the server.

## Banner improvements

The improvements to the security banners are as follows:

- The user can click on a URL that is embedded in the banner.
- New buttons added are:
  - Accept/Close—allows traffic to flow and the dialog closes.
  - Accept—allows traffic to flow, the Security banner remains visible, and all links are clickable.
  - Cancel—terminates the tunnel immediately.

## Entrust Roaming Profiles

A roaming certificate resides on an external server. When a user enrolls for a certificate, their certificate is deposited on the roaming server rather than on the user PC or smartcard. The user logs in to Entrust Entelligence, authenticates to the roaming server, and receives their certificate, which they then use to authenticate Entrust ready applications, such as VPN.

## Using the 0.0.0.0/0 subnet wildcard with Inverse split tunneling

The 0.0.0.0/0 is simply a wildcard to be expanded. The option to perform auto-detection of directly-connected local subnets is provided by adding a subnet of 0.0.0.0 with a 0.0.0.0 mask to the inverse split tunnel networks list on the CES. When the CVC receives the list of inverse split networks, it expands the 0.0.0.0 to be all of the directly-connected local subnets detected on the host. Any additional subnets in a list are processed as before.

After expansion, traffic destined for these subnets is allowed to flow outside of the tunnel. While this option is valid for both the Inverse Split and Inverse Split (Locally Connected) modes, it is useful only for the first variant. The subnets generated by the 0.0.0.0/0 expansion always pass the Locally Connected test because, by definition, they must be locally connected. Any additional subnets listed are duplicates of the wildcard expansion; otherwise, they do not pass the test.

## Clickable link in TunnelGuard Agent

TunnelGuard Agent presents an error message on desktop PCs whenever an SRS rule fails. This error message is comprised of an SRS rule name and an SRS comment. The SRS comment has clickable links that provide rule-specific locations to download information for compliance in cases where the user fails to comply. Any text with a URL, such as <http://>, <https://>, or <ftp://>, automatically transforms to a clickable link.

## No required reboot on fresh installs

You are no longer required to reboot the PC after completing a fresh installation.



---

## Chapter 2

# Issues and considerations

---

This chapter describes issues resolved since Version 5.01 and considerations that apply to the Version 6.01 release of the Contivity VPN Client.

## Customer issues fixed in this release

[Table 1](#) lists customer issues from release 5.01.100 that are fixed in this release.

**Table 1** Fixed customer issues from release 5.01.100

CR	Description
Q00585585	An enhancement added to the CVC supports Entrust roaming.
Q00960762	Enhanced IPsec Mobility feature works with Dial-up network adaptors.
Q00828114	The CVC does not disconnect a dialup connection if the profile is locked.
Q00946282	An enhancement added to the CVC allows you to change the PAP auth password. This requires Contivity switch version 5_07 and above.
Q00946190	A feature added to the CVC for MSCAPI Auto Select allows the user to create a connection profile in the CVC that selects MS-Certificate automatically.
Q00988376	The CVC has a security issue whereby system files are accessed through the VPN Client that is installed as a service.
Q00935371	If you use the CLI to establish a VPN tunnel, it creates a log file which contains the username and password on the PC, in cleartext. This posed a potential security issue.
Q00988116	An enhancement allows IPSec traffic to tunnel through SSL.
Q00947915	When you do a search on the Friendly name field of the certificate, the Friendly name is now displayed in the certificate field.

[Table 2](#) lists customer issues from release 5.01.102 that are fixed in this release.

**Table 2** Fixed customer issues from release 5.01.102

CR	Description
Q01005516	The profile command line option does not work when specifying an auth parameter.
Q00995640	ISAKMP packet fragmentation can cause a tunnel failure using certificates and some SOHO NAT routers. A new registry option chooses to use a random source port in place of the standard port 500 for ISAKMP exchanges.
Q00995640	The mandatory CRL checking is removed, and a new registry option allows you to enable or disable CRL checking.
Q01011549	CAPI subject DN is not unique.
Q01023914	LDAP Proxy password change must identify the change failure.
Q00936652	Failover is not working properly with DNS.

[Table 3](#) lists customer issues from release 5.01.103 that are fixed in this release.

**Table 3** Fixed customer issues from release 5.01.103

CR	Description
Q01022800	Enhancing the client (when installed as a service) so that it performs updates as local system instead of local server, allows DDNS updates to existing host records on the DNS server.
Q00995640	The mandatory CRL checking is removed, and a new registry option allows you to enable or disable CRL checking.
Q00936652	Entrust roaming profile users were not able to switch to on-line mode properly. Entrust files were updated to resolve this issue.
Q00988376	During the configuration of a new VPN session on the Contivity VPN Client, system files are accessed by non-administrator accounts.
Q01005516	The profile command line option does not work when specifying an auth parameter.
Q01011549	CAPI subject DN is not unique.
Q01011809	The Contivity VPN Client logs a success in client log for failed DDNS updates.
Q01023914	LDAP Proxy password change must identify the change failure.
Q01025141	A user can disable the EAC filter binding, which allows for the split tunnel feature to be bypassed.



[Table 4](#) lists customer issues from release 5.01.106 that are fixed in this release.

**Table 4** Fixed customer issues from release 5.01.106

CR	Description
Q01048123	The eNTServCtrl.log contains passwords in clear text when command line option switches are upper case.
Q01071143	The CVC checks all available drivers from the registry to ensure that they bind to the eacfilt driver. This check fails if <i>Odyssey Network Services</i> is also bound to the driver.
Q01053858	IKE keepalives are sent at incorrect intervals in configurations with IPSec Aware NAT.
Q01053804	IKE keepalives are sent each 500ms in configurations without EDPUDP encapsulation.
Q01053859	IKE keepalives are not sent in configurations with IPSec Aware NAT when ESP traffic is sent.
Q01037600	The CVC GINA does not clear auto-logon credentials when the logon processor returns an error.
Q00977609	Installing the Sygate Agent configured for 402.1x authentication on a PC that also has the CVC loaded can result in a Windows exception error.

[Table 5](#) lists customer issues from release 5.01.110 that are fixed in this release.

**Table 5** Fixed customer issues from release 5.01.110

CR	Description
Q01073265	The CVC checks all available drivers from the registry to ensure that they bind to the eacfilt driver. The code to do so did not differentiate between physical and virtual interfaces.
Q01089203	There are connection problems through UDP encapsulated tunnels connecting to a Shasta server that does not support the Quote of the Day banner.

[Table 6](#) lists customer issues from release 6.01 that are fixed.

**Table 6** Fixed customer issues from release 6.01

CR	Description
Q01121346	Encrypt/delete the user's password in memory while CVC is running. Refer to Tech Bulletin 2005005619.

## Contivity VPN Client known issues

The following section describes Contivity VPN Client known issues.

### Q01126528 — CVC6.01: Cannot save as NEW Profile

There is an incompatibility between Zone Lab's Integrity client and Contivity clients versions 4.91 and later. Zone Lab's Integrity server writes extra parameters to the .tbk file (where profiles are stored), which interferes with the operation of the Contivity Client. The result is that you cannot edit or create a new profile. You must remove the following from the .tbk file:

[]

Integrity Server=

Contact Zone Labs for an upgrade to resolve this issue.

## Contivity VPN Client considerations

The following sections describe Contivity VPN Client considerations. You must have admin privileges to install the Contivity VPN client. Also, copy the client installation files to a local drive.



**Note:** Network connectivity can be lost for a short time during the client installation, but should return after the installation connectivity. In some instances, this can cause problems with currently running network applications. To avoid any problems, always exit all programs before starting the installation process.

---

## Fast switching on Windows XP

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

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

## Interface selection by Contivity VPN Client

As a feature of IPsec Mobility, the Contivity VPN Client roams to the best interface if multiple interfaces are available. Currently, the Contivity VPN Client prioritizes the interface based on its Interface Metric. For example, you can use Interface Metric to notify the Contivity 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 the Contivity VPN Client is launched from the NNGINA, it must run in a restricted mode. This mode secures and disables some Contivity client dialog buttons and menus. The following Contivity 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

User access to these controls is restored upon successful completion of the tunnel connection and the Windows log on.

If the tunnel is terminated and the user remains logged on to the system, the restricted mode is not restored. The user has full control of the options provided by the Client when they successfully complete a Windows logon.

## **Windows 2000 delay**

After rebooting your 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 that are presented to a user 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.

## **Non-privileged users can affect system phone book entries**

On the Windows 2000 platform, users 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 a user logs off and then logs in to the Windows NT domain, reachable on the private side of the switch. When users 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 in. Dialup connections created as user dialup connections persist over a logoff/logon sequence, but are not available in the task bar after a user logs in. 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. It is no longer sufficient to 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. 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 are unable to 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 Contivity 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 in 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.

## Improper configuration parameter for Dynamic DNS

If Dynamic DNS is enabled (which is the default), the Contivity VPN Client uses Windows services to update DNS servers with its IP address. If Dynamic DNS parameters are incorrectly set, the Contivity VPN Client user interface or the status icon can become non-responsive when the Contivity VPN Client uses the incorrect parameters to communicate with the DNS server.

Nortel suggests that you disable Dynamic DNS if you do not plan to use it. However, if you use this feature, ensure the parameters are correct and the DNS Server is functional.

## Windows XP known problem

An error occurs when running an InstallShield Professional 6.x setup on a Windows XP PC with service pack 1 and Windows XP Hotfix Q328310 applied. Nortel recommends that you install the Windows XP fix available to download from Microsoft Knowledge Base article 329623. Click the *Download the 329623 package now* link in the article.

Although not recommended, if the Windows XP fix does not work, temporarily uninstall the problematic Windows XP Hotfix Q328310, then reinstall the setup. Ensure that you reinstall Windows XP Hotfix Q328310. For more information about Windows XP Hotfix Q328310, see Microsoft Knowledge Base article 328310.

## **Log off issue when running as a service**

When the Contivity VPN Client is running as a service under Windows 2000 or Windows XP, you may not be able to log off after you log in and log off several times. This is a known Windows issue when an NT service is involved with an active GUI interface. To work around the problem, you must first disconnect the Contivity VPN Client service and then log off.

## **Reboot required after uninstalling the client**

Users should reboot the PC if they plan to install the Contivity Client immediately after un-installing a previous version. Failing to reboot the PC after uninstalling, and before installing the new version, could cause driver errors.