

Version 5.01

Part No. 311773-N Rev 00
May 2004

600 Technology Park Drive
Billerica, MA 01821-4130

Contivity VPN Client Release Notes

NORTEL
NETWORKS™

Copyright © 2004 Nortel Networks

All rights reserved. May 2004.

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	7
Before you begin	7
Text conventions	7
Related publications	9
Hard-copy technical manuals	9
How to get help	9
Chapter 1	
Overview	11
Supported platforms	11
New features	11
Restricted product - export license requirement	12
Chapter 2	
Issues and considerations	13
Contivity VPN Client known anomalies	13
Q00917913 - Installing over previous version disables logging	13
Q00901531 - Installing from a network share not supported	13
Contivity VPN Client considerations	14
Fast switching on Windows XP	14
Interface selection by Contivity VPN Client	14
Restricted mode operation	15
IE5 subdirectory removed	16
Verisign Certificate Database and tool kit	16
Windows 2000 delay	16
Windows 2000 or XP running as a service can present a security issue	17
Non-privileged users can affect system phone book entries	17
Windows 2000 dialup icon in task bar issues	17

Client auto-connect limitation	17
Using the comma delimiter in the DOS command line	18
Client policy definition	18
Windows XP and Windows 2000 driver signing message	19
No duplicate dialup information screen	20
Auto Connect works only with WinSock applications	20
Native Windows client using L2TP over IPsec	20
Shared uninstall (InstallShield ID)	20
Driver names conflict	20
Entrust Negotiator dll	21
WinPOET incompatibility	21
Prompt for Ipsecw2k.sys file during installation	21
Using wizard to setup Axent Soft token	21
Entrust internal error	21
Improper configuration parameter for Dynamic DNS	22
Windows XP known problem	22
Inconsistent TokenType and UseTokens initialization	22
Connection problems caused by NAT devices	23
ActivCard PIN change alters certificate profile password	23
WebRamp and SonicWall cannot connect multiple PCs	23
Smart Card 330 with Datakey reader issue	23
Switching Smart Card readers	23
Log off issue when running as a service	24

Preface

These release notes contain the latest information about Nortel Networks* Contivity* VPN Client Version 4.91.

Before you begin

The *Contivity VPN Client Release Notes* are intended for network managers who are responsible for the Contivity Secure IP Services Gateway. They assume that you have experience with windowing systems or graphical user interfaces (GUIs) 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 ({})	<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 ldap-server source {external internal}, you must enter either ldap-server source external or ldap-server source internal, 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 show ntp [associations], you can enter either show ntp or show ntp associations.</p> <p>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.</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 ping <ip_address>, <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 > 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 the www.nortelnetworks.com/documentation URL. Find the product for which you need documentation. Then 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 Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to get help

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

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortelnetworks.com/cgi-bin/comments/comments.cgi URL, then click on Technical Support.

From the Technical Support page, you can open a Customer Service Request online or find the telephone number for the nearest Technical Solutions Center. If you are not connected to the Internet, you can call 1-800-4NORTEL (1-800-466-7835) to learn the telephone number for the nearest Technical Solutions Center.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the <http://www.nortelnetworks.com/help/contact/erc/index.html> URL.

Chapter 1

Overview

The Nortel Networks Contivity VPN Client Version 5.01 release includes bug fixes and new features added since Version 4.91. 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 Networks will provide support only for Windows XP and Windows 2000. The client works with all service packs available for each operating system.

New features

Version 5.01 provides support for:

- IPSec mobility, which allows IPSec connections to be maintained for mobile users, allowing them to roam from subnet to subnet without losing the VPN tunnel.

- Inverse split tunneling, which provides the ability to specify specific networks that are allowed access outside of a mandatory tunnel. You can also configure an option that allows only locally-connected subnets to be accessed.

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 will require 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 Nortel Networks, Inc., 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.

Chapter 2

Issues and considerations

This chapter describes issues since Version 4.86_100 and considerations that apply to the Version 5.01 release of the Contivity VPN Client.

Contivity VPN Client known anomalies

The following sections describe Contivity VPN Client issues.

Q00917913 - Installing over previous version disables logging

If you install Version 5.01 over Version 4.91, which has logging enabled, logging is disabled on Version 5.01.

Q00901531 - Installing from a network share not supported

Installing the client from a network share is not supported. When the VPN drivers are installed, Windows will temporarily interrupt the connection and may cause the installation to fail. Nortel Networks recommends that you copy the kit to a temporary area on the target PC and start the installation from that location. After the installation, the temporary kit may be deleted safely.

Contivity VPN Client considerations

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



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

Fast switching on Windows XP

Depending on how it's installed, the Contivity VPN Client behaves differently after Fast User Switch in Windows XP. The Contivity VPN Client will disconnect after a Fast Switch if it's 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 might not be properly cleaned up if you uninstall the Contivity VPN Client after a fast switch while the tunnel is active. If you do run into this situation and would like to properly uninstall the Contivity VPN Client, first install it and then and uninstall it.

Interface selection by Contivity VPN Client

As a feature of the IPsec Mobility, the Contivity VPN Client will try to roam to a better 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 can be 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 for some reason the tunnel is terminated and the user remains logged on to the system, the restricted mode will not be restored. The user will have full control of the options provided by the Client because they have successfully completed a Windows logon.

IE5 subdirectory removed

The Ie5 subdirectory under the tools directory has been removed from the Contivity VPN Client CD. This directory contained the ie5setup.exe file for Microsoft Internet Explorer Version 5.5.

Verisign Certificate Database and tool kit

The Verisign tool kit and the Verisign proprietary digital certificate store is no longer supported in the Contivity VPN Client when creating new or renewed Verisign certificates. Current Verisign certificates will continue to work when making a VPN connection. New Verisign Certificates should be stored in the MS-CAPI certificate store.

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 will be 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, you should 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.

You should 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 use the comma as a parameter that you enter 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
```

The separated client policy rules are needed under this situation. Using the 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*.

Windows XP and Windows 2000 driver signing message

Depending on how Windows XP or Windows 2000 is configured, you may receive a driver signing warning message. To prevent this message from appearing, you can change a setting in the control panel.

To disable driver signing on a system running Windows XP:

- 1 From the Start menu, choose Settings > Control Panel > Performance and Maintenance.
- 2 Choose the system icon.
- 3 Choose Hardware.
- 4 Click on the driver signing button.
- 5 Write down the current driver signing value.
- 6 Click on the ignore - install the software any, don't ask for my approval button.

To disable driver signing on a system running Windows 2000:

- 1 From the Start menu, choose Settings > Control Panel > System.
- 2 Click on the Hardware tab.
- 3 Click on the Driver Signing button and write down the current setting.
- 4 Select the Ignore - Install all files, regardless of file signature button.
- 5 Click on OK.
- 6 You can now install Version 4.65 of the client. After the installation completes, return the setting to the value.

After you install the client software, you can reset the driver signing value to the value that you previously wrote down.

No duplicate dialup information screen

In previous versions of the client, if you tried to get a new Entrust certificate using the wizard, you would be asked twice for dialup information. In Version 4.10 and higher, the second (duplicate) screen asking for dialup information has been removed, and the Remote Access Service (RAS) connection is kept until the certificate is successfully retrieved. For all wizard-initiated RAS connections, if you stop the wizard by clicking on the Cancel button, the connection is lost; however, the connection remains up for existing user-initiated RAS connections.

Auto Connect works only with WinSock applications

Client Auto Connect works only with applications that open WinSock connections. If you try to access external resources from the Network Neighborhood, the Run dialog box, or Internet Explorer, the Auto Connect feature does not work.

Native Windows client using L2TP over IPsec

The native Windows VPN client must be disabled while Contivity VPN Client is used. The Contivity VPN Client disables the windows native client automatically at installation time and performs periodic checks to make sure it's disabled.

Shared uninstall (InstallShield ID)

Uninstalling the client also removes any client versions 2.62 or later (even if each version is in its own unique directory) since the InstallShield log that is used is shared by both versions.

Driver names conflict

If you want multiple versions of the client on a single system, there is a conflict between the 4.10 and higher driver names and the older client driver names. If you subsequently decide to uninstall the 4.10 client, you must also uninstall the 3.70 client.

Entrust Negotiator dll

The default Entrust.ini file, which is generated during the 5.0PKI installation, has FIPS enabled (FIPSmode=1). To use the 5.1.100.361 Entrust Negotiator dll, you must disable FIPS (FIPSmode=0).

WinPOET incompatibility

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

Prompt for Ipsecw2k.sys file during installation

Occasionally the installation program asks you to supply the Ipsecw2k.sys file. Usually this is the result of re-installing the client in a new location. If this occurs, you see a dialog box prompting for this file. Click on the Browse button. The folder path will be the product folder where you are installing the client, for example, \myclient\Drivers. Select the Ipsecw2k.sys file and click on OK to continue the installation procedure.

Using wizard to setup Axent Soft token

Occasionally, if you are running the client on Windows 2000 with a limited amount of memory, using the wizard to configure the Axent soft token causes high CPU usage. This can occur when the Contivity VPN Client is unloading the Axent Defender soft token DLL while using the Connection Wizard.

Entrust internal error

If you are using the Connection Wizard to request an Entrust Digital Certificate and logged 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 by 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 might become non-responsive while the Contivity VPN Client is using the incorrect parameters to communicate with the DNS server.

Nortel Networks suggests disabling Dynamic DNS if you are not planning to use it. However, if you use this feature, make sure 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 Networks recommends that you install the Windows XP fix available to download from Microsoft Knowledge Base article 329623. Click on the Download the 329623 package now link in the article.

Although not recommended, if this does not work you could temporarily uninstall the problematic Windows XP Hotfix Q328310. Then reinstall the setup making sure that you reinstall Windows XP Hotfix Q328310. For more information about Windows XP Hotfix Q328310, see Microsoft Knowledge Base article 328310.

Inconsistent TokenType and UseTokens initialization

When you create a custom client profile and set the TokenType and UseTokens initialization inconsistently, you could see an inconsistent display of the desired authentication method. Select Options > Authentication Options and click on OK to fix the screen. This changes the screen for the TokenType selected in the profile and persistently changes the user profile. For more information on the TokenType and UseTokens setup, see “Configuring client profiles” in the *Configuring the Contivity VPN Client* document.

Connection problems caused by NAT devices

The Contivity VPN Client must use NAT Traversal to be able to establish an IPsec tunnel through a NAT device that does not support IPsec. If you are unable to make a connection or receive “The secure Contivity connection has been lost” error message, it indicates that NAT traversal is not enabled. Contact your site administrator to make sure that this feature is enabled.

ActivCard PIN change alters certificate profile password

If you use the ActivCard utility to change the ActivCard PIN, the existing Contivity VPN Client certificate profile logon password also changes to the new value.

WebRamp and SonicWall cannot connect multiple PCs

WebRamp 700S NAT firmware version 5.1.1 and Sonic Wall/SOHO2 boxes cannot connect multiple PCs to the Contivity gateway at the same time. You must wait up to 30 seconds between each connection. Both the SonicWall and WebRamp NAT boxes fail to pass the packets on, resulting in “Remote Host Not Responding” error messages.

Smart Card 330 with Datakey reader issue

When you are using the Datakey* reader with Smart Card 330, removing and reinserting the Smart Card may cause the client to hang. To reuse the same profile, you must reboot your PC. To work around this issue, upgrade to the latest versions of these product.

Switching Smart Card readers

When switching Smart Card readers, you should first uninstall unused software. ActivCard* and Datakey write dll entries to Entrust.ini during installation. The dll entry that appears first determines which card is recognized. If you have an ActivCard reader attached to the PC, the ActivCard entry has to appear first in the Entrust.ini file. If it does not, the client does not recognize any card reader during the enrollment process and the “store profile on Smartcard” option is grayed out.

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.