Nortel VPN Client Release Notes — VPN Client Software Release 8.01

NORTEL

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

New in this release

The following sections detail what's new in *Nortel VPN Client Release Notes —
VPN Client Software Release 8.01* (NN46110-400).

- "Features"
- "Other changes"

Features

See the following sections for information about feature-related changes:

- "Cross certification" on page 7
- "Two factor authentication" on page 7
- "IGMP" on page 7

Cross certification

Nortel VPN Client 8.01 supports cross certification configurations. For more
information, see "Cross certification" on page 18.

Two factor authentication

Nortel VPN Client 8.01 supports two factor authentication. For more information,
see "New features" on page 18.

IGMP

Nortel VPN Client 8.01 supports IGMP Proxy. For more information, see "IGMP
Proxy" on page 18.

Other changes

See the following section for information about changes that are not feature-related:

-

Document changes

The following information is updated for this release:

-
-

Preface

These release notes contain the most recent information about Nortel VPN Client Version 8.01.

Before you begin

This document is intended for network managers who install and configure Nortel VPN Client. This document makes the assumptions that you have experience with windows-based systems or graphical user interfaces (GUI) and that you are familiar 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**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed.
	Example: If the command syntax is **more disk*n*:*<directory>*/...*<file_name>*,** you enter **more** and the fully qualified name of the file.
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**.
vertical line (│)	Separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when entering the command.
	Example: If the command syntax is **terminal paging** {**off** │ **on**}, you enter either **terminal paging off** or **terminal paging on**, but not both.

Related publications

For more information about the Contivity VPN Client, see the following
publications:

*   *Contivity VPN Client Configuration — Client* (NN46110-306) provides
    information to install and configure client software for the Client.

*   *Contivity VPN Client Configuration — TunnelGuard* (NN46110-307)
    provides information to configure and use the TunnelGuard feature.

*   *Nortel VPN Router Upgrades — Server Software Release 8.0* (NN46110-407)
    provides information to upgrade the server software to the most recent release.

*   *Nortel VPN Router Installation and Upgrade — Client Software Release 8.01*
    (NN46110-409) provides information to upgrade the Nortel VPN Client to the
    most recent release.

*   *Contivity VPN Client Configuration — Basic Features* (NN46110-500)
    introduces the product and provides information about initial setup and
    configuration.

*   *Contivity VPN Client Configuration — SSL VPN Services* (NN46110-501)
    provides instructions to configure services on the SSL VPN Module 1000,
    including authentication, networks, user groups, and portal links.

*   *Nortel VPN Router Configuration — Advanced Features* (NN46110-502)
    provides configuration information for advanced features such as the
    Point-to-Point Protocol (PPP), Frame Relay, and interoperability with other
    vendors.

*   *Contivity VPN Client Configuration — Tunneling Protocols* (NN46110-503)
    provides configuration information for the tunneling protocols IPsec, Layer 2
    Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol (PPTP), and
    Layer 2 Forwarding (L2F).

*   *Contivity VPN Client Configuration — Routing* (NN46110-504) provides
    instructions to configure the Border Gateway Protocol (BGP), Routing
    Information Protocol (RIP), Open Shortest Path First (OSPF), Virtual Router
    Redundancy Protocol (VRRP), Equal Cost Multipath (ECMP), routing policy
    services, and client address redistribution (CAR).

*   *Contivity VPN Client Using the Command Line Interface* (NN46110-507)
    provides syntax, descriptions, and examples for the commands that you can
    use from the command line interface (CLI).

*   *Contivity VPN Client Configuration — Firewalls, Filters, NAT, and QoS*
    (NN46110-508) provides instructions to configure the Stateful Firewall and
    Client interface and tunnel filters.

- *Contivity VPN Client Security — Servers, Authentication, and Certificates* (NN46110-600) provides instructions to configure authentication services and digital certificates.

- *Contivity VPN Client Troubleshooting — Server* (NN46110-602) provides information about system administrator tasks such as recovery and instructions to monitor VPN Router status and performance. This document provides troubleshooting information and event log messages.

- *Nortel VPN Router Administration* (NN46110-603) provides information about system administrator tasks such as backups, file management, serial connections, initial passwords, and general network management functions.

- *Contivity VPN Client Troubleshooting — Client* (NN46110-700) provides information to troubleshoot installation and connectivity problems with the Nortel VPN Client.

Printed technical manuals

To print selected technical manuals and release notes for free, directly from the Internet, go to www.nortel.com/documentation, 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 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 Web site at www.adobe.com to download a free copy of the Adobe Reader.

How to get help

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

Finding the most recent updates on the Nortel Web site

The content of this documentation was current at the time the product was released. To check for updates to the most recent documentation and software for Client, click one of the following links.

Link	Web site
Most recent software	Nortel page for **VPN Router** software located at
	support.nortel.com/go/ main.jsp?cscat=SOFTWARE&poid=12325
Most recent documentation	Nortel page for **VPN Router** documentation located at
	support.nortel.com/go/ main.jsp?cscat=DOCUMENTATION&poid=12325

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can perform the following activities:

• download software, documentation, and product bulletins
• search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
• sign up for automatic notification of new software and documentation for Nortel equipment
• open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also 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 following Web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to the following Web site:

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, contact the technical support staff for that distributor or reseller.

Chapter 1
Overview

The Nortel VPN Client Version 8.01 includes software fixes made after the release of Nortel VPN Client 7.01.251.

Nortel no longer supports Version 5.01. If you use 5.01, you must upgrade to a more recent version.

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.

> **Note:** Nortel provides two versions of the VPN Client that supports Windows Vista, version 6.07.

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

New features

The following section identifies the new features in Nortel VPN Client 8.01.

Two factor authentication

Nortel VPN Client 8.01 supports two factor authentication. If you configure two factor authentication on the router, you must supply two credentials to gain network access. One credential is something you know (a user name and password) while the other is something you store on the workstation or on a card (a certificate).

Nortel VPN Client reacts to XAUTH messages it receives from Nortel VPN Router. If the client receives an XAUTH message, a dialog box appears in which you must type the user name and password. The username and password and the certificate authentication code combine. After both authentication methods are complete, the success dialog box appears.

Cross certification

Nortel VPN Client 8.01 supports cross certification for VPN users using Entrust. The type of cross certification can be hierarchical or peer-to-peer. You must select Digital Certification Authentication for Entrust as the client authentication options, and then select the appropriate Entrust certificate profile. For more information about cross certification, see *Nortel VPN Router Configuration — Servers, Authentication, and Certificates* (NN46110-600).

IGMP Proxy

The VPN Router uses Internet Group Management Protocol (IGMP) Proxy to appear to an IGMP client as an IGMP router. In turn, the VPN Router appears to the multicast network as an IGMP client. The VPN Router proxies IGMP requests to the network on behalf of the IGMP client. To use IGMP with Nortel VPN Client 8.01, you must configure the client to use split tunneling. For more information, see *Nortel VPN Router Configuration — Routing* (NN46110-504).

4096 bit certificates

Nortel VPN Client 8.01 increases the maximum size of a certificate from 2048 bits to 4096 bits.

Entrust toolkit updated with latest DLLs

Nortel VPN Client 8.01 is updated with the following latest DLLs for the Entrust toolkit:

- kmpapi32.dll version - 6.0.555.1258
- enterr.dll version - 6.0.520.1295

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 Nortel, 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 resolved and considerations that apply to Version 8.01 of the Nortel VPN Client.

Customer issues fixed in this release

There are no fixed CRs to report at this time.

Nortel VPN Client considerations

You must have administrator privileges to install the Nortel 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 returns after the installation. In some instances, this interruption causes problems with running network applications. To avoid problems, always exit all programs before you start the installation process.

Upgrade procedure for Nortel VPN Client 6.01 and earlier

Warning: Failure to perform these steps can result in unexpected behaviors.

Due to a problem with the Install Shield used in Nortel VPN Client (NVC) 6.01 and earlier, the upgrade to NVC 8.01 may fail. The upgrade can cause a screen dump on the client computer. Nortel strongly recommends that you manually uninstall NVC 6.01 and earlier before you install NVC 8.01.

You must perform the following procedure to ensure a successful upgrade. If you install NVC 8.01 by using automated methods, the script must follow this procedure.

1. Save a copy of the present Baynet.tbk file which can be found in the default installation directory C:/Program Files/Nortel Networks.

2. Manually uninstall the Nortel VPN Client by using Add/Remove Programs or the uninstall shortcut.

3. Restart the client computer.

4. Start the NVC 8.01 installer.

5. Change the name of the Baynet.tbk file to Profiles.dat and move it to the C:/ Programs Files/Nortel/Nortel VPN Client.

6. The group password can be reentered if a Custom Client is used. If the Custom Client is not used then the group passwords will be lost.

Fast switching on Windows XP

Depending on how you install it, the Nortel VPN Client behaves differently after you install Fast User Switch in Windows XP. The 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 client as a service. As a feature, the status icon does not show up for a user other than the user who starts the tunnel.

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

Interface selection by Nortel VPN Client

As a feature of IPSec Mobility, the Nortel VPN Client roams to the best interface if multiple interfaces are available. Currently, the client prioritizes the interface based on the interface metric. For example, you can use the interface metric to instruct the client to use Ethernet over wireless.

On Windows 2000, configure the interface metric manually from Interface Properties, Internet Protocol (TCP/IP) Properties, Advanced, Interface Metric. Windows XP automatically configures this value based on the interface speed.

Restricted mode operation

If you start the Nortel VPN Client from the NNGINA, it must run in restricted mode. Restricted mode secures and disables some client dialog buttons and menus. The following Nortel 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 terminates and you remain logged on to the system, the restricted mode is not restored. You have full control of the Nortel VPN Client options after you successfully complete a Windows logon.

Windows 2000 delay

After you restart a Windows 2000 PC, you sometimes cannot run the client immediately because the Windows startup is not complete. If you try to run the client during this period, a delay occurs before you see the client application.

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

When you install the client as a service to provide domain login, the client runs under the LOCAL SYSTEM account as an interactive service. All dialog boxes on that system run under the system account and can provide access to user files on that system. If this access 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 you install the client as a service to provide domain login, the client continues to run after 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, dialup connections created for All Users persist over a logoff and logon sequence, and appear in the task bar after the client logs back on. Dialup connections created as user dialup connections persist over a logoff and logon sequence, but are not available in the task bar after you log on; this situation is a problem when you try 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 classic 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.

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 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 separate 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 Point-to-Point Tunneling Protocols (PPTP) tunnels.

With an IPSec or PPTP tunnel running, you cannot access 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 Nortel VPN Client filter driver. Later versions of WinPOETTh resolve this problem.

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 can see the following message: `Error: open of log file failed`. If the following message appears, it indicates that you do not have access rights to certain Entrust files or directories: `Error: open of log file failed; error 13 File ....\other\elog.cpp LINE 721`.

Log off issue when the client runs as a service

When you run the client as a service under Windows 2000 or Windows XP, you sometimes cannot log off after you log on and log off several times. This is a known Windows issue when you use an NT service with an active GUI interface. The workaround for this issue is to first disconnect the client service, and then log off.

Restart required after you uninstall the client

Restart the PC if you plan to install the Nortel VPN Client immediately after you uninstall a previous version. Failing to restart the PC after uninstalling, and before installing the new version, can cause driver errors.

Version 8.01 known anomalies

There are no known anomalies to report at this time.