Nortel VPN Gateway

Release Notes - Software Release 7.1

Release: 7.1
Document Revision: 02.01

www.nortel.com

NN46120-400 216372-W

Nortel VPN Gateway
Release: 7.1
Publication: NN46120-400
Document status: Standard
Document release date: 14 July 2008

Export

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or reexport may be required by the U.S. Department of Commerce.

Licensing

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software developed by the Apache Software Foundation http://www.apache.org/.

This product includes a TAP-Win32 driver derived from the CIPE-Win32 kernel driver, Copyright © Damion K. Wilson, and is licensed under the GPL.

See Appendix D, "License Information", in the *Users Guide* for more information.

Contents

Release Notes

This document describes the new features and enhancements introduced in this release. It also provides details on the software installation, upgrade instructions, supported hardware, licenses, and limitations in software for the Nortel Virtual Private Network Gateway.

For a list of related publications, see “Related documentation” (page 43). The documentation suite for Nortel Virtual Private Network Gateway can be found on the documentation CD included with the software or on the Nortel technical documentation website http://www.nortel.com/support. For more information, see “How to get help” (page 45).

The following topics are discussed in this document:

Licenses

The following licenses are available to enhance the capabilities of the Nortel VPN Gateway (NVG) software.

- SSL/IPSec License
- IPsec User License
- Secure Service Partitioning License
- Portal Guard License
- Transitions Per Second (TPS) License
- Demo License
- Emergency Recovery Access (ERA) License
- Secure Portable Office License

For information on these licenses see, *BBI Application Guide (NN46120-102) and CLI Application Guide (NN46120-101).*

New features/enhancements in software version 7.1

This section summarizes the new features:

Secure Portable Office

The Secure Portable Office (SPO) client provides Virtual Private Network (VPN) access from portable storage such as Universal Serial Bus (USB) compliant flash memory and CD-ROM. The SPO client provides enhanced mobility, portability, and security compared to traditional VPN access methods. The SPO client can be deployed and managed from the Nortel VPN Gateway (NVG) server thus simplifying SPO client distribution and updates.

This solution is ideal for providing secure remote access to employees, partners, customers, and contractors when they are mobile or in fixed locations.

Benefits

The following are the benefits of SPO:

- Business continuity
  Instant access from any PC for authorized users
- Mobile users
  Access for users who do not have their business laptop with them.
- Personal business continuity
  Access when PC is broken, lost or stolen
- Multiple user access
  Multiple user access from shared PCs.

Key features

The following are the SPO features:

- Access to enterprise applications and resources based on dynamic authentication/authorization. The access rules are based on extended profiles managed on the VPN Gateway.
- Client installed on portable flash memory can be centrally provisioned and maintained from the VPN Gateway.
- Client provides multiple stored connection profiles that can be preconfigured for end-users or easily configured by the end-users.
- Storage of application on the portable flash drive and creation of links to the applications resident on the host PC. As a result, SPO provides one interface for securely running applications that are available on the private network, USB flash drive, and host PC.
- Supports multiple authentication methods (user name password, one time password/token based, and certificate/smartcard authentication).
- New link type to associate Net Direct with applications requiring network extension mode. For example, when a VoIP client is started, Net Direct is automatically launched.
- Net Direct is automatically cached on SPO for faster connections.
- Can be run from generic USB 1.x and 2.0 flash drives, U3 USB flash drives, and from CD-ROM.
- Can be customized with corporate logo.

Note: To activate SPO Client feature, order the SPO client feature license key from Nortel and then install it. For more information on the available NVG licenses, how to order, install and activate them, see licenses section in *VPN Gateway BBI Application Guide* (NN46120-101) and *VPN Gateway BBI Application Guide for VPN* (NN46120-102).

Additional feature enhancements in this Release

The following are the additional features enhancements in this Release:

- When the administrator tries to delete an active user (aaa_cache list) from the local database using the command `/cfg/vpn 1/aaa/auth local/local/del <username>` a confirmation message, "**WARNING as active user is being deleted**" appears. The administrator can delete or allow the active user in the local database by entering **`Yes`** or **`No`** respectively.
- BBI and CLI now shows system uptime in `/info/isdlist` menu.
- The command `/cfg/dump` displays platform information along with the configuration data. The following information is displayed for command `/cfg/dump`:

- Hardware platform
- Software version
- Host IP address
- System up time
- MAC address
- Disk space used

- The new features and software fixes added in Release 7.0.3 are supported in Release 7.1.

  For more information on these features, see New Feature Enhancements in Release 7.0.3 section in Release Notes 7.0.3 (NN46120-400).

  Note: All feature enhancements and software fixes affecting user commands for Release 7.0.3 are incorporated in Release 7.1 documentation suite.

Documentation download

The documents for Nortel VPN Gateway are available for download from Nortel Customer Support website:

Step	Action
1	Point your browser to: http://www.nortel.com.
2	Under Support and Training, select **Technical Support > Technical Documentation** .
3	Select **Security & VPN** from the list.
4	Select **VPN Gateway 3050** or **VPN Gateway 3070** from the Virtual Private Networking (VPN), IPSEC, and SSL list.
5	Select the desired document from **Documentation**.

--End--

Software installation and upgrade notice

SSL VPN Server software

The SSL VPN server software is delivered in two different forms, as described following:

- **`SSL-7.1.1.0-upgrade_complete.pkg`**
  This package is the preferred method for upgrading an existing SSL VPN cluster, as the upgrade is propagated across the cluster and all current configuration is preserved.
  The upgrade procedure is described in "Performing Minor/Major Release Upgrades" in Chapter 4 in the *VPN Gateway User's Guide*.

  Note: TFTP cannot be used when upgrading to version 7.0.1 or later from an earlier version.

- **`SSL-7.1.1.0-boot.img`**
  This image resets the VPN Gateway to its factory default configuration. It must be used when a VPN Gateway with a different software installed is to be added to a cluster, to bring the additional device to the same software version as in the cluster before joining it to the cluster. The software reinstall procedure is described in "Reinstalling the Software" in Chapter 3 in the *VPN Gateway User's Guide*.

  Note: TFTP cannot be used when installing version 7.0.1 or later through the reinstall procedure.

Server software download

The server software is available for download from Nortel Customer Support website. The following is the procedure to access the site:

Step	Action
1	Point your browser to: http://www.nortel.com.

2 Under Support and Training, select **Technical Support > Software Downloads**.

3 Select **Security & VPN** from the list.

4 Select **VPN Gateway 3050** or **VPN Gateway 3070** from the Virtual Private Networking (VPN), IPSEC, and SSL list.

5 Select the desired software release which you want to download.

6 Downloading the software requires registered user name and password assigned by Nortel Customer Support.

If you are not a registered user at Nortel, click on **Register** on the left-hand column of the Nortel's Customer Support website, and follow the 5-step registration process.

--End--

Nortel SSL VPN client

The manually installable SSL VPN transparent client software is available on request. Contact Nortel Support.

The SSL VPN client comes in two versions (for limitations, see "Nortel SSL VPN Client" (page 31)):

- Version 1.1.0.4 (LSP client): Compatible with Windows 98, ME, NT (with IE 5 or later) 2000 and XP
- Version 1.5.0.9 (TDI client): Compatible with Windows 2000 and XP

Nortel IPsec VPN client (formerly Contivity)

The IPsec VPN client software can be downloaded from Nortel's Customer Support website. In the three-step Product Finder guide, select Contivity VPN Client Software.

Nortel Net Direct installable client

The Net Direct SSL VPN installable client software can be downloaded from Nortel VPN Gateway server when an internal link pointing to the server is created by the administrator. For example, https://VIP/nortel_cacheable/NetDirect_Setup.zip.

Upgrading from Releases 6.x to 7.x on Nortel Application Switch 2424-SSL

New disk repartitioning feature is available for Releases 6.0.9.0 and later to accommodate the future releases. This is due to the increase in image size from Release 6.0.7.0a (and later) and limited storage space available

in the NAS 2424-SSL. To upgrade from Releases 6.0.5.0, 6.0.7.0a, or 6.0.9.0 to Release 7.x there are specific upgrade procedures. For more information, see:

- Upgrading Release 6.0.5.0 to 7.x
- Upgrading Release 6.0.7.0a to 7.x
- Upgrading Release 6.0.9.0 to 7.x
- Upgrading from 7.0.x to 7.1.1

Upgrading from Release 6.0.5.0 to 7.x

To upgrade Release 6.0.5.0 to 7.x:

Step	Action
1	Upgrade to Release 6.0.9.0.
2	Run repartition command. For more information, see "Disk repartitioning required for Releases 5.x to 6.x on Nortel Application Switch 2424-SSL" (page 18).
3	Upgrade to Release 7.x.
	--End--

Upgrading from Release 6.0.7.0a to 7.x

The following are the options to upgrade Release 6.0.7.0a to 7.x:

- Upgrade through Release 7.x boot image.

  Note: After upgrade, the configurations are lost.

- Use the following procedure to upgrade:

Step	Action
1	Downgrade to Release 6.0.5.
2	Upgrade to Release 6.0.9.0.
3	Run repartition command. For more information, see "Disk repartitioning required for Releases 5.x to 6.x on Nortel Application Switch 2424-SSL" (page 18).

4 Upgrade to Release 7.x.

Note: All configurations are lost while upgrading through Release 7.x boot image.

--End--

Upgrading from Release 6.0.9.0 to 7.x

To upgrade Release 6.0.9.0 to 7.x:

Step	Action
1	Run repartition command. For more information, see "Disk repartitioning required for Releases 5.x to 6.x on Nortel Application Switch 2424-SSL" (page 18).
2	Upgrade to Release 7.x.

--End--

Upgrading from Release 7.0.x to 7.1.1

To upgrade Release 7.0.x to 7.1.1:

Step	Action
1	Run repartition command. For more information, see "Disk repartitioning required for Releases 5.x to 6.x on Nortel Application Switch 2424-SSL" (page 18).
2	Upgrade using SSL-7.1.1.0-upgrade_complete.pkg file.

--End--

Disk repartitioning required for Releases 5.x to 6.x on Nortel Application Switch 2424-SSL

This applies to the Nortel Application Switch 2424-SSL delivered with a software version prior to 5.0 pre-installed.

In the following text, 5.x should be interpreted as 5.x *or later*.

On this system, the existing disk partitioning does not allow for a 5.x version to be installed simultaneously with version 4.x. that is it isn't possible to do a standard upgrade from 4.x to 5.x, or from one version of 5.x to another. Software reinstall using a 5.x version is still possible.

Hence, the following applies regarding standard upgrade to version 5.x from versions prior to 5.0 for clusters that include a system of the preceding type:

Current version	Procedure
Prior to 4.2.1.11	Upgrade to 4.2.1.11 or later 4.x, repartition, and then upgrade to 5.x.
4.2.1.11 or later 4.x	Repartition before upgrade to 5.x.

When 5.x is installed, the **`/boot/software/download`** command will give an error if one or more systems of the preceding type are running in the cluster, listing the hosts that need disk repartitioning.

To support the repartitioning procedure, the following commands are present as of version 4.2.1.11:

- **`/boot/software/repartcheck`**
  Checks for and reports hosts in the cluster that need repartitioning.
- **`/boot/repartition`**
  Initiates repartitioning for the local host.
- **`/cfg/sys/cluster/host #/repartition`** (in version 4.2)
  `/cfg/sys/host #/repartition` (in version 5.x)
  Initiates repartitioning for the given host (which must be running).

These commands are hidden and are not shown in the menu or considered for auto-completion through <TAB>, because they shouldn't be used in normal operation. During the repartition, which includes two automatic reboots, the host is effectively out of service.

The time required for the repartition is approximately 7 to 10 minutes.

Note 1: It is vitally important to avoid power cycle, reset, or any other manually initiated reboot of the host while the repartition procedure is running - this may lead to a totally non-functional system.

Note 2: After repartition is completed, it will not be possible to downgrade to software versions prior to 4.2.1.8, even through software reinstall.

Note 3: When doing the repartition after an upgrade, the new SW version must be "permanent" (see Chapter 4 of the User's Guide) before the repartitioning is started. If the repartitioning is started while

the new SW version is "current", the system will be non-functional after repartitioning, requiring a complete SW reinstall using the boot.img.

Upgrading from versions earlier than 2.0.11.15

If you are currently running a software version earlier than 2.0.11.15, upgrade to version 2.0.11.15 (or a later 2.0.11.x version) prior to upgrading to version 6.x. The "intermediate" upgrade to version 2.0.11.15 is necessary to maintain your current configuration, and to provide reliable fallback in case the upgrade should fail.

Downgrading to versions prior to 5.1.5.4

NVG clusters running software version 7.0 or later cannot be downgraded directly to software versions prior to 5.1.5.4. This is due to changes in the internal database format. To downgrade such a cluster to a version lower than 5.1.5.4, first perform an intermediate downgrade to 5.1.5.4 (or later 5.x).

Downgrading to 5.1.5.4 or later

- If a ClearTrust authentication scheme has been configured, downgrading to a version prior to 6.x will fail. Delete the ClearTrust authentication scheme before downgrading.
- In version 6.x, several IP pools may exist for a VPN. In version 5.x, only one IP pool per VPN may exist in the configuration. On downgrading from 6.x or later to 5.1.5.4 or later 5.x, the settings for the default IP pool in the 6.x configuration will be kept in the 5.x configuration, provided the default IP pool is of the type **`local`**. The Net Direct and IPsec network attributes are configured accordingly. If the default IP pool in the 6.x configuration is not of the type **`local`**, the first found local IP pool (lowest number) is selected to form the IP pool in the 5.x configuration. If no local IP pool is found, the IP pool will be disabled in the 5.x configuration.
- The TunnelGuard features introduced in 6.0.1 will be filtered out during the downgrade.
- If Net Direct, IE Wiper and/or Citrix Metaframe support is set to **`group`**, the setting is changed to the respective default value.
- The TunnelGuard pre-defined SRS entries will be lost, if the software is downgraded from 7.0.x release to 6.0.x or 5.1.x release. The pre-defined SRS is introduced for the first time in 7.0.x as OPSWAT feature. It is recommended to delete the pre-defined SRS entries from TG SRS rule definitions before downgrade.
- During upgrade and downgrade, the cached version of TG admin applet can be invoked. It is recommended to delete the browser cache.

- Single TunnelGuard SRS data cannot have more than 255 pre-defined software entries.
- Due to changes in RADIUS accounting server information in the configuration. Downgrade to 6.0.x and 5.0.x release and upgrade to 7.0.x will cause RADIUS server information inconsistency. Administrator must re-configure the RADIUS account server again once upgrade back to 7.0.x again.

Reload license after upgrade

In version 6.0.1, the default license has been increased from 10 to 50 concurrent users, for SSL and IPsec connections. On upgrades from earlier versions where additional licenses (besides the default license) have been loaded to the devices, the additional license must be reloaded to make use of the extra 40 number of users in the default license.

Downgrade IE Cache Wiper Cab, Net Direct Cab, and SODP ActiveX files

If the server is downgraded, the upgraded version will not be cleaned up. That is, the object files, the IE cache wiper, Net Direct and SODP files are the originial upgraded version. You have to manually delete the IE Wiper Control cab, Net Direct cab and SODP activeX files. Follow these steps to delete the files:

Step	Action
1	Open Internet explorer.
2	From the **Tools** menu, select **Internet Options**.
3	Click **Settings**.
4	Click **View Objects**.
5	Select the files and remove.

--End--

Supported hardware platforms

The 7.1.1 server software is supported on the following hardware platforms:

- Nortel VPN Gateway 3050
- Nortel VPN Gateway 3070
- Nortel Application Switch 2424-SSL
- SSL VPN Module 1000

Note: SPO client hosting and distribution from the 2424SSL and SSL VPN Module 1000 is not supported due to device memory limitations. All other SPO features are supported.

Software - Support on Hardware that has reached MD (Manufacture Discontinued) Product Status

Software releases may operate on Hardware that has reached MD (Manufacture Discontinued) Product Status. In this situation, the Software will be supported as per the Software Standard Life Cycle Support Practice - but not to exceed twelve (12) months from date of Hardware MD (Manufacture Discontinued) and is limited to supporting only the current software release on HW at time of MD declaration.

According to the preceding principle, the hardware models Nortel SSL Accelerator 310, 410 and 310-FIPS are not supported from NVG release 6.0 and onwards.

Resolved issues

This section lists the resolved issues (CRs) since version 7.0.1:

- The TunnelGuard applet (client security check launched from the Portal) is not applicable while accessing the VPN server using installed VPN clients. It uses the installed TunnelGuard agent. (Q01297451)
- Log all access requests rejected by NVG ACLs to the syslog. (Q01476301)
- Error message does not appear when the administrator tries to delete an active user (active in portal aaa_cache list) from local data base using the command **`/cfg/vpn 1/aaa/auth local/local/del <username>`**. The administrator is not prompted to confirm if the active user still needs to be deleted and also after deleting the changes are not applied and the user is not deleted. (Q01614830)
- Certificate index added to revocation list using addx can be deleted. (Q01467922)
- While sending an E-mail using OWA (Outlook Web Access), if the client PC contains S/MIME control plugin, there is a "**Catastropic failure**" error window pop-up. This window pop-up no longer appears. (Q01743719-02)
- Fixed when using Domino iNotes, mails could not be sent successfully. (Q01737559-01)
- Fixed Net Direct crash while launching the VPN with two groups with Net Direct enabled and mobility set to group. It is recommended to set roaming values only on per VPN basis. (Q01747740)
- NDIC displays all the authentication types when Gateway IP address is entered. (Q01754941-02)
- Fixed hotmail rewrite sign up url failure. (Q01744878)
- Fixed CLI crash due to the application timeout while importing huge configuration using **`/cfg/gtcfg`**. (Q01846244)
- Fixed inconsistency in ClearTrust SSO (single sign-on) behavior. After getting connected to the NVG Portal, ClearTrust single sign-on session

cookie is received from another ClearTrust-enabled web agent (not the NVG). The Portal login page is bypassed and then the single sign-on cookie is validated against the NVG. This occurs only during the first login, but subsequent attempts fail. (Q01341726)

- Fixed server pools refreshment when several ClearTrust authorization servers or dispatchers are configured on the NVG. (Q01341793)
- Fixed the issue with a generic logon failed message when a user attempts to log on with an invalid username. (Q01743544-01)
- Fixed non-validation taking place for IPSec Group Login Secret. (Q01740005)
- Fixed Full Access menu with Contivity VPN Client 7.0. (Q01690000)
- Fixed SMB/FTP-Folder size shown as 0 even though non empty files exists in it. (Q01606425)
- The new features and issues resolved in Release 7.0.3 are supported in Release 7.1.
  For more information on these features, see New Feature Enhancements in Release 7.0.3 section in Release Notes 7.0.3 (NN46120-400).

Known limitations

VPN limitation

VPN Gateway Release 7.1.0 supports 256 VPNs, even though the CLI and Web UI allows you to create 1024 VPNs. Therefore, the user should create up to 256 VPNs only.

Browser requirements

The following browsers are recommended while using the NVG software for basic Portal access, that is when not using the applets:

Basic Portal Access (no applets)

When using the NVG software for basic Portal access, that is when not using the applets, the following browsers are recommended:

- Internet Explorer 5 or later
- Mozilla 1.1 or later
- Netscape 4 or later
- Firefox 2.0
- Safari 2.0

Applet support

To support the Telnet/SSH Access, HTTP Proxy, FTP Proxy, Port forwarder applets (available on the Portal's Advanced tab) and the Citrix Metaframe applet, the following browser and Java combinations are recommended:

- Windows
  - — Internet Explorer 5 or later with Sun's JRE 1.4.2 or later
  - — Mozilla 1.5 or later with Sun's JRE 1.4.2 or later
  - — Firefox with Sun's JRE 1.4.2 or later
- Unix/Linux

  - Mozilla 1.5 or later with Sun's JRE 1.4.2 or later
  - Firefox with Sun's JRE 1.4.2 or later
- Mac OS X
  - Safari 2.0 with Sun's JRE 1.4.2 or later

TunnelGuard Applet support

To support the TunnelGuard SSL applet (used for checking the client machine), Internet Explorer 5.5 or later is recommended.

The following browsers support the TunnelGuard management applet (used for configuring SRS rules):

- Windows
  - Internet Explorer 5.5 or later
  - Netscape Navigator 7.1 or later
  - Mozilla 1.5 or later
  - Firefox 2.0
  - Java 1.4.2 or later is required

BBI support

Configuration through the Browser-Based Management Interface (BBI) is supported when the following browsers are used:

- Windows
  - Internet Explorer 5.5 or later
  - Netscape Navigator 7.1 or later
  - Mozilla 1.5 or later
  - Firefox 2.0
- Unix/Linux
  - Netscape Navigator 7.1 or later
  - Mozilla 1.5 or later

Secure Portable Office client

The Secure Portable Office Client is supported on the following browser and platform combinations:

- Windows 2000, 32 bit Operating System (OS)
- Windows XP (Home, Professional, and Media Center with latest service pack) 32 bit OS
- Windows 2003, 32 bit OS
- Windows Vista all versions 32 bit OS

Net Direct client

The Net Direct client is supported using the following browser and platform combinations:

- Internet Explorer on Windows 2000, XP, and Vista (32 bit)
- Firefox on Linux, Windows 2000, XP, and Vista (32 bit)
- Safari 2.0 on Mac OS version 10.4

The following Linux distributions have been verified to support Net Direct and Firefox:

- RedHat 7.3, Kernel 2-4-18
- RedHat 9.0, Kernel 2-4-20
- Knoppix 4.0.2, Kernel 2-6-12-4
- Fedora Core 2, Kernel 2-6-5
- Fedora Core 3, Kernel 2-6-2
- Fedora Core 4, Kernel 2-6-11
- SUSE 10.0, Kernel 2-6-16

Note: Other distributions work if they have a tun driver.

Other limitations

- The installable Net Direct client is not available for Linux and Mac OS X
- Caching of Net Direct components is not supported for Linux and Mac OS X
- Mobility Feature is not supported for MAC and Linux platforms
- If Net Direct is disconnected in improper way, restoration of DNS will fail. Few improper ways of disconnecting the Net Direct that a user should avoid are:

— Closing the portal browser when Net Direct is On.

— Clicking the Close(X) button in the title bar of the applet when Net Direct is On.

- Portal Net Direct in Vista will not work for non-administrator user. Installable Net Direct has to be used instead. For Portal Net Direct to work in Vista for user with administrator rights follow these steps:

Procedure steps

Step	Action
1	From the Control Panel, select **User Account** and **Family safety**.
2	Click **User accounts**.
3	Turn User Control **On** or **Off**.
4	Uncheck the option "**Use User Control (UAC) to protect your computer**".
5	Click **OK** and restart the Vista Client.
6	Launch the Net Direct.

--End--

TunnelGuard Agent

Version TG_1.1.2.0_001 of the *installed* TunnelGuard agent is the minimum requirement for use with the Nortel IPsec VPN client (formerly the Contivity VPN client).

Special notice for customers using both Nortel VPN Gateway (NVG) Release 7.0 or later and Nortel Secure Network Access (NSNA) Release 1.6.1 products

The installable TunnelGuard 4.0 client shipped with this release does not have all of the functionality contained in TunnelGuard 3.5 that was shipped with Nortel NSNA 1.6.1 Customers who need complete NSNA 1.6.1 and NVG 7.0 functionality should use version 4.5 of TunnelGuard which includes the full functionality of both TunnelGuard releases. Customer can get the software through their normal support channels.

Nortel IPsec VPN Client (formerly Contivity VPN Client)

Nortel IPsec VPN client versions 5.x, 6.x, and 7.x are supported.

Nortel SSL VPN Client

The installable SSL VPN client comes in two versions:

- Version 1.1.0.4 (LSP client): Compatible with Windows 98, ME, NT (with IE 5 or later), and XP. This client does not support UDP.
- Version 1.5.0.9 (TDI client): Compatible with Windows 2000 and XP. This client supports UDP as well as TCP. Native Microsoft Outlook is not supported because not fully qualified domain names cannot be resolved.
- The NVG software includes commands for allowing/rejecting access for certain SSL VPN clients, based on client version and which operating system the client currently runs on. These commands have been added as a preparation for future releases of the TDI/LSP clients, where the clients will be capable of sending version number and OS version to the NVG. Until the new TDI/LSP clients are released, existing TDI/LSP clients will be regarded as "old clients".

  — CLI path:
  `/cfg/vpn #/sslclient/tdiclient` and **`lspclient`** (these commands currently have no effect) and **`cfg/vpn #/sslclient/oldclients`**

  — BBI path:
  VPN Gateways >>VPN Client >>TDI Client and LSP Client (these options currently have no effect) and **VPN Gateways >>VPN Client >> Old Clients**.

Portal

- Proxy chaining (option to specify an intermediate HTTP Proxy host and port, for example for the Portal's Telnet/SSH and Custom Port forwarder features) is only supported if SSL is enabled on the portal server.
- Proxy chaining is not supported for the Outlook Port forwarder feature.
- Microsoft Outlook 2003 is not supported when using the Outlook Port forwarder in combination with Exchange 2003.
- Running the Outlook Port forwarder on a Windows 2000 client requires installing the latest service pack for the operating system.
- Applications using *dynamic* UDP port number allocation (for example NetMeeting, FTP and all streaming media) are not supported by the Port forwarder feature. Applications using *static* port number allocation (for example DNS, SNMP) are supported.
- When specifying a URL without a path for an iauto (automatic login) link, for example http://www.example.com, enter the URL as **`http://www.example.com/`**. This will ensure that the root path

is implied in the link. Iauto links are created using the **/cfg/vpn #/linkset #/link #/iauto** command.

- When an iauto link should be used for login to web servers using two-tier basic authentication with domain (that is one field for domain\user and one for password), the **/cfg /vpn #/linkset #/link #/iauto/mode** command must be set to **add_domain**.
- Creating a Port forwarder link for mapping a network drive is not supported on Windows 98 and XP clients.
- The features available on the Portal's Advanced tab (that is Telnet/SSH access, HTTP Proxy and Port forwarder) are supported only with SSL v3 and cipher type RC4-MD5.
- The features available on the Portal's Advanced tab are not supported for the TLS protocol.
- To create a Port forwarder link for mapping a network drive – and the link is to be used on a Windows 2003 server acting as client – port 445 has to be used instead of the suggested port 139. On the Windows 2003 server, port 445 should be disabled by following these steps:
  - Click Start, select Run and enter **regedit**. The registry editor is started.
  - Locate and select the following key: **HKLM\System\CurrentControlSet\Services\NetBT\Parameters**.
  - On the right panel, double-click the **TransportBindName** entry.
  - In the **Edit string** dialog, delete the displayed value. No value should be specified.
  - Click OK, exit the registry editor and restart the computer.
- Some SSH versions may not be supported when using the SSH feature on the Portal's Advanced tab, for example Alteon 184 SSH-1.5-1.2.27.
- Some of Microsoft's Telnet server versions may not be supported when using the Telnet feature on the Portal's Advanced tab.
- To create a WTS port forwarder link that works on Windows XP systems that have not yet been upgraded to Service Pack 2, configure the port forwarder to listen on 127.0.0.2 instead of 127.0.0.1 (localhost). Then configure the Remote Desktop client to connect to 127.0.0.2. With the Windows XP SP2 version of the Remote Desktop client, it is possible to connect to 127.0.0.1 (localhost) as long as the port being used is other than the default (3389). Note that connections through 127.0.0.2 do not work on Windows XP SP2.
- JVM 1.5 and later includes support for using the browser's certificate database. If the NVG is set to ask for client certificates, any Java

applet started during a Portal session may display a window asking for a client certificate, even though the user has already logged in to the Portal with a client certificate. The solution is to click Cancel without selecting a certificate.

- Some web applications, if started, takes over existing instances of Internet Explorer, which may cause problems for the Portal session. For example, if the Portal page is reused by a web application and the Net Direct client is running, the client will be shut down. To solve this problem in IE, go to Tools>Internet options. On the Advanced tab, under Browsing, disable the setting "Reuse windows for launching shortcuts".

General

- A maximum of 32000 sessions is allowed on the VPN Gateway 3070 with 2 GB RAM.
- The license is not part of the configuration and is also not included when exporting the configuration using the CLI command **`/cfg/ptcfg`**. If a configuration is deleted, the license is also deleted.
- When using the IPsec VPN client together with the installed TunnelGuard agent, the result of the TunnelGuard check cannot lead to an IP address being allocated from an IP pool that is assigned to an extended profile. This is because the IP address has to be allocated before the TunnelGuard check is run.

Known issues

This section lists the known issues with the NVG software.

Net Direct

- When running Net Direct on Knoppix, the tun device node must be set up manually. (Q01281449)
  To set the tun node, run the following commands as root:
  `mkdir /dev/net mknod /dev/net/tun c 10 200`
- When running Net Direct on Linux, root must be enabled on the remote user's machine and the administrator must see to it that the user account is authorized to use the command **`su root`**. (Q01278965)
- Net Direct on Windows may not be compatible with some internet security software for clients. This is expected to be fixed in the future patch releases.
- On Linux (SUSE 10.0) and Firefox, while starting Net Direct from the Portal, the message "Net Direct already running" appears in the Java applet window although the Net Direct is not started. When this error occurs, the Net Direct cannot be started.
- In Net Direct, if the administrator password configured on the NVG does not match the Windows PC client password, the browser closes sometimes.
- If the remote user runs an old version of installable Net Direct client, there is no message displayed to upgrade or continue the old version. This will be fixed in future releases.
- While using Virtual Desktop, Downloadable Net Direct can not be connected in portal mode, instead use Net Direct Installed Client. (Q01546498)
- When using Net Direct in Windows 2000 with 2 NIC's and one NIC becomes disabled, there is an issue in reconnection for Net Direct. (Q01619895)
- The Siebel portal does a client check before the application loads but fails if it is run through proxy. The application works correctly if

it is connected through Net Direct and after passing the client check through Net Direct, the site can be used through proxy without any issues. (Q01464430)

Portal

- When HTTPS is used, Internet Explorer version 7.0.2800.1106.xps p2_gdr.040517-1325. does not allow downloading or saving a file in the system (for example, files with extension .txt, .exe, .zip) though the SSL VPN server HTTP setting of **addnostore** is set to **off**.
- Outlook 2003 client does not work through native outlook port forwarder. (Q00757505)
- maxPwdAge attribute is returned before presenting a password\account expiry message to the portal user. (Q01244929)
- In Windows Vista, if you configure the proxy entry using IP address, the Internet Explorer crashes while launching port forwarders. (Q01852590)
- When a user:

  — creates a OWA link,

  — sets the `cookiedb` to **on** in the NVG, and

  — clicks on the OWA link in the portal

  iauto OWA link is not logged in automatically. The system requests for the user name and password. (Q01889808-01)
- Simpleproxy crashing when OWA link is launched through portal. (Q01893312-01)

  Workaround:

Step	Action
1	Add custom rewrite for Accept -Encoding http header in command `/cfg/vpn #/adv/rewrite`.

--End--

Secure Portable Office and Portal

- Windows Vista running on 64 bit, does not allow Active X, PFs, Citrix, WTS, and ND installation. (Q01813351)
- SPO crashes when given a client name cfg/vpn #/spoclient/name with double quotes. (Q01846937)
- In SPO client Windows Vista, the Telnet Port forwarder is not working and error is displayed. (Q01807738)
- The language lists box options for non English do not function properly. English is the only officially support language option for this release. (Q01845435)
- The extended profile access rules do not get applied to the SPO client when TunnelGuard is not configured for that group. (Q01832974)
- When the usage time increases, the system tray interface tool tips freeze and do not sync with the Dashboard interface status tab. (Q01848465)
- After starting the SPO client and launching the Virtual Desktop, the connected profile is not shown in the Dashboard status tab in the Virtual Desktop mode. (Q01849156)
- Users running SPO inside the Virtual Desktop may experience excessive delay when clicking on an SPO link. The IE instance will start but will take excessively long to navigate to the correct web page. This is seen where IE has an active plugin such as Google toolbar. The user should disable or uninstall the plug in. (Q01877432)
- Symantec On Demand Protection (SODP) has an option called Secure Mode. Secure Mode is designed to support the default web browser that comes with SODP and to disallow other applications. Secure Mode provides application isolation from the host PC by preventing any local applications from running inside the virtual desktop. With Secure Mode on, the end user will see error messages when the SPO client starts and when the user clicks on any SPO links. SPO client and SPO links will work but the user experience will interrupted by error messages. Customers may decide to run with Secure Mode off and enable SODP File Separation in order to prevent information from being saved to the PC in this scenario. (Q01885125 and Q01870880)
- The SPO client auto update feature is not compatible with CDROM deployment because CDROM is read only memory. TG may fail to start inside Virtual Desktop on Windows Vista (SPO CDROM image only. (Q01886811)
- SPO Clients fails to load the NVG links when it is configured using %hex characters for example, https%3a%2f%2fexchange2007.cse.nort

el.com%2fowa. (Q01888114).

- Virtual Desktop exits immediately with Persistent mode on with U3 USB .

  When the user launches the SPO using U3 USB (prelogon), the virtual desktop starts successfully. After this if the user creates a file/folder inside the virtual desktop with `persistent mode` set to **`on`**, it should get retained for next login. When the user exits from Dashboard, the SPO and Virtual Desktop also exits which creates a SODP link. On navigating to *start->programs* and running the SODP application, the vdesktop is launched but it exits immediately without any warning/ message. (Q01890378)
- Some Portable Apps launched from SPO do not close when SPO is logged out/exited. (Q01892159)
- Even though many links are available in the linksets and many linksets, only the first 16 links will be shown in the system tray menu. (Q01833490)
- The SPO Client fails to start the IE instance and gets the Operating System error message "Server Busy". (Q01871715)
- When using SPO with client certificate based authentication, Net Direct is not available in conjunction with Virtual Desktop. (Q01899418)

Browser-Based Interface

- The output for command `/maint/starttrace` is not available in WebUI. (Q01475271)
- When the system time in the Minute list box (Cluster>Time) is changed to 15 or a higher value an error message appears and the BBI hangs. This issue is expected to be fixed in the future patch releases. (Q01341831)
- After checking NVG configuration using, Diagnostics » Maintenance » error in test is displayed. (Q01688298)
- Not able to download Netdirect setup file from BBI **VPN Gateways >> VPN-# >> VPN Client >> Net Direct**. (Q01848065)
  Workaround:

Step	Action
1	Create a Net Direct link.
2	Download the setup file from that link to the VPN portal.

3 Download the setup file through the following URL:
https:\\<portal-IP/nortel_cacheable/NetDirect_Setup.zip>.

--End--

- Monitor takes long time to load data when more number of users are logged into the VPN. (Q01819115)
- Restoration of the system icon fails in the default .ico format from **VPN Gateways >> VPN-# >> SPO >> General**, **Sys Icon Restore**, but restores in .gif format. (Q01828647)
  To restore the correct system icon in .ico format, enter the following in CLI:
  `/cfg/vpn #/spoclient/restoresysicon`
- The license usage excel sheet created through Cluster Manager does not include the Virtual Desktop license usage count. (Q01846455)
  To view the Virtual Desktop license usage, enter the following:
  - BBI path
    Monitor >> License Usage
  - CLI command:
    `info/licenses`
- SPO feature is not available in BBI when the hardware platform is Contivity.
  When the hardware platform is Contivity, access or configure SPO through CLI. (Q01849602)
- CLI validates the integer in the NetDirect banner/license but BBI does not. (Q01447773)
- urlobscure breaks Citrix Java client connection through web interface. (Q01692215-01)

Command Line Interface

- **`/maint/tsdmp`** which dumps **`/info/cur`**, **`/cfg/dump`**, and **`/st/dump`** is not consistent with the Alteon switch command. (Q00980212)
- No kick all command within the CLI for the Alteon 5.0 code. (Q01040624)
- When more number of users are logged into the VPN it takes time to retrieve user information using **`/info/users`**. (Q01819817)

Miscellaneous

- While upgrading 7.0.1 to 7.1.x the NVG devices in the cluster reboot continuously for sometime and then fall back to 7.0.1. This occurs in a cluster configuration when NVG is connected using any L2 switch with Spanning Tree Protocol (STP) enabled on it. (Q01813363)
  Workaround:
  While upgrading the cluster to 7.1.x, disable the STP on the NVG Management port.
- **`/cfg/ssl/server 1/adv/traflog`** facility is not consistent with **`/cfg/sys/syslog`** add facility options. (Q01143777)
- Saved value of the maximum number of users ever logged in at the same time is required by the user. (Q00963356)
- Alteon not rewriting URL for addImport function of stylesheet object. (Q01161363)
- Syslog and trap for ippool is not available. (Q01320410)
- Option to view all license usage in a single graph is required. (Q01658589)
- IPsec minimum agent version logoff reason not quite correct in startTrace. (Q01338181)
- The 4.2 Outlook 2003 client does not work through native outlook port forwarder. (Q00757505)
- If e-mail is forwarded using OWA with picture embedded in the signature or in the body of the e-mail it does not display that picture on recipient's end. (Q01622315)
- When SRS rule succeeds no message is being shown. (Q01674703)
- Fails to sign in to yahoo if cookiedb is `off`. (Q01735155)
- Accessing the lotus notes mail box using Firefox throws error. (Q01533176)

Known anomalies

This section lists known anomalies with the NVG software.

- In SSL Acceleration mode (type=http), the secure option on the session cookie was introduced in v4.2.1.11 and it can be controlled by /cfg/ssl/server #/http/securecook <on/off>. The old behavior in software versions prior to 4.2.1.11 is OFF. Also, in 4.2.1.11 and later (4.x, 5.1, 6.0), the default value of "securecook" is OFF. But if the software version earlier than 4.2.1.6 to 4.2.x later than 4.2.1.11 or 5.1 or 6.0 is upgraded, the value of "secorecook" is set to ON. (Q01452086-01)
- Netdirect is only adding the first dns server in the list, so for example, if the search list containing alteonlab.com, netslab.com, abctest.com, is configured, after connecting, only alteonlab.com is seen against the adapter. In the Winxp registry under the path My computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters SearchList value is, alteonlab.com. (Q01731956)

Related documentation

- *VPN Gateway 7.1 Users Guide*
  (part number NN46120-104, April 2008)
- *VPN Gateway 7.1 Command Reference*
  (part number NN46120-103, April 2008)
- *VPN Gateway 7.1 Application Guide for SSL Acceleration*
  (part number NN46120-100, April 2008)
- *VPN Gateway 7.1 CLI (Command Line Interface) Application Guide for VPN*
  (part number NN46120-101, April 2008)
- *VPN Gateway 7.1 BBI (Browser-Based Interface) Application Guide for VPN*
  (part number NN46120-102, April 2008)
- *VPN Gateway 7.1 VPN Administrators Guide*
  (part number NN46120-105, April 2008)
- *VPN Gateway 3050/3070 Hardware Installation Guide*
  (part number 216213-B, March 2005)
- *VPN Gateway Configuration - Secure Portable Office Client*
  (part number NN46120-301, April 2008)
- *VPN Gateway 7.1 Troubleshooting Guide*
  (part number NN46120-700, April 2008)

How to get help

Getting Help from the Nortel website

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

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. The following can be accessed from the Nortel website:

- download software, documentation, and product bulletins
- search the Technical Support website 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 through a Nortel distributor or reseller

If a service contract for the Nortel product is purchased from a distributor or from an authorized reseller, contact the technical support staff for the distributor or reseller.

Getting Help over the phone from a Nortel Solutions Center

If the required information is not available in the Nortel Technical Support website, and if there is a Nortel support contract, then the help can be obtained over the phone from the Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7865).

Outside North America, go to the following website to obtain the phone number for that region:

www.nortel.com/callus

Getting Help from a specialist by using an Express Routing Code

An Express Routing Code (ERC) is available for many Nortel products and services. When an ERC is used, the call is routed to a technical support person who specializes in supporting that product or service. To locate the ERC for the product or service, go to:

www.nortel.com/erc

Nortel VPN Gateway

Release Notes - Software Release 7.1

Release: 7.1
Publication: NN46120-400
Document status: Standard
Document revision: 02.01
Document release date: 14 July 2008

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

Export

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or reexport may be required by the U.S. Department of Commerce.

Licensing

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software developed by the Apache Software Foundation http://www.apache.org/.

This product includes a TAP-Win32 driver derived from the CIPE-Win32 kernel driver, Copyright © Damion K. Wilson, and is licensed under the GPL.

See Appendix D, "License Information", in the *Users Guide* for more information.