



Nortel VPN Gateway

# Release Notes — Software Release 6.0.9

---

part number: 216372-T, August 2007

4655 Great America Parkway  
Santa Clara, CA 95054  
Phone 1-800-4Nortel  
<http://www.nortel.com>

Copyright © 2007 Nortel Networks. All rights reserved.

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

Nortel Application Switch, Nortel 2208, Nortel 2216, Nortel 2224, Nortel 2424 Nortel 2424-SSL, Nortel 3408, Nortel 180, Nortel 180e, Nortel 184, Nortel AD3, Nortel AD4, and ACEswitch are trademarks of Nortel, Inc. in the United States and certain other countries.

BEA, and WebLogic are registered trademarks of BEA Systems, Inc.

Netegrity SiteMinder® is a trademark of Netegrity, Inc.

Confidence Online is a trademark of WholeSecurity Inc. (acquired by Symantec Corporation).

RSA ClearTrust and RSA SecurID are trademarks of RSA Security Inc.

CryptoSwift® HSM is a registered trademark of Rainbow Technologies, Inc.

Portions of this manual are Copyright 2001 Rainbow Technologies, Inc. All rights reserved.

Any other trademarks appearing in this manual are owned by their respective companies.

### **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 ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto: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 *User’s Guide* for more information



# Release notes

---

These Release Notes provide the latest information regarding your VPN Gateway (NVG) with version 6.0.9 software. This supplement lists the new features and modifies some information found in the complete documentation:

- *VPN Gateway 6.0 User's Guide*  
(part number 216368-D, April 2006)
- *VPN Gateway 6.0 Command Reference*  
(part number 216369-D, April 2006)
- *VPN Gateway 6.0 Application Guide for SSL Acceleration*  
(part number 216370-D, April 2006)
- *VPN Gateway 6.0 CLI (Command Line Interface) Application Guide for VPN*  
(part number 216371-D, April 2006)
- *VPN Gateway 6.0 BBI (Browser-Based Interface) Application Guide for VPN*  
(part number 217239-C, April 2006)
- *VPN Gateway 6.0 VPN Administrator's Guide*  
(part number 217238-C, April 2006)
- *VPN Gateway 3050/3070 Hardware Installation Guide*  
(part number 216213-B, March 2005)

## Documentation download

---

These manuals are available for download from Nortel's Customer Support Web site:

1. **Point your browser to:** <http://www.nortel.com>.
2. **Under Support and Training, select Technical Support>Technical Documentation.**
3. **Choose "Security & VPN" from Documentation, Software, and Bulletins in the listed Categories.**
4. **Then select the following:**  
VPN Gateway 3050 or VPN Gateway 3070 Documentation  
  
SSL VPN Module 1000  
  
Application Switch 2424-SSL (from the Content Networking category)
5. **Select the desired documentation or Show All for a listing of all documents associated with the product.**

## New Features/Enhancements in Software Version 6.0.9

---

This section lists software features and enhancements added for version 6.0.9.

### General

- Added support for more than 250 characters in the 6.0.3 linkset. (Q01571210)

### BBI (Browser-Based Management Interface)

- Added support in BBI to the Tunnel profile display name so it no longer truncates after 20 characters. (Q01669002)

### Net Direct

- Net Direct now provides the option to access links directly via the Proxy browser address and not through the VPN gateway. (Q01581966)

- Net Direct now captures the username, password and domain, authenticates to the proxy server and runs. (Q01529467)
- Net Direct now supports up to 1024 IP Pools across all VPNs. To enable this feature, the administrator must set: (Q01479508)

**/cfg/sys/adm/enanumpool** to “on” .

The **/cfg/vpn\*/numippool** menu is only available if **/cfg/sys/adm/enanumpool** is “on”.

CLI Description:

**/cfg/vpn\*/numippool** gives the user the ability to set the number of IP Pools for each VPN. By default the number of IP Pools for each VPN is set to 30. In order to increase the number of IP Pools for a given VPN beyond 30, this value needs to be set, but the total number of IP pools across all VPNs must not exceed 1024.

**/cfg/sys/adm/enanumpool** must be properly configured to use more than the default number of IP Pools for each VPN. Each VPN is defaulted to 30 IP Pools, the user can specify up to 1024 IP Pools for one VPN, but the total number of IP Pools across all VPNs can not exceed 1024.

To enable the IP Pool feature using the WebGUI you must follow the steps indicated:

1. **Select Administration -> IP Pool**
2. **Enable 1024 IP Pool feature**
3. **VPN Gateways -> Gateway Setup -> IP Pool**
4. **Set the appropriate IP Pool number for your installation.**

- Net Direct now resolves the DNS and successfully connects to the VPN. (Q01500922)

## Portal

- A password aging policy is now in effect on the portal. This requires the user to change their password at a pre-configured time and date, and create a new password each time the old password expires. (Q01576163)
- ICSA Violations V01: Weak ciphers need to be disabled by default. (Q01620841)

# Software installation and upgrade notice

---

## SSL VPN server software

The SSL VPN server software is delivered in two different forms, as described below.

- `SSL-6.0.9.0-upgrade_complete.pkg`

Using 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 6.0.9 from an earlier version.

- `SSL-6.0.9.0-boot.img`

Using this image will reset the NVG to its factory default configuration. It must be used when a NVG with 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 6.0.9 through the reinstall procedure.

## Server software download

The server software is available for download from Nortel’s Customer Support Web site. To access the site, proceed as follows:

1. **Point your browser to: <http://www.nortel.com>.**
2. **Under Support and Training, select Technical Support>Software Downloads.**
3. **Choose ‘Security & VPN from Documentation, Software, and Bulletins in the listed Categories.’**
4. **Then select the following:**  
VPN Gateway 3050 or VPN Gateway 3070 Software
5. **Select the desired software or Show All for a listing of all software associated with the product.**
6. **Downloading software requires that you enter the registered user name and password previously assigned to you 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 Web site, and follow the 5-step registration process.

Due to an increase in software image sizes in the 6.0.7.0a and 6.0.9.0 releases and limited storage space available in the 2424-SSL, 6.0.7.0a and 6.0.9.0 cannot be installed on the same platform. However, the 6.0.9.0 release has a new disk repartitioning feature to accommodate any future releases.

2424-SSL users with 6.0.7.0a and above, have the following options for installing 6.0.9.0:

- 1. 6.0.9.0 image upgrade: the user will lose all configuration.**
- 2. Downgrade to 6.0.5 and upgrade to 6.0.9.0: the user will retain existing configuration.**

## 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:

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

## Nortel IPsec VPN client (formerly Contivity)

The IPsec VPN client software can be downloaded from Nortel's Customer Support Web site. (<http://www.nortel.com>) Select **Security & VPN ▶ VPN Client ▶ Software**. Choose **Show All** for a complete list of software available.

## Disk repartitioning required for version 5.x or later on NAS 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. 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 above 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 above 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”, i.e. not shown in the menu or considered for auto-completion through <TAB>, since they shouldn't be used in normal operation. During the repartition, which includes two automatic reboots, the host will effectively be out of service.

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

---

**NOTE** – 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** – 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** – 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 in order 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 6.0 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 will be filtered out during the downgrade.
- If Net Direct, IE Wiper and/or Citrix Metaframe support has been set to `group`, the setting will be changed to the respective default value.

## Reload license after upgrade

In version 6.0 and later, 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 in order to make use of the extra 40 number of users in the default license. (See *VPN Gateway 6.0 CLI (Command Line Interface) Application Guide for VPN* (part number 216371-D, April 2006))

## Supported hardware platforms

---

The 6.0.9 server software is currently supported on the following hardware platforms:

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

### **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 above principle, the hardware models Nortel SSL Accelerator 310, 410 and 310-FIPS are not supported from NVG release 6.0 and onwards.

## Fixes

---

This section lists fixes added for version 6.0.9.

### General

- Fixed a problem where Active Directory would fail when the option “user must change password on next logon” was selected. (Q01646152)
- Fixed a problem where the password expiry popup did not appear with Active Directory. (Q01671020)
- Fixed a problem where Port Forwarder was giving an SSL Alert error. (Q01655300-01)
- Fixed a problem where IPSec statistics did not show any active sessions once it was cleared. (Q01687471)
- Fixed a problem where Cross Site Scripting (XSS) or HTML injection was possible. (Q01690022)
- Fixed a problem where the IP Pool modification did not work after MIP migration. (Q01716330)
- Fixed a problem where an interface index number larger than 50 caused the SNMP module to crash. (Q01719769)
- Fixed a problem where NVG 3050 would randomly reboot due to conflict with spin\_lock and spin\_unlock. (Q01541417)
- Fixed a problem where a custom Port Forwarder would close unexpectedly. (Q01559607)
- Fixed a problem where Simple Proxy would crash intermittently. (Q01662048)

### BBI (Browser-Based Management Interface)

- Fixed a problem when using BBI and CLI was not able to create authentication of type radius, ldap, or ntlm. (Q01690714)
- Fixed a problem where the Cluster manager did not sync network and service names in the access lists. (Q01665748)
- Fixed a problem where exporting the configuration was causing an error and deleting the local database users. (Q01691776)
- Fixed a problem where names were truncated to 20 characters in the drop down menu, now the full name appears regardless of length. (Q01586130)

## CLI

- Fixed a problem where STATS under /stats/sslstats/local/isdhost 1/ was not working in CLI. (Q01651094)

## Portal

- Fixed a problem where the proxy initialization failed when using the HTTP Proxy link option with ntlm authentication. (Q01682696)
- Fixed a problem when using "Swedish" characters in a folder name, the SMB link did not list the share. (Q01686632)
- Fixed a problem where the Portal version of Net Direct did not show the same version number as the server. (Q01689932)
- Fixed a problem where the VPN Administration menu was not working. (Q01689030)

## Net Direct

- Fixed a problem where Net Direct or Port Forwarder, while trying to establish a tunnel, would issue a second DNS request causing a break in persistency in a multi-cluster setup. (Q01643782)
- Fixed a problem where the portal Net Direct client was unable to reach hosts on the same network as the assigned IP when splitnets were disabled. (Q01662802)
- Fixed a problem where an invalid URL for Net Direct client caused a “registry error” in Microsoft Vista. (Q01666048)
- Fixed a problem where installing NDIC on Microsoft Vista Enterprise or Professional caused a blue screen. The user must uninstall the older version of NDIC (6.0.7.0a) before installing 6.0.9.0 NDIC. (Q01685490)
- Fixed a problem when Split tunneling is enabled, Net Direct should add the networks configured in the routing table of the PC but no default route. With windows 2000, 2 default routes with the same cost after connection would display. (Q01425656)
- Fixed a problem where Net Direct (NDIC/ActiveX) client was incompatible with the Kaspersky Anti-Virus program. (Q01531880)
- Fixed a problem with Net Direct failing to connect with “Adapter Logic Failed” error. (Q01579255)
- Fixed a problem with the Vista Net Direct agent showing an incorrect version in the “About” box. (Q01665158)

- Fixed a problem where the Net Direct agent closed if the VISTA Web browser was closed. (Q01666063)
- Fixed a problem where after Net Direct download to the client, 2 default gateways could be detected using the ipconfig command. (Q01686624)
- Fixed a problem where the Net Direct error "Route table" could not be altered while Net Direct was active. (Q01297873)

## SSL

- Fixed a problem with a Java parameter rewrite only rewriting the first file but not the remaining files. (Q01639426)
- Fixed a problem where the 2424 SSL /isd file system was not large enough to hold multiple copies of the releases. File system size has been increased to allow for more than one release. (Q01615845-01)
- Fixed a problem with NVG generating a truncated "Encrypted Alert" when communicating with a slow response client. (Q01585511-01)
- Fixed a problem where the SSL IPsec BO tunnels failed to connect when "nailed up" parameter was enabled. (Q01667259)
- Fixed a problem where the depth of a requested html page and the frame inside the HTML page was different, so the image which was called by the frame was taking the depth as the HTML page's depth making the requesting path of the image wrong. (Q01483997)
- Fixed a problem with Port Forwarder failing with errors when using SSL chain certificate. (Q01128789-01)
- Fixed a problem with Port Forwarder link window failing to auto minimize. (Q01622704)
- Fixed a problem where connection with an SMB server failed when using Swedish passwords. ((Q01640826)
- Fixed a problem where NVG couldn't interpret Chinese LDAP group attribute from LDAP server. (Q01649737)
- Fixed a problem where the subscriber thread took too much time in event processing and missed the tick update. (Q01653679)
- Fixed a problem where /i/kick would fail when RADIUS accounting was enabled. (Q01663897)
- Fixed a problem when the tag <?xml...> was present certain parts of an HTML page were not being rewritten. (Q01508116-02)

## Tunnel Guard

- Fixed a problem where Tunnel Guard would throw the error: “Failed to save to LDAP server” while saving the SRS rules. (Q01596647-01)

# Known limitations

---

## Browser Requirements

### Basic Portal Access (no applets)

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

- Internet Explorer 5 or later
- Mozilla 1.1 or later
- Netscape 4 or later
- Firefox
- Opera
- 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

### Tunnel Guard Applet Support

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

The following browsers support the Tunnel Guard 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 1.0

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 1.0
- Unix/Linux:
  - Netscape Navigator 7.1 or later
  - Mozilla 1.5 or later

## Net Direct Client

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

- Internet Explorer on Windows 2000, XP and Vista.
- Firefox on Linux, Windows 2000, and XP.
- Safari 2.0 on Mac OS version 10.4

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

- Fedora Core 2
- Fedora Core 3
- Fedora Core 4
- Red Hat 9.0
- Knoppix 4.0.2
- SUSE 10.0

## 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.

- The Net Direct mobility capabilities are not supported for Linux and Mac OS X.
- The split tunneling modes `enabled_inverse` and `disabled` are not supported for Mac OS X. For non-supported split tunneling modes, Net Direct falls back to the `enabled_inverse_local` mode.
- The split tunneling mode `enabled_inverse` is not supported for Linux. For non-supported split tunneling modes, Net Direct falls back to the `enabled_inverse_local` mode.
- If the remote user has proxy settings configured in Internet Explorer and split tunneling is enabled, Net Direct will use the proxy settings but split tunneling will be disabled, i.e all traffic will be tunneled.
- When using Net Direct on Linux and Mac OS X, the DNS server(s) specified on the NVG (in the IP pool or under `/cfg/sys/dns/servers`) must be able to resolve all host names that should be accessible (internal as well as external host names). This is because no external DNS server will be used as fallback.
- Downloading and installing Net Direct on Windows, requires the user to be administrator on his/her PC. For users that are not administrators, the Windows administrator user name and password can be stored (on group level) on the NVG. If the user is not administrator and the credentials are not stored on the NVG, the user will be prompted for the Windows administrator user name and password upon downloading Net Direct.
- Downloading and installing Net Direct on Mac OS X requires the user to be member of the admin group. If the user is not a member of the admin group or enters the wrong password when prompted, he/she can log in with the root password as an alternative option. This in its turn requires that the user account is authorized to perform the command `su root`.
- Downloading and installing Net Direct on Linux requires the user to be root user or see to it that the user account is authorized to perform the command `su root`. If the user is not running as root when attempting to download Net Direct, a window is displayed prompting the user for the root password.
- Downgrade of IE cache wiper does not happen automatically.
  - a. When downgrading Netdirect, you need to manually delete the IEwiper Control and the NetDirect cab files.
  - b. When logged on to the portal page it will install the cab files from the server.
  - c. If you want to use the downgraded version then delete the cab files in **Tools->Internet options->Settings->View Objects**. Otherwise no action is required.

## Tunnel Guard Agent

Version TG\_1.1.2.0\_001 of the *installed* Tunnel Guard agent is the minimum requirement for use with the Nortel IPsec VPN client (formerly the Contivity VPN client).

## Nortel IPsec VPN Client (formerly Contivity VPN Client)

- For IPsec termination on the NVG, the following Nortel IPsec VPN client versions have been tested: 4.15, 4.86, 4.91, 5.01, 5.11 6.1 and 6.1.0.102.
- For use with the Portal's Full Access feature, version 4.91 and later 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), Vista and XP. This client does not support UDP.
- Version 1.5.0.9 (TDI client): Compatible with Windows 2000, Vista 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

- When accessing an FTP server through the NVG Portal, the maximum supported file size is 2 gigabytes. (Q01435793)
- Sun's JRE earlier than 1.4 cannot download any applets from the NVG if the device has been setup to use a key length above 4096. This is supported in the native Microsoft JVM and may be supported in Sun's JRE 1.5 (yet unclear).

- Proxy chaining (option to specify an intermediate HTTP Proxy host and port, e.g. 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 (e.g. NetMeeting, FTP and all streaming media) are not supported by the Port forwarder feature. Applications using *static* port number allocation (e.g. DNS, SNMP) are supported.
- When specifying a URL without a path for an iauto (automatic login) link, e.g. `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 (i.e. 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 (i.e. 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, e.g. 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".

## SSL VPN Module 1000 (SVM 1000)

When using the BBI (Browser-Based Management Interface) to configure the SVM 1000, some options in the BBI are available but not supported. The following features in the NVG software are not supported on the SVM 1000:

- Local authentication.  
**BBI path:** VPN Gateways>Authentication>Local
- Standalone mode.  
**BBI path:** VPN Gateways>Gateway Setup>Standalone and SSL Offload>Servers>General (Standalone Mode)
- Transparent proxy mode.  
**BBI path:** SSL Offload>Servers>General (Transparent Proxy Mode)
- Tunnel Guard Agent settings.  
**BBI path:** VPN Gateways>TunnelGuard>Agent

## General

- A maximum of 32,000 sessions is allowed on the NVG 3070 with 2 GB RAM.
- The license is not part of the configuration and will not be included when exporting the configuration using the `/cfg/ptcfg` command. If a configuration is deleted, the license will be deleted as well.
- When using the IPsec VPN client together with the installed Tunnel Guard agent, the result of the Tunnel Guard 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 Tunnel Guard check is run.
- The Net Direct Installable Client (NDIC) upgrade fails on a Windows Vista client. (Q01717550)

## Known Issues

---

This section lists known issues with the NVG software.

- For the Full Access feature (available on the Portal's Access tab) to work, the fully qualified domain name (FQDN) of the VPN *must* be specified as the server alias in the SSL VPN client (Servers tab>Add>Alias field).  
(CR Q01043664)
- Problem with Internet Explorer version 6.0.2800.1106.xpsp2\_gdr.040517-1325.  
When HTTPS is used, this version of Internet Explorer does not permit download of files that require an external program for processing, or that should be saved in the file system (e.g. files with extension .txt, .exe, .zip), even if the SSL VPN server HTTP setting of `addnstore` is set to `off`. Thus it cannot be used to download such files through the Portal.
- When running Net Direct on Knoppix, the tun device node must be set up manually. To do that, run the following commands as root:  

```
mkdir /dev/net  
mknod /dev/net/tun c 10 200
```

  
(CR Q01281449)
- 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`.  
(CR Q01278965)
- The installed Net Direct client does not support client security checks using the *installed* Tunnel Guard agent. If a user tries to connect to a VPN for which Tunnel Guard is enabled, the user cannot log in to that VPN if using the installed Net Direct client. This will be fixed in a coming patch release.
- The Tunnel Guard applet (client security check launched from the Portal) is not applicable when accessing a VPN using *installed* VPN clients.  
(CR Q01297451)
- Net Direct on Windows may not be compatible with some Internet security software for clients. This will be fixed in a future patch release.
- Inconsistent ClearTrust SSO (single sign-on) behaviour. When a user connects to the NVG Portal after having received a ClearTrust single sign-on session cookie from another ClearTrust-enabled web agent (not the NVG), the Portal login page should be bypassed,

i.e. the single sign-on cookie should be validated against the NVG. This only happens the first time the user connects to the NVG Portal, subsequent attempts fail.

(CR Q01341726)

- If several ClearTrust authorization servers or dispatchers are configured on the NVG, the server pools are not refreshed. For example, if a previously failed server is up and running again, this is not reflected in the server pool list. In a coming patch release, the ClearTrust server pools on the NVG will be refreshed periodically.

(CR Q01341793)

- Changing the system time in the Minute list box in the BBI (Cluster>Time) to 15 or a higher value generates an error message and may cause the BBI to hang.

(CR Q01341831)

- On Linux (SUSE 10.0) and Firefox, when starting Net Direct from the Portal, the message “Net Direct already running” may be displayed in the Java applet window although Net Direct has not been started. When this occurs, Net Direct cannot be started.

- When configuring the parameters for the downloadable Net Direct client, the administrator has the option to suppress display of the default license agreement. The following applies when the license agreement is suppressed (the text will be added to the relevant sections in the manuals in the next release):

*IMPORTANT: By suppressing presentation of the Nortel Software License Agreement you agree to accept the terms of the agreement on behalf of the users receiving the client software from you. If you do not wish to accept the license terms on behalf of the users, then do not suppress presentation of the agreement.*

- For Net Direct, if the administrator password configured on the NVG does not match the Windows PC client’s password, the browser can in some cases be closed.
- After performing an upgrade the "securecook" value should be set to “OFF” in SSL acceleration mode. (Q01452086)

If you are upgrading from a version older than 4.2.1.25, after the upgrade, the "secure cookie" option will be automatically enabled for all existing SSL servers (/cfg/ssl/server #/http/securecookie). This will cause problems for web sites that want to share the cookies between http and https sessions. If this happens, you must disable the securecookie option manually.

- If a remote user runs an old version of the installable Net Direct client, the client should be able to detect this upon connecting to NVG and a dialog where the user can choose to update the client or continue with the old version should be presented. In this release the dialog is not displayed.
- The user must uninstall the older version of NDIC (6.0.7.0a) before installing 6.0.9.0 NDIC.



- When using iauto with Internet Explorer an error is produced with Exchange Server 2007. (Q01591376)
- Following the user login and attempting to access Siemen's MagicWeb application a rewrite error is produced. (Q01513601)
- When the depth of a requested html page and the frame inside the html page is different, the image which is called by the frame is taking the depth as the html page's depth making the requesting path of the image wrong. (Q01483997)
- Navigating the SMB share folders which have Swedish characters in the folder name does not work. (Q01656067)





## Nortel VPN Gateway - Release Notes - Software Release 6.0.9

### VPN Gateway

Release 6.0.9

Document Number: **216372-T**

Document Status: **Standard**

Document Version: **01.01**

Part Code: **216372-T**

Release Date: **August 2007**

Copyright © Nortel Networks Limited 2007 All Rights Reserved

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

\*Nortel, Nortel (Logo), the Globemark, and This is the way, This is Nortel (Design mark) are trademarks of Nortel Networks.

\*Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

To provide feedback, or to report a problem in this document, go to [www.nortel.com/documentfeedback](http://www.nortel.com/documentfeedback).

