NORTEL

**NORTEL VPN GATEWAY (NVG)**
**Software Release 7.1.3.0**

# 1. Release Summary

Release Date : March 2009
Purpose : Software maintenance release to address customer software issues

# 2. Software Installation and upgrade notice

**SSL VPN Server Software**
The SSL VPN server software is delivered in two different forms, as described below:

• SSL-7.1.3.0-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 configurations are preserved. The upgrade procedure is described in "Performing Minor/Major Release Upgrades" in Chapter 4 in the VPN Gateway User's Guide NN46120-104.
Note: TFTP cannot be used when upgrading to version 7.0.1 or later from an earlier version.

• SSL-7.1.3.0-boot.img
Using this image will reset the VPN Gateway to its factory default configuration. It must be used when a VPN Gateway 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 NN46120-104.
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's Customer Support website. For more details, refer 7.1 release notes.

**SSL VPN Client Software**
Refer 7.1 release notes for download and installation details of SSL/IPSec VPN client & Secure Portable office.

## Disk repartitioning required for upgrade/downgrade from Release 7.x to 7.1.3.0 on NVG 3050/3070

To support the repartitioning procedure, the following commands are used:

- **/boot/repartition**

This will initiate repartitioning for the local host.

- **/cfg/sys/host #/repartition**
- **/cfg/sys/cluster/host #/repartition**

This will initiate repartitioning for the given host (which must be running).

These are "hidden" commands and hence auto-completion through <TAB> is not possible. Repartitioning includes multiple automatic reboots and the host will be effectively out of service. The time required for the repartition is approximately 5 to 7 minutes.

Refer 7.0.7.0 release notes for upgrade details of previous versions.

## 3. Hardware Platforms Supported

Nortel VPN Gateway 3050
Nortel VPN Gateway 3070
SSL VPN module 1000

## 4. Notes for Upgrade

**File Names for This Release**

| File Name | Module Or File | Type File Size(K.B) |
|---|---|---|
| SSL-7.1.3.0-upgrade_complete.pkg | Upgrade package | 54722 |
| SSL-7.1.3.0-boot.img | Boot image | 54699 |
| SPOClient-7.1.3.0.zip | SPO client files – iso, u3p and msi | 17792 |
| SSL-7.1.3.0-mibs.tgz | MIB files | 111 |
| SSL-7.1.3.0-mibs.zip | MIB files | 779 |

| File Name | MD5 Checksum |
|---|---|
| SSL-7.1.3.0-upgrade_complete.pkg | e200342e131ce3d0d65cbb9448f770f9 |
| SSL-7.1.3.0-boot.img | 26c9c58e8985fd9a1efe89d826bd5047 |
| SPOClient-7.1.3.0.zip | e6f8d778742e822ff86339e8163bcb21 |
| SSL-7.1.3.0-mibs.tgz | 51daf8f73c83a6d91721af7a75c11600 |
| SSL-7.1.3.0-mibs.zip | c38cb5871444ff8929acbdb95090e4a7 |

## 5. Version of Previous Release

Software version 7.0.7.0, Release date - Dec 2008.
Software version 7.1.1.0, Release date - Jun 2008 (previous release with SPO support).

Note: NVG 7.1.3.0 combines all the features/fixes from 7.0.7.0 and 7.1.1.0 releases.

## 6. Compatibility

N/A

## 7. Changes in This Release

**Problems resolved in this release**

**Q01982821** SNMP OID incorrectly reports the number of IPSec users connected when IPSec Licenses are exhausted and SSL licenses are used. This issue is fixed.

**Q01971349** The issue with distorted page layout in Opera browser in case of SSL offloading to backend server is resolved.

**Q01931398** The Netdirect Split-network routes were not taking precedence over existing routes in client PC. The issue occurred due to the improper handling of static routes in client PC split-tunnel enabled mode and is resolved.

**Q01973678** WTS access via Java RDP client always use UK English as default keyboard layout instead of using the client PC default keyboard layout. This issue is fixed.

**Q01868986** The issue with proxy authentication failure for SPO client has been resolved.

**Q01933206** SharePoint document links (shared document links) are not rewritten properly. So when we take shared document links listed in SharePoint server through NVG it was failing to load the shared document. This issue is fixed.

**Q01982756** Enabling http compression causes xnet.js JavaScript to fail to decompress in IE 6.0. This issue is fixed.

**Q01924285** When using external authentication server for a backend access, there is a chance that the NVG will not send the POST body to the backend server. This issue is fixed.

**Q01965505** The issue with 95% CPU utilization for Netdirect client on Red Hat Enterprise Linux 5 has been resolved.

**Q01934484** Intermittent Netdirect disconnects experienced and the logs show simpleproxy crash message. This simpleproxy crash due to buffer corruption has been fixed.

**Q01940134** Intermittent display of login page in English and the configured non English language can be observed if the login page is continuously refreshed after a logout. This issue is fixed.

**Q01986637** The load balancing issue with SSL offload server configured to use leastconn matrix is resolved.

**Q01992122** In the BBI, the value for "Config -> VPN Gateways -> VPN # -> Ipsec -> NAT Traversal -> Client IKE Source Port Switching" was not set correctly as in the CLI. In the CLI, when the command /cfg/vpn #/ipsec/sys/nat-t/portswitch was set to on, the BBI showed it as disabled. When it was set to off in the CLI, BBI showed it as enabled. Now the value in BBI corresponds correctly to the value in CLI when set to "ON/OFF".

**Q01984014** Netdirect failed authentication when launched on a PC configured with NTLM proxy. This issue has been fixed

**Q01906198** The issue with NVG reboot due to memory leak under heavy IPSec load has been fixed.

**Q01982756** Java script failure in 7.0.7.0 when http compression is enabled (/cfg/vpn #/server/http/compression on) has been fixed.

**Q01470763** CleanupNortelRPC.reg has wrong registry path when the outlook port forwarder is used. This issue is fixed. CleanupNortelRPC.reg is used to restore registry setting changes during boot up via CleanupNortelVPN.bat.

**Q01966236** SNMP DISMAN-EVENT-MIB help command does not display content. Help details added to resolve this issue.

**Following CRs are forward propagated to 7.1.3.0 from previous releases/patches**

**Q01964853-01** SSL connection to the backend server fails when the NVG offload server with end to end encryption is running under heavy load for few hrs. The issue is related to synchronization b/w ssl library and the crypto card during ssl session cache update resulting in maximum allocation of driver buffers. When this issue happens, the ‘nspstats’ command output shows current buffer allocation as 99%.
New hidden cli command is added to disable SSL session cache mode to address problem.
/cfg/ssl/server #/adv/sslconnect/cachemode.

**Q01741290-02** Exporting default language definition file via ftp/tftp from BBI/CLI gives “Bad Language Code" error. In cli, the issue occurs only when the language code is specified. When the language code is not specified in cli, the language file is successfully exported. In BBI, the language code must be specified always and export operation will always fail. The issue in BBI & Cli is fixed.

**Q01939182-01** When using SSL offload server with connection pooling enabled the NVG sometimes combines requests from different clients to the backend server. The possibility for this issue is only when connection pooling is enabled and the previous client requests has Expect header. This issue is resolved.

**Q01780813-01** When using entrust certificates with IPSec client to authenticate with NVG, the NVG is not able to parse the user based on common name (CN) if that's not the first object in the cert DN. This results in the user getting connected as "anonymous-clicert". This issue is fixed.

**Q01788985-01** Microsoft office 2007 extensions are not recognized by portal when accessed via SMB. Content type shows text/plain rather than application/vnd.openxmlformats. IE tries to open file as .zip file when this occurs. Firefox opens file based on extension correctly. This issue is fixed.

**Q01478071-01** Fixed the issue with 'allowdoc' command to work with *.csv files. Now the 'no cache' field in http header is removed when allowdoc is enabled for the server.

**Q01825972-01** SSP with TG does not allow multiple VPN's to use same backend interface. Only one TG instance per interface works which is preventing customer with SSL feature from enabling TG on other VPN's that use same backend interface. This issue is fixed. The fix is in TG server and there is no change in TG client.

**Q01878383-01** info/kick does not work with more than 10000 users. If there are more than 10K users, the command exits saying that there are too many users. This scenario makes /info/kick command unusable for large user base. To fix this issue, a new command option is added to kick all users without displaying the list.

**Q01918424-01** When the DN of a certificate in the format of "email Address = xxx + CN = yy", NVG is appending space at the end of email Address when it retrieves it from the cert DN. This issue with the parsing of DN is resolved.

**Q01590186-01** Netdirect fails to authenticate when Radius timeout happens. The NVG doesn’t wait for as much time as the timeout and the number of Radius servers is configured, and throws an error saying authentication failed or timed out. This issue is fixed.

**Q01488611-01** Net Direct was creating multiple adaptor interface entries into Windows Registry (W2K, XP, and Vista) and not deleting older entries automatically. Even though cleanup of this entry is expected while the driver gets uninstalled from the client machine it was not happening. The issue has been fixed.

**Q01591323-01** Domain Name System (DNS) entry cached by the captive portal not getting flushed when Macintosh Net direct is loaded. This issue is fixed.

**Q01778272-01** The issue with failure of NetDirect client to detect the Proxy auto Configuration (PAC) Settings in the client browser has been resolved.

**Q01791077-01** XNET Embedded JavaScript is getting Exposed/Modified by 3rd-Party MailScanner. When the script tag (which is added by NVG during dynamic rewrite) is modified by some third party software like Mailscanner, the script NVG injected is getting meaningless. Since the script tag is changed like <Mailscriptxxx>, the script is throwing alert messages. This issue has been resolved.

**Q01399305-02** The SSL keep alive causes traffic to fail. This issue was seen because we are not handling the EXPECT 100 continue header from the client. This issue has been resolved by handling the EXPECT 100 continue header.

**Q01830278-01** The issue while accessing portal link to Citrix 4.5 Presentation Server resulting in continuous reloading of a blank page is fixed.

**Q01788967-01** Accessing Domino Web Access (DWA) through the NVG internal portal link causes issues while attaching, saving / reading documents. When trying to save/read documents, it gives DWA error "unable to download file". Normal emails without any attachments work fine. This issue is fixed.

**Q01730590-01** The issue of NTLM authentication failure with Java port forwarder in client machine using Chinese regional language has been resolved.

**Q01673460-01** The issue of NTLM authentication failure with Java port forwarder in Japanese windows XP machine has been resolved.

**Q01793688-02** The issue of file corruption while uploading large files to win2k3 smb server is fixed.

**Q01808776-01** The issue in accessing IIS ftp server configured to use UNIX directory listing through the VPN portal has been fixed. Earlier the ftp access from portal via ‘File -> Specify server’ was resulting in error ‘Unable to parse server listing’.

**Q01961172-01** LDAP password change via CVC breaks when multiple authentications servers are configured. This issue has been fixed.

**Q01977882-01** The TrustSite feature in 7.0.7.0 is broken due to corrupted trustsite.cab file in the release package. This issue is fixed by replacing the cab file with the correct one.

**Q00973720-01** When the "upload" button is clicked from the Files tab while inside an SMB share page, a script dialog box error occurs stating "Debug: top.placeholder is undefined". This unnecessary javascript alert message that occurs in both IE and Firefox has been removed

**Q01729388-01** HTTP to HTTPS Redirect Server May Truncate URLs. Some client URLs may not be rewritten when using the HTTP to HTTPS redirect functionality is enabled in NVG. This issue is fixed.

**Q01828847-01** Backend server pages having <jsp> tag throws java script error while accessing via portal. This issue has been resolved by supporting <jsp> tag in rewrite module.

**Q01983091-01** OpenSSL vulnerability CVE-2008-5077 is resolved. The issue occurs in all OpenSSL releases prior to 0.9.8j as an SSL/TLS client when connecting to a server whose certificate contains a DSA or ECDSA key.

**Q01972034-01** Abrupt termination of SSL connections is observed when SSL renegotiation is invoked from backed server. This occurs when NVG does an SSL write operation to backend server which results in SSL_ERROR_WANT_READ due to re-negotiation invoked from server. This issue is fixed.

**Q01981075-01** Base64 encoding the user name field is causing confusion to end users while login to portal page. This issue is fixed by avoiding base64 encoding for the user name field.

**New enhancements in this release**

**Q01960592-01** This enhancement allows IPSec or NDIC based users to bypass TunnelGuard checks when the TunnelGuard agent is not installed in the client machine. Previously the users were logged out in this case. Now the users will have restricted access to the backend based on "tg_failed" rule. The existing CLI menu for bypass (/cfg/vpn #/aaa/tg/bypass) which is for facilitating users with unsupported operating systems is extended to enable this option for Supported OS without TG installed. The following tables show the scenarios for both applet and installable TG, where tg_success refers to full access, tg_fail refers to restricted access to the backend & tear_down refers to no access.

| | TG downloadable - enabled | | TG installable - enabled | |
|---|---|---|---|---|
| | bypass on | bypass off | bypass on | bypass off |
| action teardown | tear down | tear down | tear down | tear down |
| action restricted | tg_fail | tg_fail | tg_fail | tear_down |

**Q01983197-01** Port forwarder Host mapping feature support added for windows vista.

**Q01860194-02** The idle TTL and session TTL timeout override option is now available for the siteminder users. New control is provided to override the timeout values returned by the siteminder server with the values configured in NVG.
CLI command: /cfg/vpn #/ aaa/auth id/siteminder/override
When set to OFF, NVG uses the session timeout and idle timeout returned by the siteminder server. When set to ON, NVG uses only the configured session TTL and idle TTL values and ignores the values returned by the siteminder server. Default value is OFF

**Q01732692-02** Option to provide DNS Hostname to define the siteminder servers in the NVG

Siteminder agent has been added. LDAP server name menu is added in cli auth/LDAP menu to configure the hostname.
New cli menu is /cfg/vpn #/aaa/auth #/ldap/servername

**Q01988065** In 6.0.15/7.0.7, separate NetDirect packages were used for portal ND and NDIC for different Windows OS. This has been changed to single NetDirect package (NDIC - NetDirect_Setup.zip & Portal ND - NetClient.zip) that supports different variants of windows (Win 2k, XP and Vista). This improves maintainability and reduces NVG image size.

**Q01979559** This enhancement is to improve debugging options for simpleproxy module. Proxydebug option is enhanced to specify the max number of log files thereby increasing the data capture. The max size of the proxydebug log file is now set as 10MB. Earlier it was 5MB.

"/maint/debug/proxydebug on" will prompt to enter max log files. Accepted input range is 3 - 30. If user entered value within limit, it will be accepted and write to /tmp/proxydebug file and simpleproxy will be restarted as before. If user entered incorrect input, default value of 3 will be used. There is no further prompt to re-enter the value.

To enable proxydebug via script and set the max log file, the following commands can be used.
“echo <logfilesize> > /tmp/proxydebug (eg: echo 10 > /tmp/proxydebug)”
“killall simpleproxy.”
In this case also, the value limit is 3 - 30. For any other value, default 3 will be used.

## 8. New Outstanding Issues

**Q01988417** Portal rewrite of web sphere application fails to rewrite path to flash object in Internet Explorer. Works correctly with Firefox

**Q01998186** NVG configured to have Client authentication with client certificate and traflog (/cfg/ssl/server#/adv/traflog) is also enabled. In this setup, when sending a client request continuously, the access sometimes fails after several requests.

**Q01995678** On a NVG with SSL offloading (end-to-end encryption) configured, the NVG may fail to send the POST body to the backend server resulting in a HTTP 500 Error response from server. This issue occurs only when ssl renegotiation happens during backend communication. In this particular case, NVG receives HelloRequest from server after it sends POST request and starts SSL renegotiation, but fails to send POST body.

**Q01985579** Simpleproxy crash with “Internal error 125” in error logs is observed at couple of sites under heavy load.

**Q01999277** Connecting to OWA through NVG and adding the recipient to a new mail message from contacts list results in error. The issue occurs only when the first

name is selected from the table populated by searching the contacts based on Display name.

**Q01970780** Citrix activex applet prompts user for install when portal is added to default trusted site. But the script that is being used throw errors and does not allow the user to install the activeX client - it always falls back to java client.
Workaround is to change default trusted site setting "Initialize and script ActiveX controls not marked as safe" from Prompt to Enable.

**Q01967302** Intermittent health check failures to backend server are observed in ssl offload server configuration. The issue occurs when the health check type is script.

**Q01994974** With NVG configured for SSL Acceleration with backend Webdav Server/ Application, it is observed that PUT header gets corrupted some times.

**Q01997708** CRL retrieval is not happening when the server URL for CRL retrieval is given as FQDN. If URL is configured based on IP address of server, CRL retrieval will be invoked, but NVG closes the connection if it's not completed in 5 seconds.

**Q01986033** Netdirect user's loose connection intermittently and the logs points to TG heartbeat failure while NVG does TG recheck.
Workaround for this issue is identified as increasing the TG recheck interval to higher value.

**Q02000999** Portal TG fails and triggers logout when host failure occurs in cluster. This occurs only when TG is used with portal, but TG + ND works fine. The trace shows that the TG is sending a TCP packet every couple min regardless of recheck time which triggers the logout.

**Q01985475** SPO virtual desktop fails to launch on certain XP SP2 clients.

**Q01992649** Netdirect client will be re-downloaded after the client PC is rebooted despite having "caching on" (/cfg/vpn #/sslclient/caching on) configured in NVG. This only occurs after a reboot of the client.

**Q01959939** Reports produced via MicroStrategy's reporting product are not rewritten correctly with 7.x. In 6.0.x, this is working properly. The issue is that the graphs in the application/report do not display at all and yield an html error.

**Q01987820** Simpleproxy crash observed with SSL offload server configuration and the core files points to crash in ssl library.

**Q01985570** Simpleproxy crash is observed at couple of sites under heavy load. The portal is configured mainly for OWA access.

**Q02003101** SPO supports the ability to run local client applications via port forwarder. The port forwarder needs to update the local etc/host file with the NVG hostname mappings. These updates are not occurring.

**Q02003646** Portal link to Enterprise Reporting application login page fails in IE, but it works fine in Firefox.

**Q02002918** ike process hangs in 2-3 days time frame due to memory leak. In most cases, ike process has to be killed and allowed to restart. Also observed a kernel panic on one occasion when the ike process is killed.

**Q01959862** NTLM proxy authentication failure occurs with custom port forwarder application that uses NVG PF API's.

## 9. New Known Limitations

**Q01904885** NetDirect initialization times out when primary DHCP server fails. NVG will pull address from 2nd DHCP server but NetDirect client will have timed out by then and not receive the address.
Only workaround is to re-launch Netdirect after initial failure. As session will be cached, it will use the assigned address the 2nd time.
No plan to fix this in 7.x maintenance release. Q01904885-01 submitted for consideration in 8.x release.

**Q01968639** The default WTS port forwarder configuration on the NVG configures the tunnel with a local address of 127.0.0.2. On Mac OS the port forwarder fails to initialize and gives a java error. This behavior occurred because loopback behavior of MAC OS differs from Linux and Windows. On Linux and Windows, anything in 127.0.0.x is treated as a loopback. On Mac OS only 127.0.0.1 works for loopback. Any of the other 255 numbers fail to loopback. And in Mac OS, the loop back alias has to be added manually.
Workaround is to use local tunnel address as 127.0.0.1 while configuring the WTS link or by manually adding alias for loop back interface lo0 as 127.0.0.2.
No fix is planned for this CR in any future maintenance or major software releases.

**Q01903561** The Symantec Enterprise Vault installed on the exchange server adds a search option for OWA in the Navigation bar which is displayed when using the premium mode (IE6 / IE7 supported mode). With IE6 this is working properly but when using IE7 the gif file is missing from the navigation bar as such can't run the query. The issue is related to gzip compression.
Work around is to add Accept-Encoding header in /cfg/vpn #/adv/rewrite menu so that gif will load properly.
No plan to fix this in 7.x maintenance release. Q01903561-01 submitted for consideration in 8.x release

**Q01977822** Upgrade from 7.x to 7.1.3.0 in SSL 1000 module will fail due to memory constraints.
Work around is to backup the config (/cfg/ptcfg), install 7.1.3.0 boot image, do the initial setup and import the saved configuration (/cfg/gtcfg).
No fix is planned for this CR in any future maintenance or major software releases.

**Q01987343** Portal wts link fails to access Windows Vista terminal server while using java RDP client. The reason is Vista supports RDP v6.0 and NVG's java RDP client supports RDP v5.0 only.
This is submitted for consideration in 8.x release.

**Q01351656** Siteminder authentication is not working properly when crossing from a realm with a lower protection level, to another realm with a higher protection level. The expected behavior is to verify client session cookie and if the protection level is found to be less that its realm, it should force client to authenticate to the realm. But NVG is seeing the presence of the SMSSESSION cookie, and simply tries to present it to access realm with higher protection level.
No plan to fix this in 7.x maintenance release. Q01351656-01 submitted for consideration in 8.x release

**Q01930997** There is a security threat that the Symantec on Demand Agent (SODA) setup.xml file can be edited to alter anything including the security settings of virtual desktop.
Workaround is to disable switching between desktops via cli command
/c/vpn #/vdesktop/switch off
No plan to fix this in 7.x maintenance release. Q01930997-01 submitted for consideration in 8.x release.

**Q01957891** WTS screen size settings do not work when hidepf setting is ON.
No plan to fix this in 7.x maintenance release. Q01957891-01 submitted for consideration in 8.x release.

**Q01886963** When the client on port 81 sends a reset, the SSL in turn converts this to a FIN-ACK followed by a RST to backend server on port 443 which seems to be incorrect. The correct way is that SSL should also send a RST to the backend server once it received a RST from the client.
No plan to fix this in 7.x maintenance release. Q01886963-01 submitted for consideration in 8.x release.

**Q01956973** SMB link to Windows 2008 Fails with POSIX error.
No plan to fix this in 7.x maintenance release. Q01956973-01 submitted for consideration in 8.x release.

# APPENDIX A
# NVG Compatibility Matrix for 7.1.x Maintenance Releases
**(See release notes above for limitations)**

| Client OS (Minimal Java Runtime Engine (JRE) is 1.4.2 if applicable) | Portal Mode | Port Forwarder | NetDirect | NetDirect installed | TG/NHA agent | TG/NHA portal | SPO | SODP |
|---|---|---|---|---|---|---|---|---|
| **Windows 2000 Professional** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |
| **Windows XP Professional** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |
| **Windows XP 64-bit** | 7.1.3.0 | x | x | x | x | x | x | x |
| **Windows Vista Home Basic** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |
| **Windows Vista Premium** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |
| **Windows Vista Business** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |
| **Windows Vista Ultimate** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |
| **Windows Vista 64-bit** | 7.1.3.0 | x | x | x | x | 7.1.3.0 | x | x |
| **MAC OS - 10.4** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | x | x | x | x | x |
| **MAC OS - 10.5** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | x | x | x | x | x |
| **MAC OS - 10.6** | 7.1.3.0 | x | x | x | x | x | x | x |
| **Redhat 9** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | x | x | x | x | x |
| **Fedora Core 4** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | x | x | x | x | x |

| Applications | Win2K | Win XP | WinXP64 | Vista | Vista 64 | MAC OS 10.4/10.5 | RH 9 | Fedora |
|---|---|---|---|---|---|---|---|---|
| **IE6** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | x | x | x | x | x |
| **IE7** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | x | x | x |
| **IE8 (Beta 2)** | x | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | x | x | x |
| **Firefox 3** | x | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 | x | 7.1.3.0 | 7.1.3.0 |
| **Safari 3.0** | x | x | x | x | x | 7.1.3.0 | x | x |
| **Opera** | x | x | x | x | x | x | x | x |
| **TunnelGuard/NHA 4.0** | 7.1.3.0 | 7.1.3.0 | x | 7.1.3.0 | x | x | x | x |
| **TunnelGuard/NHA 4.5** | 7.1.3.0 | 7.1.3.0 | x | 7.1.3.0 | x | x | x | x |
| **TunnelGuard/NHA 5.0** | 7.1.3.0 | 7.1.3.0 | x | 7.1.3.0 | x | x | x | x |

| Backend Servers | Portal Mode | Port Forwarder | SPO |
|---|---|---|---|
| **OWA 2003** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |
| **OWA 2007** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |
| **Sharepoint 2003** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |
| **Sharepoint 2007** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |
| **Lotus Domino 7.0** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |
| **RSA Soft token** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |
| **Citrix-4.0** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |
| **Citrix-4.5** | 7.1.3.0 | 7.1.3.0 | 7.1.3.0 |

x - Not officially supported or not applicable

For other known issues, please refer to the product release notes and technical documentation available from the Nortel Technical Support web site at: http://www.nortel.com/support.

---