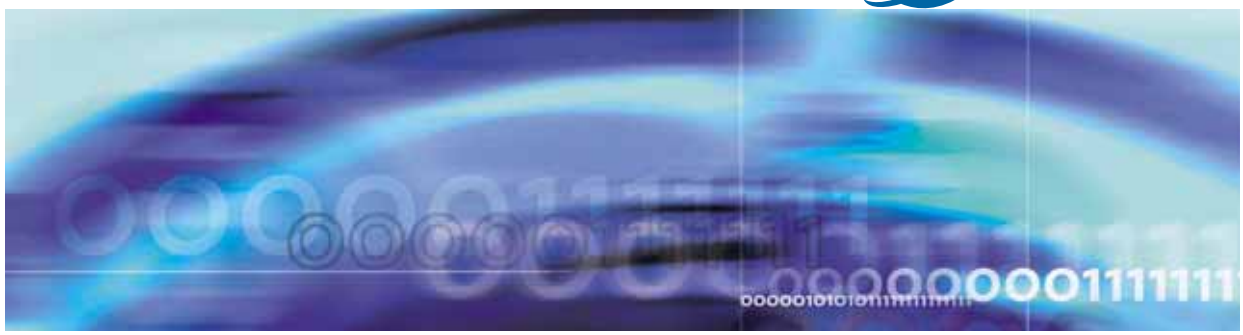

Nortel Secure Network Access Switch

Release Notes for Software Release 1.6.1.X

NN47230-400

Document status: Standard
Document version: 02.08
Document date: 16 July 2008

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.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

*Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other products or services may be trademarks or registered trademarks of their respective owners.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

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.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

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.

Portions of the TunnelGuard code include software licensed from The Legion of the Bouncy Castle.

See *Nortel Secure Network Access Switch 4050 Configuration - Using CLI (NN47230-100)* for more information.

Nortel Networks software license agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. **Licensed Use of Software.** Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.
2. **Warranty.** Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.
3. **Limitation of Remedies.** IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS),

WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The foregoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. **General**

   a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

   b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

   c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

   d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

   e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

   f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Release Notes for Nortel Secure Network Access Solution 1.6.1.X **7**

Overview 7
- Nortel Secure Network Access Switch 4050 8

New software features in this release 8
- Improved Multi-OS Support in TunnelGuard Applet 8
- LDAP enhancements 9
- User remediation 10
- NSNA Client for Linux and Mac 10

Customer Enhancement requests 11

Supported hardware and software 12
- Switch hardware and software 12
- Client hardware and software 12
- Back-end services 14
- Delivered software images 14
- Threshold specifications 15
- Performance and scalability 16

Upgrading to Nortel SNAS 1.6.1.X 16

Implementing the Nortel SNA solution 17
- Nortel SNAS 4050 upgrade 17
- Implementation guidelines 17

Issues fixed in Nortel SNAS 1.6.1.4 release 18

Issues fixed in Nortel SNAS 1.6.1.3 release 19

Issues fixed in Nortel SNAS 1.6.1.2 release 19

Issue fixed in Nortel SNAS 1.6.1.1 release 20

Issues fixed in Nortel SNAS 1.6.1 release 20

Known limitations and considerations in this release 21

Reading path 27
- Related publications 27

Hard-copy technical manuals 28

How to get help 28

Release Notes for Nortel Secure Network Access Solution 1.6.1.X

These release notes for the Nortel* Secure Network Access (Nortel SNA) solution describe the hardware, software, and any known limitations and considerations that exist in this release. The release notes are based on Nortel Secure Network Access Switch Software Release 1.6.1.X (all versions 1.6.1, 1.6.1.1, 1.6.1.2, 1.6.1.3, and 1.6.1.4).

For a list of related publications, see "Related publications" (page 27). For copies of Nortel SNA solution documentation, see the CD included with your software or the Nortel technical documentation Web site, www.nortel.com/support. For more information, see "Reading path" (page 27).

These release notes cover the following topics:

Topic
"Overview" (page 7)
"New software features in this release" (page 8)
"Supported hardware and software" (page 12)
"Implementing the Nortel SNA solution" (page 17)
"Known limitations and considerations in this release" (page 21)
"Reading path" (page 27)
"Hard-copy technical manuals" (page 28)
"How to get help" (page 28)

The information in these release notes supersedes applicable information in other NSNA documentation.

Overview

The Nortel SNA solution is a protective framework to completely secure the network from endpoint vulnerability. The Nortel SNA solution addresses endpoint security and enforces policy compliance. Nortel SNA

delivers endpoint security by enabling only trusted, role-based access privileges premised on the security level of the device, user identity, and session context. Nortel SNA enforces policy compliance, such as for Sarbanes-Oxley and COBIT (Control OBjectives for Information and related Technology), ensuring that the required anti-virus applications or software patches are installed before users are granted network access.

For Nortel, success is delivering technologies providing secure access to your information using security-compliant systems. Your success is measured by increased employee productivity and lower network operations costs. Nortel's solutions provide your organization with the network intelligence required for success.

Nortel Secure Network Access Switch 4050

The Nortel Secure Network Access Switch 4050 (Nortel SNAS 4050) controls the operations that secure the network, working with edge switches and network back-end servers and applications to provide an out-of-path solution. The Nortel TunnelGuard network manager monitors user sessions controlled through ports enabled for Nortel SNA. The Nortel Security & Routing Element Manager (SREM) and Browser Based Interface are GUI tools that you can use to configure and manage the Nortel SNA switch and to monitor solution statistics

The 1.6.1.4 is a maintenance release. You can find the list of resolved CRs for the Release 1.6.1.4 in "Issues fixed in Nortel SNAS 1.6.1.4 release" (page 18) section.

New software features in this release

This section provides the information about the new Nortel SNAS feature in this release.

Improved Multi-OS Support in TunnelGuard Applet

TunnelGuard is currently supported on Windows. It does not run on non-Windows operating systems (OSes). The "Multi-OS Support" feature allows the TunnelGuard to identify Linux operating system or Macintosh operating system users and collect the necessary information. The TunnelGuard is allowed to identify the operating system as Linux or Macintosh and collect the device specific information and also performs additional compliance checks for those operating systems.

The following types of Linux operating system are supported:

- RedHat Enterprise Linux 4
- RedHat Enterprise Linux 3
- Fedora Core 5 and later
- SUSE Linux Enterprise 10

The following types of Macintosh operating system are supported:

- Mac OS X Server v10.5 Leopard
- Mac OS X Server v10.4 Tiger
- Mac OS X v10.3 Panther
- Mac OS X v10.2
- Mac OS 9

- SNAS management using BBI

  The Browser Based Interface (BBI) is an internet browser based application you can use to configure and manage the Nortel SNAS 4050.

  For specific information about using BBI, see *Nortel Secure Network Access Switch 4050 Configuration – Using BBI (NN47230-500)*.

- Nortel TunnelGuard System Agent

  The Installed Tunnel Guard Agent provides a client component for the NSNA solution that runs as a system service under the Microsoft Windows 2000, XP, and Vista operating systems. The TunnelGuard System Agent supports both system and user authentication and provides single sign-on support for user authentication.

  For more information on installable TunnelGuard agent, see *Nortel Secure Network Access Switch 4050 Configuration – Using TunnelGuard System Agent (NN47230-501)*.

- Nortel TunnelGuard Desktop Agent

  The TunnelGuard Desktop Agent is a small cached version of a JAVA application. TunnelGuard desktop agent helps ensure that clients are always running the latest version of the application and eliminates complicated installation or upgrade procedures.

- Nortel TunnelGuard Browser Applet

  A browser based JAVA applet providing a client-less captive portal solution for Windows, Mac and Linux endpoints.

LDAP enhancements

Following are enhanced features for the backend LDAP authentication support:

- Native groups

  The use of native groups from LDAP eliminates the need of managing multiple sources of user data while integrating the NSNAS with an environment based on LDAP as user database.

- Short Group Format

Lets you configure the SNAS to extract the first part of a returned Distinguished Name (DN) as the group name to be used.

- Advanced

  The Advanced LDAP menu is used to configure the desired attribute/value when searching for a user record in an LDAP/Active Directory database. The feature is disabled by default, which means that no extra requirement is added when searching for a user record.

User remediation

The 'kick' command in the CLI has been modified to kick a user session based on username, IP address, or MAC address. An updated Nortel Threat Protection Remediation Module is also provided as part of this release.

```
Main# /info/kick/

[Kick Menu]

user - Kick user by name

addr - Kick user by ip or mac address
```

NSNA Client for Linux and Mac

To provide DHCP-based IP address renewal on Linux or Mac, NSNA Client uses shell script to determine system configuration and perform necessary operations, which is automatically deployed to user machine by TunnelGuard applet.

Certain configuration changes must be done to allow low-privilege users to execute necessary commands for DHCP-related operations (these commands require root-level permissions by default).

Some systems or distributions can lack in one or more system tools to perform IP renewal operations.

Requirement summary

This section gives a quick overview of required tools for correct operation of TunnelGuard client.

System Tools Following is the list of system tools:

- **Text-processing/parsing**—grep, sed, awk. (Linux/Max) Usually, present out of the box on most distributions.
- **Network configuration information**—ifconfig (/sbin/ifconfig, Linux, Mac). Usually, present out of the box. Our script only uses this utility to get information about internet connection (such as IP address, network mask), thus no special permissions or configurations required, all users are allowed to this.
- **Network routing information**—ip (/sbin/ip, Linux Only). This utility is required to determine, which network interface is used for

communication with SNAS server. Mostly present on most distributions but Debian 3.1 (Sarge) is missing this system tool in default installation.

- **Java Runtime Environment 6.0 or later**— this is prerequisite for TunnelGuard operation.

Supported DHCP client tools Following is the list of supported DHCP client tools:

- **ISC's dhclient**—most often used modern DHCP client tool. (Usually found in RedHat-based, Debian-based, Ubuntu, and other distributions)
- **dhcpcd**—another popular DHCP client tool (Usually found in Slackware, SuSE, and few other distributions)
- **pump**—deprecated RedHat's dhcp client tool, found in old RedHat builds.
- **Mac OS X DHCP Client**—mac OS X native DHCP client.

Tested Distributions

The operation of NSNA Linux/Mac client are tested and verified on the following distributions.

- Debian Sarge 3.1
- Debian Etch 4.0
- Fedora Core 4 – Core 8
- Mac OS X Tiger 10.4
- Mac OS X Leopard 10.5

Customer Enhancement requests

This section lists the customer enhancement request CRs.

- User profile should not allow login after system profile login failure. - Q01744656
- Based on group policy, user authentication is allowed only from system authenticated and system policy compliant PCs. A new group policy "sysauthmust" is added to make restriction configurable. The "sysauthmust" will be false by default. User Authentication is allowed without system login with default setting.
  BBI
  Config > Secure Access Domain > AAA > Groups

  - Q01814752

Supported hardware and software

The Nortel SNAS performs authentication and posture assessment for end points connected to access devices typically deployed at the network edge. Nortel SNAS SSCP technology has been incorporated into ERS 5500 and ERS8300 series of products. Nortel SNAS technology also can perform authentication and posture assessment for non-SSCP enabled switches and Ethernet routers by using the DHCP mode of enforcement. In this mode SNAS provides a network agnostic mode of operation supporting non-SSCP switching platforms such as (and not limited to) ES 325, 425, 450, 460, 470, and ERS 2500, 4500, 8600, and non-Nortel Ethernet Switching platforms. The Nortel SNA solution secures both PC and Voice over IP (VoIP) phone clients in the network.

Switch hardware and software

"Supported network hardware and software" (page 12) lists supported network hardware and software.

Supported network hardware and software

Component	Specifications
Core router	Nortel Ethernet Routing Switch 8600 or any make or model router of similar specifications
Nortel SNAS 4050	Nortel Secure Network Access Switch Software Release 1.6.1.X Nortel Tunnelguard System agent Release 3.5 or later
Edge switch (network access device) options:	
• Nortel Ethernet Routing Switch 5510, 5520, 5530 • Nortel Ethernet Routing Switch 8300	Nortel Ethernet Routing Switch 5500 Series, Software Release 5.0.4 or later Nortel Ethernet Routing Switch 8300 Series, Software Release 4.0 supports NSNA 1.6.1.X) Java Device Manager (JDM) 6.0.2.0 or later

Client hardware and software

"Supported PC client hardware and software" (page 13) lists supported PC client hardware and software.

Note: The current release of SREM client software is not supported on UNIX or Linux platforms.

Supported PC client hardware and software

Client hardware and software	Versions
PC clients	Microsoft Windows 2000 Professional SP4 Microsoft Windows XP SP2 Windows Vista MAC OS Linux OS Non-Interactive Devices
Browser options	Internet Explorer 6.x, and 7.x Mozilla Firefox 1.x, and 2.x Netscape Navigator 8.0.x Safari
Java Runtime Environment (JRE)	JRE 1.5.0.10+ (JRE 1.6 recommended)

"Supported VoIP client phone models, call servers, and firmware versions" (page 13) lists supported VoIP phone models, call servers, and firmware.

Supported VoIP client phone models, call servers, and firmware versions

VoIP phone model	Business Communications Manager BCM50e: Build_1.28 BCM1000: Version 3.6	Communication Server 1000, Version 4.5	Multimedia Communication Server 5100, Version 3.0
IP Phone 2002 model NTDU76 (Nortel SNA Phase1)	F/W 0603B60	F/W 0603B60	F/W 0603B60
IP Phone 2002 model NTDU91 (Nortel SNA Phase2)	F/W 0603D65	F/W 0603D65	F/W 0603D65
IP Phone 2004 model NTDU92 (Nortel SNA Phase2)	F/W 0604D65	F/W 0604D65	F/W 0604D65
IP Phone 2007 model NTDU96 (Nortel SNA Phase2)	F/W 0621C23	F/W 0621C23	F/W 0621C23

VoIP phone model	Business Communications Manager BCM50e: Build_1.28 BCM1000: Version 3.6	Communication Server 1000, Version 4.5	Multimedia Communication Server 5100, Version 3.0
IP Phone 1140 model NTDU (Nortel SNA Phase 2)	F/W 0625C3C	F/W 0625C3C	F/W 0625C3C
IP Phone 1120 model NTDU (Nortel SNA Phase 2)	F/W 0624C3C	F/W 0624C3C	F/W 0624C3C

Back-end services

"Authentication software and back-end services" (page 14) lists authentication and other back-end services specifications.

Authentication software and back-end services

Software	Version
LDAP authentication	Microsoft Windows 2000 SP4, Windows 2003, Windows Vista, Open LDAP 2.2.26, iPlanet 4.1 LDAP-S: iPlanet 4.1, Open LDAP 2.2.13
RADIUS authentication	PAP: FreeRadius, Steel-Belted Radius (SBR) 5.0.2 MS-CHAP v2: Steel-Belted Radius (SBR) 5.0.2, Microsoft Windows IAS (2000 SP4, 2003)
DHCP	NSNAS, Microsoft Windows 2000 Server SP4, Linux Fedora
DNS	Microsoft Windows 2000 Server SP4, Linux Fedora

Delivered software images

"Nortel SNAS 4050 software images" (page 14) lists Nortel Secure Network Access Switch 4050 software images you can download from the Nortel Service Portal. For initial installation, download the boot image. For upgrades, download the complete upgrade package.

Nortel SNAS 4050 software images

Product	Image type	File name
SNAS	Boot	NSNAS-1.6.1.4-boot.img
	Upgrade Package	NSNAS-1.6.1.4-upgrade_complete.pkg
SREM	Windows exe	srem_1.2.2.0_016.exe

Product	Image type	File name
TunnelGuard System Agent Release 4.5	with bundled JRE	TgVm_4_5.exe
	without JRE	TgNoVm_4_5.exe
	Customizable MSI package with bundled JRE	TgCstVm_4_5.msi
	Customizable MSI package without bundled JRE	TgCstNoVm_4_5.msi

Note: During a SREM software upgrade, the window with the previous version does not close automatically. Close the window with the previous SREM version before installing a new version.

Threshold specifications

"Hardware and software upper limit thresholds" (page 15) lists upper limit thresholds for hardware and network security software in the Nortel SNA solution.

Hardware and software upper limit thresholds

Item	Maximum
Nortel SNAS 4050 devices in a cluster	4
Network access devices for each Nortel SNAS 4050 (where the Ethernet Routing Switch 8300 series access device is a single chassis, and the Ethernet Routing Switch 5500 can have a stack of eight units representing one logical unit controlled by the Nortel SNAS 4050)	25
Users for each Nortel SNAS 4050 *By default, each Nortel SNAS 4050 device ships with 200 user licenses. Upgrade license packs of 100, 250, 500, 1000, 2000, and 5000 additional licenses are available.	2500*
Users for each Nortel SNAS 4050 cluster	10,000
Red VLANS for each network access device	1
Yellow VLANS for each network access device (number mapped to switch parameters)	5
Green VLANs for each network access device (number mapped to switch parameters)	5

Performance and scalability

A single Nortel SNAS 4050 supports 2500 concurrent user connections. When clustered for high availability and load balancing, the Nortel SNA solution supports 10,000 concurrent user connections in a cluster. A single cluster supports a maximum of 4 Nortel SNAS 4050 devices. Nortel SNAS supports up to 200 policy enforcement points. It can include a combination of SSCP Enabled PEPs, SSCP-Lite PEPs and 802.1x or Radius Enabled PEPs. To meet these numbers, recommended hardware configuration of Nortel SNAS is:

- IBM 3060 Platform
- 2 x 2.33 GHz Dual-Core
- 6 GB RAM
- 1 x 250 GB SATA
- Dual Power 2 x 10/100/1000
- Cavium 1010 Crypto

Upgrading to Nortel SNAS 1.6.1.X

Secure Network Access Switch running on prior versions of SNAS software can be upgraded to SNAS Release 1.6.1.X. SNAS Release 1.6.1.X includes a new SNAS quick setup wizard that pre-configures many of the sophisticated features, embedded by default with Release 1.6.1.X.

The new SNAS quick setup wizard:

- is available only for network administrator who creates a ‘new’ SNAS cluster while configuring the SNAS
- includes sample configurations for TunnelGuard System Agent, TunnelGuard Desktop Agent and enables the new BBI for web management
- helps the network administrators in configuring the SNAS with the new capabilities of SNAS Release 1.6.1.X

With the help of TunnelGuard tool, the network administrator can associate a SRS rule to a specific OS (Windows 2000, XP, and Windows Server 2003). After upgrade from Release 1.5.1 to 1.6.1.X the existing rules gets applied for all the Operating Systems. If the admin is creating a SRS rule, specific to Operating System in Release 1.6.1.X and performs the downgrade followed by upgrade i.e. Release 1.6.1.X -> 1.5.1 -> 1.6.1.X, all the SRS rules are applied to Operating Systems.

For more information, see the *Nortel Secure Network Access Switch 4050 Configuration – Using BBI (NN47230-500)*.

Implementing the Nortel SNA solution

Implement the Nortel SNA solution by considering the current topology, planning the implementation, and then installing and configuring the switches, the Nortel SNA network security software, and the back-end services.

Nortel SNAS 4050 upgrade

Before you start, upgrade the Nortel SNAS 4050 to use the latest software, following instructions listed in the *Nortel Secure Network Access Switch 4050 Configuration - Using CLI (NN47230-100)* ,*Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*, or *Nortel Secure Network Access Switch 4050 Configuration – Using BBI (NN47230-500)*.

Implementation guidelines

To implement the solution, follow these general guidelines. For guideline details, see the *Nortel Secure Network Access Solution Guide (NN47230-200)*.

Step	Action
1	Make a preliminary study and plan the implementation.
2	Configure the DHCP server.
3	Configure the Ethernet Routing Switch 8600 with VLAN and port number assignments, VLAN tagging, and DHCP relay enabling. For instructions, see the configuration samples in the *Nortel Secure Network Access Switch 4050 Configuration - Using CLI (NN47230-100)*, *Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*, or the *Nortel Secure Network Access Switch 4050 Configuration – Using BBI (NN47230-500)*.
4	Configure edge switches, either the Ethernet Routing Switch 55xx or the Ethernet Routing Switch 8300. For instructions, see *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 5.0.2 (NN47200-400)* or *Nortel Ethernet Routing Switch 8300 Configuration — Security using Device Manager (NN46200-508)Nortel Ethernet Routing Switch 8300 Configuration — Security using Device Manager (NN46200-508)* and *Nortel Ethernet Routing Switch 8300 Configuration — Security using CLI and NNCLI (NN46200-503)*.
5	Configure the Nortel SNAS 4050 with TunnelGuard rules, and enable the edge switches for Nortel SNA management.

For instructions, see the *Nortel Secure Network Access Switch 4050 Configuration - Using CLI (NN47230-100)*, *Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*, *Nortel Secure Network Access Switch 4050 Configuration – Using BBI (NN47230-500)*, or the *Nortel Secure Network Access Switch 4050 Configuration – Using TunnelGuard System Agent (NN47230-501)*.

Note: To enable TunnelGuard to run on all PC clients, download the Java Runtime Environment (JRE) from the Nortel SNAS 4050 to each PC being secured through Nortel SNA. (During use, The TunnelGuard applet does not exit when the browser is closed, in all cases. Nortel SNA functionality is not affected.)

6 Test the system.

7 Add LDAP and/or RADIUS authentication.

8 Customize the Nortel SNAS 4050 portal.

For instructions, see the *Nortel Secure Network Access Switch 4050 Configuration - Using CLI (NN47230-100)*,*Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*, *Nortel Secure Network Access Switch 4050 Configuration – Using BBI (NN47230-500)*, or the *Nortel Secure Network Access Switch 4050 Configuration – Using TunnelGuard System Agent (NN47230-501)*.

—End—

Issues fixed in Nortel SNAS 1.6.1.4 release

The following table lists the issue fixed with the Nortel SNAS in this release:

Change Request Number	Issue Description
Q01895327	DNS Cache ttl values do not function or clear cache
Q01744656	User profile should not allow login after system profile login failure.
Q01888919	Client goes to system green even if syscredent is disabled for a group.
Q01844941	DHCP Discovery is ignored by the SNAS, if the DHCP packet contains "PADDING" before "END OPTION", SNAS ignores the packet.
Q01746547-01	BBI support missing for /cfg/domain 1/aaa/auth x/ldap/enashortgr support.
Q01736701-01	NSNA unable to forward admin rights through BBI.

Q01753630	Web authentication and desktop agent are not working after 5 or 10 minutes, even though the user is not idle, the user is logged out. Web authentication and desktop agent work when single sign on with system agent.
Q01814752	File log does not give all information. Added new radius accounting attributes like framed-ip, calling-station-id, event-timestamp. Also interim-update accounting type added for client IP address change events.
Q01853417	Webstart does not work when TG Installable Client 4.5 is installed in the client. Webstart Agent upgraded 4.5.0.10

Issues fixed in Nortel SNAS 1.6.1.3 release

The following table lists the issue fixed with the Nortel SNAS in this release:

Change Request Number	Issue Description
Q01791067	With DHCP Hub Mode, Portal not working with Fedora 7
Q01801928	License problem when using TG System Health Agent
Q01822404	With fresh windows client installation, unable to load the Desktop agent
Q01736421	NSNA unable to forward admin rights through Mgmt GUI
Q01816251	With DHCP Hub mode on Debian, IP not changed even though Compliance successful
Q01655151	No meaningful message to user when installing TgNoVm on non JVM PC
Q01791078	With DHCP Hub, Portal not showing the policy compliance page
Q01774038	Single Sign On Logout Failure - syscredentials /BBI issue
Q01803706	With Dhcp Hub mode, observing portal logout if TG runonce is configured
Q01799914	Observing mismatch in the client port number
Q01839974	SNAS crashing for Portal login-hubmode-nonadmin-vista client
Q01437702	Linux OS- Click on home page takes it back to portal page after

Issues fixed in Nortel SNAS 1.6.1.2 release

The following table lists the issue fixed with the Nortel SNAS in this release:

Change Request Number	Issue Description
Q01694693	Tunnel Guard should not display warning window for failed sessions in non-snas networks.
Q01716538	Tunnel Guard should allow inheritance for preferences from global profile.ini.
Q01717277	Problem writing global profile.ini on Vista.
Q01721351	Bypass user authentication when SSO is with blank password profile.

Q01723916	Supports SSO on non-english versions of Windows.
Q01719753	Tunnel Guard needs to use same VIP Address to help SNAS support Clustering environment.

Issue fixed in Nortel SNAS 1.6.1.1 release

The following table lists the issue fixed with the Nortel SNAS in this release:

Change Request Number	Issue Description
Q01693855	Fixes a minor issue where after an upgrade to 1.6.1.0 from a previous version of software the new configuration menu items for new SNAS 1.6.1 features were not available.

Issues fixed in Nortel SNAS 1.6.1 release

The following table lists the issues fixed with the Nortel SNAS in this release:

Change Request Number	Issue Description
Q01400674	Non-admin VLAN movement works on Windows XP in all cases, but works on Windows 2000 only if non-admin users are added to "Act as Part of Operating System".
Q01400683	CLI: A subnet cannot be enabled unless known settings for SNAS DHCP filter mode and unknown stdopts (standard options) 51 for unknown settings are set.
Q01404163	When using any browser with Tunnel Guard debug logging enabled, there can be an increase in browser memory use during an extended session.
Q01441795	MAC OS X session is removed from the SNAS after being logged in for approximately 30 minutes. This is because the MAC OS X Sleeping feature shuts down the interface, which subsequently causes the switch to send the SNAS a Port Down event.
Q01445368	If a PC has a MAC trusted entry with a group having no extended profile, the PC still able to do MAC authentication but the session is RED.
Q01451799	When deleting a user from the local database, the session that has username be same with the user will be logged out even this session come from other authenticators (LDAP, Radius).
Q01463622	When using pasted configuration information an error can occur.
Q01453733	If a TunnelGuard rule is dynamically changed, it won't be in effect until users have been kicked out and logged back in. At this time, users must be kicked out individually. The change will take place the next time a user logs in.
Q01390392	The SNAS may not delete an unused phone session.

Q01441788	A improper message may appear when a user logs into a group which has no extended profile.
Q01444510	There may be a hostname mismatch when obtaining a certificate from the portal.
Q01413600	May not show a proper error when importing or exporting incorrect info.
Q01449086	URL Redirect not showing correctly.
Q01452070	Surfing from a redirected page causes a user to be logged out.
Q01453514	Login may take extended period of time if LDAP is placed ahead of authenticators. To work around this issue always put authenticators ahead of LDAP.
Q01346043	Software Definition is deleted after user hit Esc key to cancel the deletion. Use the Cancel button instead.

Known limitations and considerations in this release

The following table lists the open issues with the Nortel SNAS, the SREM and the 5500 Series Switch.

Nortel SNAS

Change Request Number	Issue
Q01355912	"A PC IP address may remain in the Green VLAN (the user had successfully logged in) after the user closes the browser and the NSNAS has detected the heart beat time-out. This may occur when the user has had multiple tabs open on the browser. Workaround: Issue the ipconfig/release and ipconfig/renew commands."
Q01400674	"The error reported by TunnelGuard, ""ERROR_PRIVILEGE_NOT_HELD"", is a known issue. Non-admin VLAN movement works on Windows XP in all cases, but works on Windows 2000 only if you set the following: 1. Open **Control Panel > Administrative Tools > Local Security Settings**. 2. Click on **Local Policies > User Rights Assignment**. 3. Select "**Act as Part of Operating System**", and add your non-admin user here.
Q01400683	CLI: A subnet cannot be enabled unless known settings for SNAS DHCP filter mode and unknown stdopts (standard options) 51 for unknown settings are set.

Change Request Number	Issue
Q01408803	Syslog messages do not indicate if a client changes filter only when only the filter is changed and not the VLAN. The messages indicate only that the client moved to the Green VLAN.
Q01342957	A PC client may not be able to log in if it is rapidly disconnected and reconnected. To enable access, a PC client can do one of the following: 1. Enter these commands at the Windows command prompt: Ipconfig /release Ipconfig /renew 2. Disconnect the PC client and reconnect after a few seconds.
Q01427662	Clients using MAC OSX Safari browser may encounter pop up Certificate acceptance messages. ***Workaround***: Accept the messages
Q01434429	Network access is denied if admin rights for the user using the device are not configured in hub mode setup
Q01404163	When using any browser with Tunnel Guard debug logging enabled, there may be an increase in browser memory use during an extended session. ***Workaround***: Use the fatal level for TunnelGuard logging and the default configuration of Java Console enabled.
Q01437702	If a user has logged into the portal using a Mozilla browser and tries to open a new tab or window to access their homepage, they get directed to the portal login page. After several attempts, a user may be able to access the homepage. **Solution**: Use another instance of the browser.
Q01440906	When adding a MAC database entry for a PC with parameter dev = phone, the PC will be placed in the GREEN VLAN. In this scenario, the PC should be placed in the RED VLAN.
Q01441795	MAC OS X session is removed from the SNAS after being logged in for approximately 30 minutes. This is because the MAC OS X Sleeping feature shuts down the interface, which subsequently causes the switch to send the SNAS a Port Down event.
Q01445368	If a PC has a MAC trusted entry with a group having no extended profile, the PC still able to do MAC authentication but the session is RED.

Change Request Number	Issue
Q01446249	The Opera web browser cannot run the TunnelGuard applet, so the user cannot login. This is a limitation of the Opera web browser. To workaround this issue, use Internet Explorer or Mozilla as a web browser.
Q01451774	Command "/info/sessions 1 1 tg" does not show users with a “tg” username prefix. To workaround this issue, use the "/info/sessions 1 1 tg*" command.
Q01451799	When deleting a user from the local database, the session that has username be same with the user will be logged out even this session come from other authenticators (LDAP, Radius)
Q01342957	When a PC on the GREEN VLAN is unplugged from its port and plugged into another, it will be directed to the login page when trying to access the internet. This is due to a PC limitation. To workaround this issue, perform the commands “ipconfig/ release” and “ipconfig /renew”.
Q01348979	In some cases, the Ctrl-X TunnelGuard hotkey may not function. To workaround this issue, close TunnelGuard using the Close button in the upper right, or close from the file menu.
Q01362593	If users change the window view settings on a Windows operating system, the portal pops up asking if the user would like to log out. Users can choose if they want to log out or stay logged in.
Q01411833	When closing a TunnelGuard applet that is running in a tab of the Firefox web browser, TunnelGuard is not able to renew the address and an error message is displayed in the java console. Due to different implementations of the tabbed browsing feature, tabbed browsing is not supported at this time.
Q01418068	In a cluster, performing the /boot/delete command to delete a SNAS which handle MIP and control a switch, TG PCs on the switch might be logged out.
Q01454897	No error message appears if a user is created and not assigned to a group. The user should require a group assignment prior to creation, and an error message should appear.
Q01387768	The "Add MAC" option for phone devices is redundant and will be removed.
Q01415269	To join a Multi-trunking NSNAS into a cluster unplug all unused ports when running the join wizard.

Change Request Number	Issue
Q01427585	The Admin Rights feature may reveal the admin password to a normal user.
Q01437701	When kicking out a TG PC login session, if the logout button is clicked, the user may not be able to log back in immediately.
Q01439061	RADIUS Authentication cannot fallback to a local user.
Q01439871	inet_dns command crashes the SNAS.
Q01440956	Hub support cannot resist against DHCP attacks.
Q01442679	A TG PC may be logged in, but redirected to the login page when trying to access the portal homepage.
Q01443515	A PC's green status may remain the same after the MAC has been removed from the database.
Q01444426	A PC may maintain a green filter even if removed from the MacDB.
Q01445148	Yahoo Instant Messenger may lose its connection after logging into the SNAS. To workaround this behavior, put YIM in the exclude list.
Q01445279	When saving trace output to an external TFTP server, the SNAS may only log the first TG PG login.
Q01445327	When update a Global option, DHCP subnets still provide old values for clients. Disable/re-enable subnets required to make the change affected.
Q01449080	TG icon may not display properly when combined with hyperlinks.
Q01454814	When exporting a certificate using the wrong username or password via scp/sftp, an error message displayed with no information.
Q01664804	TunnelGuard Agent does not work properly after stop/start services.
Q01684744	Enhance to have user session back after switched user back to a logged user.

Nortel SREM

Change Request Number	Issue
Q01348029	"You cannot close the following SREM dialog boxes using the Esc key: 1. Create New On Disk SRS Entry 2. Create New Memory Module SRS Entry 3. Registry Entry 4. Modify Registry Entry 5. Custom Path 6. Version Range 7. Date/Time Range 8. Software Definition Comment"
Q01425606	When copying Authentication and Switch info, the pasted info may not be the same as the copied info.
Q01436277	If a user is set to a non-existent group, the username will be removed from the database.
Q01422867-01	When inserting ranges, the Apply and Insert buttons perform the same function.
Q01453910	If a user clicks Refresh while viewing a client from the Sessions Table, the Session Table will be empty. To workaround this issue, use the Apply button instead.
Q01451801-01	Sessions Table does not refresh to reflect the numbers of sessions after users are kicked out. In accordance with Q01453910, use the Apply button to workaround this issue.
Q01463625	In almost all cases, searching from SREM search engine will return unexpected results.
Q01464557	SREM Help Index may not include all topics.
Q01466507	If both Performance and DHCP Stats charts are open and set to stay on top, a conflict will occur as each window wants to stay on top.
Q01343873	HashAlg is changed to "none" when modifying specify min/max version.
Q01346061	TunnelGuard SRS Builder: Hotkey Alt+E then M to select "Add Selected Memory Module as entry" does not function.
Q01346059	TunnelGuard SRS Builder: Hotkey Ctrl-C and Ctrl-V does not function. To utlize these function choose Copy or Paste from the Edit menu.
Q01348979	In some cases, the Ctrl-X TunnelGuard hotkey may not function. To workaround this issue, close TunnelGuard using the Close button in the upper right, or close from the file menu.

Change Request Number	Issue
Q01660174	SREM does not display AuthType values for connected clients. Connected Client Table does not have a column for AuthType.
Q01678434	SREM does not support the command CLI /cfg/dom 1/aaa/tg/desktopnam
Q01648236	SREM does not support these CLI commands revoke, gensigned, sign, test, and validate certif.
Q01647366	Windows Vista can not join domain in red vlan but Windows XP does.
Q01671454	SSO does not support Novell login from the taskbar icon. Novell SSO is supported only with GINA based Logon. It does not support Novell Logon from application that is launched after login to the desktop.

Nortel TunnelGuard System Agent

- Rebooting after uninstalling TunnelGuard 3.5 is required

  The Windows PC must be rebooted after uninstalling TunnelGuard 3.5. The uninstallation program does not prompt for a reboot, however if the PC is not rebooted certain functions such as mapping network drives and printers may not work properly.

- Microsoft Remote Desktop connections and TunnelGuard user session behavior

  While TunnelGuard has an active user session with the NSNAS, Microsoft Remote Desktop connections are supported only if a single user is logged into the computer at the same time (locally and remotely). System sessions with the NSNAS are unaffected by Remote Desktop connections.

  — Windows XP Professional

  If the system joins a domain OR if “fast user switching” a.k.a. FUS is disabled through the Windows registry or local computer policy then Remote Desktop connections are supported while TunnelGuard has an active user session as long as the same user is logging in remotely. If FUS is not disabled or if a different user is logging in remotely, the active TunnelGuard user session gets disconnected when the Remote Desktop session is established. If TunnelGuard user session termination is configured on the NSNAS to trigger a VLAN change then the Remote Desktop connection can also be lost.

  — Windows 2003 Server

Supported only if multi-user Terminal Services connections are disabled through registry. See the Microsoft article and search for AllowMultipleTSSesssions for instructions on how to disable multi-user terminal services connections in this link (*http://technet2.microsoft.com/windowsserver/en/library/5c96a496-6d14-43c7-a89f-4b4561a6fb9d1033.mspx?mfr=true*).

Note: Windows XP Professional, and Windows Vista are not supported.

- Fast User Switching

  Any active TunnelGuard user session with the NSNAS will be disconnected when a user switch is detected. System sessions are unaffected by fast user switching.

Reading path

This section lists documentation for the Nortel SNA solution, Nortel Secure Network Access Switch Software Release 1.6.1. For information about finding and accessing up-to-date documentation, see "Hard-copy technical manuals" (page 28).

Related publications

These publications are related to the Nortel SNA solution:

- *Nortel Secure Network Access Switch 4050 Installation Guide (NN47230-300)*
- *Nortel Secure Network Access Solution Guide (NN47230-200)*
- *Nortel Secure Network Access Switch 4050 Configuration - Using CLI (NN47230-100)*
- *Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*
- *Installing and Using the Security & Routing Element Manager (SREM) (NN47230-301)*
- *Release Notes for Enterprise Switch Manager (ESM), Software Release 6.2 (NN47300-400, Rev 02.02)*
- *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 5.1 (NN47200-400)*
- *Release Notes for the Ethernet Routing Switch 8300, Software Release 4.0 (NN46200-401, Rev 2.01)*
- *Ethernet Routing Switch 4500 Series Release Notes — Software Release 5.1 (NN47205-400_5_1)*

Hard-copy technical manuals

You can download current versions of technical documentation for your Ethernet Routing Switch 8300 from the Nortel customer support web site at www.nortel.com/support.

If, for any reason, you cannot find a specific document, use the **Search** function:

Step	Action
1	Click **Search** at the top right-hand side of the web page. The **Search** page opens.
2	Ensure the **Support** tab is selected.
3	Enter the title or part number of the document in the **Search** field.
4	Click **Search**.

—End—

You can print the technical manuals and release notes free, directly from the Internet. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.comURL to download a free copy of the Adobe Acrobat Reader.

How to get help

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

If you purchased a Nortel service program, contact Nortel Technical Support. To obtain contact information online, go to the www.nortel.com/contactus web page and click Technical Support.

Information about the Nortel Technical Solutions Centers is available from the www.nortel.com/callus web page.

An Express Routing Code (ERC) is available for many Nortel products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate the ERC for your product or service, go to the www.nortel.com/erc web page.

Nortel Secure Network Access Switch

Release Notes for Software Release 1.6.1.X

Publication: NN47230-400
Document status: Standard
Document version: 02.08
Document date: 16 July 2008

Sourced in Canada, India, and the United States of America

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