Nortel Secure Network Access Switch

Release Notes — Software Release 2.0

Release: 2.0
Document Revision: 03.04

www.nortel.com

NN47230-400 320850-E

Nortel Secure Network Access Switch
Release: 2.0
Publication: NN47230-400
Document release date: 24 March 2009

Printed in Canada, the United States of America, and India
LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS "WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Contents

Software license

This section contains the Nortel Networks software license.

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.

New in this Release

The following sections detail what's new in *Nortel Secure Network Access Switch Release Notes — Software Release 2.0*, NN47230-400 for Release 2.0.

Navigation

Features

See the following sections for information about feature changes.

New Features

For more information about new features, see "New features in Release 2.0 Software" (page 13).

Feature enhancements

Software enhancements in NSNAS includes, location based security, multiple language support, SRS policy, and LDAP enhancements. For more information about new features, see "New features in Release 2.0 Software" (page 13).

Other changes

See the following sections for information about changes that are not feature-related.

File names for upgrade

File names are updated; see "File names for this release" (page 20).

Document changes

The NSNA document suite is reformatted to comply with the Nortel Customer Documentation Standards. For more information about the new documents and changes, see *Nortel Secure Network Access Switch — Documentation Roadmap* (NN47230-103).

Multi-OS applet support

This release updates the OS that are currently supported for MAC and Linux. For more information, see “Multi-OS applet support” (page 17).

Introduction

This document describes new features, limitations, and known and fixed issues for Nortel Secure Network Access Switch (Nortel SNAS) Software Release 2.0.

For information about how to upgrade SNAS software, see “Upgrading to Nortel SNAS 2.0” (page 26).

Navigation

Important notices and new features

This section describes the supported hardware and software features in the Nortel Secure Network Access Switch Software Release 2.0, fixes to previously-known issues, and any remaining known issues.

ATTENTION
The new features and issues resolved up to Release 1.6.1.4 are supported in Release 2.0. For more information on these features, see New software features in this release section in Release 1.6.1.X section in Release Notes for Software Release 1.6.1.X (NN47230-400).

Navigation

New features in Release 2.0 Software

Microsoft NAP Interoperability

Microsoft Network Access Protection (NAP), introduced with Windows Vista and Windows Server is a new set of operating system components that provides a platform for protected access to private networks. The NAP platform provides an integrated way of detecting the health state of a network client, which attempts to connect to a network and restricts the access of the network client until the policy requirements for connecting to the network are met.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

RADIUS server/proxy

The Nortel SNAS is a full featured RADIUS server. The RADIUS server can be used to authenticate users through PAP/CHAP or work in more complex 802.1x environments supporting EAP-MD5, TLS, PEAP, and TTLS.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

802.1x functionaltiy

Integration of SNAS RADIUS server and Nortel Health Agent with MS Windows 802.1x EAP supplicant for user authentication and health assessment.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

Nortel SNAS Scheduler

The SNAS scheduler allows customers to run automated system maintenance tasks like system and configuration backup at scheduled intervals.

The SNAS Scheduler performs scheduled execution of tasks such as upgrade, self-test, start/stop trace, reboot, ptcfg, and export.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

SSCP-Lite

Switch to SNAS Communication Protocol (SSCP-Lite) is a SNAS enforcement protocol that uses Simple Network Management Protocol (SNMP) to restrict a users network access using dynamically provisioned VLAN's based on users credentials and device health assessment. SSCP-Lite supports Nortel ES 325, 425, 450, 460, BPS, 470, and ERS 2500, 4500, 5500, 8300, and 8600. In addition, SSCP-Lite supports Cisco 2900, 3500, and 3700 series Ethernet switches plus HP 2600 and 3400 series switches.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

Nortel SNAS TPS integration

TPS is the Nortel Threat Protection System. An enhanced version of the remediation API that supports blacklisting of users. Blacklisting allows organizations to configure a time-out value where the specified user/device is not allowed to connect to the network.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

VLAN Transition with MAC Address Database

Using the SNAS MAC database a VLAN can be specified for a MAC address. Ethernet switches that support VLAN transition with SNAS MAC database will now transition the device into the specified VLAN. This feature is especially useful for devices that do not support 802.1x or have an interactive console like printers. Currently ERS 4500 supports this feature.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

Lumension PatchLink integration

Nortel SNAS is integrated with the Lumension PatchLink security patch management system, which allows to proactively enforce user and device compliance by ensuring that devices are properly patched and up-to-date.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

Portal Enhancements

The portal enhancement supports the Self service portal and Internationalization or localization feature:

Self Service Portal

The SNAS self-service portal provides a web-based ‘help desk’ for users to collect information about their network connection, compliance, and user status.
Guest registration tool is also available for admin users.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

Internalization or Localization

The SNAS captive portal can be customized using localized language files.

The Nortel SNAS supports multiple languages. Language packs can be downloaded and installed for use in the Nortel SNAS portal (http://www.nortel.com/support).

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

Nortel Health Agent

The Nortel Health Agent supports the following features:

- “Admin Tool Enhancements” (page 17)
- “Windows 802.1x Supplicant” (page 17)

Following table explains the Nortel Health Agent Compatibility Matrix.

Nortel Health Agent Compatibility Matrix					
		Nortel Health Agent software Release			
		3.5	4.0	4.5	5.0
SNAS Software Release	1.0.X	"Portal based Java applet only" support			
	1.5.X	"Portal based Java applet only" support			
	1.6.1.X	F	F	F	NC
	2.0.X	NS	NS	F	F
Key F = Fully Functional NC = Not Compatible NS = Not Supported but should work					

Admin Tool Enhancements

The Nortel Health Agent administrative applet allows security policies to be configured with predefined applications and a new intuitive policy builder.

Windows 802.1x Supplicant

The Nortel Health Agent integrates with the Microsoft NAP Agent providing customers with a robust EAP supplicant for Windows Vista and XP SP3 Operating Systems.

Multi-OS applet support

Multi-OS support allows the Nortel Health Agent to identify Linux and MAC OS X Operating Systems, collect system and user information and perform a VLAN transition with IP address renew script after user authentication. Support for a system health assessment is planned for a later software release for these operating systems.

The following OS are currently supported for MAC and Linux:

- RedHat Enterprise Linux 4
- Fedora Core 7
- Mac OS X Server v10.4 Tiger

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500), Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100), Nortel Secure Network Access Switch Configuration

— Using the Nortel Health System Agent (NN47230-501), and Nortel Secure Network Access Switch Nortel Health Agent Administration (NN47230-601).

On-the-fly SRS policy change

When the Nortel Health Editor is used to modify a security policy, the new health policy will be distributed, by the Nortel SNAS, to the Nortel Health Agent during the next health agent heartbeat message.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

VMWare support

VMware (Virtual Machine) supports environments with which you can run a native operating system in addition to running a VMware instance on the host operating system (OS). The host operating system and guest operating system (GuestOS) can go through either L2 or L3 authentication and authorization.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

Additional enhancements

Software enhancements in SNAS includes location based security, MAC authentication, and LDAP enhancements.

Additional enhancements navigation

- “Location based security” (page 18)
- “MAC authentication” (page 19)
- “LDAP enhancements” (page 19)

Location based security

Group configuration of SNAS controlled switches is done on the basis of identity/location networking. Network access is granted or denied based on the identity and the location of the user. To grant and deny the network access for the particular IP address and unit/port, specify the IP address and unit/port of a switch.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

MAC authentication

Media Access Control (MAC) supports entries that contain the wildcard (*) search character. The wildcard character is used to specify a MAC search string.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

LDAP enhancements

Following are the enhanced features for back-end Lightweight Directory Access Protocol (LDAP) authentication support:

- Native groups

  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

  Allows to configure the SNAS to extract the first part of a returned Distinguished Name (DN) as the group name.

- Advanced LDAP menu

  It is used to configure the desired attribute/value when searching 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.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500) and Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100).

New Hardware

In Release 2.0, Nortel Secure Network Access Switch 4070 is the new hardware.

If you experience an option failure (DOA) for any of the following options:

- EB1639185E5 (IBM PN: 40K1146) 146 GB, 15K rpm, 3.5” Hot-swap SAS Hard Disk Drive
- EB1639186E5 (IBM PN: 40K1905) xSeries 835W Redundant Power Option (110- 127v)
- EB1639188E5 (IBM PN: 42C1750) Intel PRO/ 1000 PF Server Adapter – Supports Intel I/O Acceleration Technology for System x IOAT Capable Servers

In this case you must provide the serial number of the system to the Nortel in which the option is installed to get a replacement from IBM under the warranty.

If you need to return a system (Secure Network Access Switch 4070) and has purchased and installed any of the above options, you must remove those options before returning the system to Nortel for replacement or repair.

For more information, see Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500), Nortel Secure Network Access Switch Configuration — Using the Command Line Interface (NN47230-100), and Nortel Secure Network Access Installation — Switch 4070 (NN47230-302).

File names for this release

This section describes the Nortel Secure Network Access Switch Software Release 2.0 software files.

The updated software images for Nortel Secure Network Access Switch 4050 and 4070 can be downloaded from the Nortel Service Portal. The SNA switches are shipped with SNA image installed.

For upgrades, download the complete upgrade package. For more information on upgrade procedures, see “Upgrading to Nortel SNAS 2.0” (page 26).

Table 1
Nortel SNAS software images

Product	Image type	File name
SNAS	Boot	NSNAS-2.0.1-boot.img
	Upgrade Package	NSNAS-2.0.1-upgrade_complete.pkg

Table 1
Nortel SNAS software images (cont'd.)

Product	Image type	File name
Nortel Health System Agent Release 5.0	with bundled JRE	NhaVm_5_0.exe
	without JRE	NhaNoVm_5_0.exe
	Customizable MSI package with bundled JRE	NhaCstVm_5_0.msi
	Customizable MSI package without bundled JRE	NhaCstNoVm_5_0.msi

ATTENTION
SREM Software is not supported with Release 2.0 and later software.

Implementing the Nortel SNA solution

Implement the Nortel SNAS 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 upgrade

While upgrading from 1.5.1 or 1.6.1.X to 2.0.1, the list of servers under the configuration of authentication server type Radius is reversed. List under /cfg/domain #/aaa/auth #/radius/servers will be reversed. While downgrading from 2.0.1 to 1.6.1.X to 1.5.1, the list of servers are erased under /cfg/domain #/aaa/auth #/radius/servers.

Before you start, upgrade a Nortel SNAS to the latest software, following instructions listed in the Nortel Secure Network Access Switch Upgrades — Software Release 2.0 (NN47230-401).

Guidelines for Nortel Health system agent

The following are the guidelines that needs to be followed for Nortel Health system agent.

- Microsoft Remote Desktop connections and Nortel Health Agent user session behavior

  While Nortel Health Agent has an active user session with an SNAS, 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 SNAS 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 Nortel Health Agent 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 Nortel Health Agent user session gets disconnected when the Remote Desktop session is established. If Nortel Health Agent 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).

ATTENTION
Windows XP Professional, and Windows Vista are not supported.

- Fast User Switching

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

Performance and scaling capabilities

The following table describes the performance and scaling capabilities of Nortel SNAS 4050 and 4070 switch.

No.	For 4050	For 4070
1.	A single Nortel SNAS 4050 supports 2500 concurrent user connections. When clustered for high availability and load balancing, the Nortel SNAS supports 10,000 concurrent user connections in a cluster.	A single Nortel SNAS 4070 supports 5000 concurrent user connections. When clustered for high availability and load balancing, the Nortel SNAS supports 20,000 concurrent user connections in a cluster.
2.	A single cluster supports a maximum of 4 Nortel SNAS 4050 devices.	A single cluster supports a maximum of 4 Nortel SNAS 4070 devices.

No.	For 4050	For 4070
3.	Nortel SNAS supports up to 256 policy enforcement points. It can include a combination of SSCP Enabled PEPs, SSCP-Lite PEPs and 802.1x or Radius Enabled PEPs.	Nortel SNAS supports up to 256 policy enforcement points. It can include a combination of SSCP Enabled PEPs, SSCP-Lite PEPs and 802.1x or Radius Enabled PEPs

ATTENTION
The performance of a hybrid configuration of 4050 and 4070 SNAS will vary from a pure configuration of only 4070's.

Supported hardware and software

The Nortel SNAS solution performs authentication and posture assessment for end points connected to access devices typically deployed at the network edge. Nortel SNAS SSCP technology is incorporated into ERS 4500, 5500, ERS 8300, and 8600 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 non-Nortel Ethernet Switching platforms. The Nortel SNAS secures both PC and Voice over IP (VoIP) phone clients in the network.

Supported software and hardware navigation

- "Switch hardware and software" (page 23)
- "PC client hardware and software" (page 24)
- "VoIP client phone models, call servers, and firmware" (page 25)
- "Back-end services" (page 25)
- "Threshold specifications" (page 26)

Switch hardware and software

The following table lists the supported network hardware and software.

Table 2
Supported network hardware and software

Component	Specifications
Core router	Nortel Ethernet Routing Switch 8600 or any make or model router of similar specifications

Table 2
Supported network hardware and software (cont'd.)

Component	Specifications
Nortel SNAS 4070 and 4050	Nortel Secure Network Access Switch Software Release 2.0 Nortel Health System agent Release 5.0 **ATTENTION** The SNAS 4070 needs a minimum version of Release 2.0 Software.
Edge switch (network access device) options:	
• Nortel Ethernet Routing Switch 5510, 5520, 5530 • Nortel Ethernet Routing Switch 8300 • ERS 4500 • Nortel Ethernet Routing Switch 8600	Nortel Ethernet Routing Switch 5500 Series, Software Release 5.1 or later Nortel Ethernet Routing Switch 8300 Series, Software Release 4.1 Nortel Ethernet Routing Switch 4500 Series, Software Release 5.1 or later Java Device Manager (JDM) 6.0.2.0 or later Nortel Ethernet Routing Switch 8600, Software Release 5.0

PC client hardware and software

The following table lists the supported PC client hardware and software.

Table 3
Supported PC client hardware and software

Client hardware and software	Versions
PC clients	Microsoft Windows 2000 Professional SP4 Windows 2003 Microsoft Windows XP SP2 Windows Vista MAC OS Linux OS Non-Interactive Devices

Table 3
Supported PC client hardware and software (cont'd.)

Client hardware and software	Versions
Browser options	Internet Explorer 6.x and later Mozilla Firefox 2.x and later Netscape Navigator 8.0.x Safari 2.0 and later
Java Runtime Environment (JRE)	JRE 1.5.0.10+ (JRE 1.6 recommended)

VoIP client phone models, call servers, and firmware

The following table lists the supported VoIP phone models, call servers, and firmware.

Table 4
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 2001 model NTDU90	F/W 0604DBP	F/W 0604DBP	F/W 0604DBP
IP Phone 2002 model NTDU76	F/W 0603B60	F/W 0603B60	F/W 0603B60
IP Phone 2002 model NTDU91	F/W 0604DBL min version F/W 0603D65	F/W 0604DBL min version F/W 0603D65	F/W 0604DBL min version F/W 0603D65
IP Phone 2004 model NTDU92	F/W 0604DBL min version F/W 0604D65	F/W 0604DBL min version F/W 0604D65	F/W 0604DBL min version F/W 0604D65
IP Phone 2007 model NTDU96	F/W 0621C4P F/W 0621C23	F/W 0621C4P F/W 0621C23	F/W 0621C4P F/W 0621C23
IP Phone 1140 model NTYS05	F/W 0625C3C	F/W 0625C3C	F/W 0625C3C
IP Phone 1120 model NTYS03	F/W 0624C3C	F/W 0624C3C	F/W 0624C3C
IP Phone 1110 model NTYS02	F/W 0623C3C	F/W 0623C3C	F/W 0623C3C

Back-end services

The following table lists the authentication and other back-end services specifications.

Table 5
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, Windows 2003, Linux Fedora
DNS	Microsoft Windows 2000 Server SP4, Windows 2003, Linux Fedora

Threshold specifications

The following table lists the upper limit thresholds for hardware and network security software in the Nortel SNAS.

Table 6
Hardware and software upper limit thresholds

Item	For 4050	For 4070
Nortel SNAS devices in a cluster	4	4
Network access devices for each Nortel SNAS (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)	256	256
Users for each Nortel SNAS *By default, each Nortel SNAS ships with 200 user licenses. Upgrade license packs of 100, 250, 500, 1000, 2000, and 5000 additional licenses are available.	2500*	5000
Users for each Nortel SNAS cluster	10,000	20,000
Red VLANS for each network access device	1	1

Upgrading to Nortel SNAS 2.0

Nortel Secure Network Access Switch running on prior versions of SNAS software can be upgraded to SNAS Release 2.0.

The allowed upgrade paths are 1.5.1 --> 2.0.1 and 1.6.1.x --> 2.0.1.

With the help of Nortel Health Policy Administrator 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 2.0.1 the existing rules gets applied for all the Operating Systems. If the admin is creating a SRS rule, specific to Operating System in Release 2.0.1 and performs the downgrade followed by upgrade i.e. Release 2.0.1 -> 1.5.1 -> 2.0.1, all the SRS rules are applied to Operating Systems.

On upgrade recheck/heart beat interval value will be updated to next valid value. The following table explains all possible combinations and their modification on upgrade.

1.6.1.4 version		**-->**	**2.0 version**		
HB	**Recheck**	**-->**	**HB**	**Recheck**	**Modification Details**
60	60	-->	60	61	(Recheck value incriminated by one)
100	101	-->	100	101	(No change)
86400	86400	-->	86399	86400	(Case of maximum value. HB decremented by one)

For more information, see the Nortel Secure Network Access Switch Configuration — Using the BBI (NN47230-500), and Nortel Secure Network Access Switch Upgrades — Software Release 2.0 (NN47230-401).

Resolved issues

This section details all issues resolved for Release 2.0.

ATTENTION
All resolved issues up to Release 1.6.1.4 are also included in Release 2.0. For more information, see Resolved Issues section in Release Notes for Software Release 1.6.1.X.

Navigation

Nortel Health Agent resolved issues

Table 7
Nortel Health Agent

Change Request Number	Description
Q01348979	In some cases, the Ctrl-X Nortel Health Agent hotkey may not function. To workaround this issue, close Nortel Health Agent using the Close button in the upper right, or close from the file menu.
Q01411833	When closing a Nortel Health Agent applet that is running in a tab of the Firefox web browser, Nortel Health Agent 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.
Q01437701	When kicking out a NHA PC login session, if the logout button is clicked, the user may not be able to log back in immediately.
Q01442679	A NHA PC may be logged in, but redirected to the login page when trying to access the portal home page.

Table 7
Nortel Health Agent (cont'd.)

Change Request Number	Description
Q01844941	NSNA 4050 1.6.1.2 DHCP Discovery is ignored by the NSNA
Q01753630	Desktop NHA client time-out issue
Q01814752	NSNA 4050 1.6.1.2 Need RADIUS account file log does not give all information
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."
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.
Q01427662	Clients using MAC OSX Safari browser may encounter pop up Certificate acceptance messages. Workaround: Accept the messages
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.
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)
Q01445327	When update a Global option, DHCP subnets still provide old values for clients. Disable/re-enable subnets required to make the change affected.

Table 7
Nortel Health Agent (cont'd.)

Change Request Number	Description
Q01445148	Yahoo Instant Messenger may lose its connection after logging into the SNAS. Workaround: Put Yahoo Instant Messenger in the exclude list.
Q01454814	When exporting a certificate using the wrong username or password via scp/sftp, an error message displayed with no information.

Browser-Based Interface resolved issues

Table 8
Browser-Based Interface

Change Request Number	Description
Q01736421 and Q01736701-01	NSNA unable to forward admin rights through BBI.
Q01774038	NSNA 4050 1.6/Single Sign On Logout Failure - syscredentials /BBI issue
Q01785368	Request system previous password to be input after reset system credentials
Q01746547 and Q01746547-01	Missing /cfg/domain 1/aaa/auth x/ldap/enashortgr support - CLI catchup

Known issues

Use the information in this section to learn more about known issues and outstanding issues. Where appropriate, use the workaround provided for the known issues and issues.

Navigation

Known issues

The following section lists known issues in Nortel Secure Network Access Switch Release 2.0. Some known issues are targeted for resolution in future releases.

Known issues navigation

Feature known issues

Table 9
Feature

Change Request Number	Description
Q01780147	Redirecting to the captured URL after successful login on the portal using the Browser doesn't work for clients connected to non-SSCP capable switches.
Q01789133	Microsoft XP supplicant hangs when using McAfee firewall with autoremediation.
Q01866746	With Cisco EtherChannel setup, PCs work fine and only phones are not supported.

Table 9
Feature (cont'd.)

Change Request Number	Description
Q01728687	For SNAS cluster which is already joined to Windows Domain for performing NTLM authentication, a new node that is becoming a part of the cluster, must be joined to Windows Domain manually.
Q01721667	SNAS host IP must be used if it is acting as a client for remote RADIUS server.
Q01866111	Access to the network is not allowed for devices connected to SSCP-Lite switches without using any flavor of Nortel Health Agent.
Q01744832	The tagging features are not available on the ES 450 so you cannot put a particular port in multiple vlans. Switches does not allow such configuration. To support both PC and a phone, you need to place the port in PC as well as VOIP vlan membership. Switches ES 460, 470 works perfectly.
Q01777190	username@domain.com syntax does not work with PEAP and TTLS-MSCAHPv2. This behavior is only observed with Mac OS X Tiger supplicant when doing MS-CHAPv2 based authentication. Windows XP SP2, Windows Vista, and Funk Odyssey supplicants works fine. The Mac OS X Tiger Supplicant performs MS-CHAPv2 NT response calculation incorrectly when the user name is "user@domain.com". Workaround: Users on Mac OS must use "DOMAIN\user" format to perform one of the following authentication methods: EAP-PEAPv0/EAP-MS-CHAPv2 EAP-TTLS/EAP-MS-CHAPv2 EAP-TTLS/MS-CHAPv2
Q01827522	Enforcement on Cisco switches does not work using SNMPv1 profile for SSCP-Lite.
Q01833077	When new SNAS joins the cluster, switches do not get redistributed to new SNAS. Workaround: Use the /cfg/sys/adm/red command to redistribute the switch manually.
Q01835835	SNAS supports only two devices (phone and a PC) per port.

Table 9
Feature (cont'd.)

Change Request Number	Description
Q01810395	Due to DNS cache related issue, redirecting to the captured URL after successful login on the portal using the Browser does not work in Mozilla and Firefox. Workaround: You can configure firefox (internal params) using the user set params network.dnsCacheExpiration and network.dnsCacheEntries to zero. Open about:config url in firefox, add new params with above specified name and value.
Q01769580	NHA Applet failed to load required Modules in Windows 2000. Workaround: Runtime libraries can be downloaded and installed from Microsoft site (http://www.microsoft.com/downloads/details.aspx?FamilyID=200B2FD9-AE1A-4A14-984D-389C36F85647&displayinglang=en).
Q01873750	NAP_802.1x: SNAS does not show correct port number when switches are in stack. The port number showed in sessions can be represented in a single digit format or unit/port format. With 802.1x the port number is determined from NAS-Port RADIUS attribute. Considering that different switches use different numbering for the units/ports, but they all report the port in NAS-Port attribute, no attempt to map it to UNIT/PORT format will be made to accommodate a wider range of 802.1x authenticators.
Q01721697	Load balancing of request for SNAS Radius server is not supported as Radius server listens on Management IP address (MIP) and MIP can be owned by only one node at a time.
Q01794780	SSCPLite should not accept 0 as Unit or Port input. SSCPLite treats ports as a strings (if Name's) not numbers for some switches. Switch management does not work if a wrong port number is entered.
Q01841647	Sometimes session information for a user/device using 802.1X will not be deleted if the device or user disconnects from the network. It will take either session-ttl interval to cleanup the session.

Table 9
Feature (cont'd.)

Change Request Number	Description
Q01727887	With SNAS acting as a Radius server, you cannot authenticate a user@domain.com against NTLM domain. Use DOMAIN\user or domain\user. You can authenticate user@domain.com if domain.com realm is of type LDAP, LOCAL or RADIUS.
Q01800752	Starttrace command from CLI does not write the trace logs into files if TFTP is used as the output mode. This is because of the TFTP protocol limitation. TFTP protocol assumes file transfer is over and it will close the file If the payload is less than 512 bytes. Trace logging to TFTP server can only be done this way. For each trace message there will be a separate file. It will generate a huge number of files if enable trace for a long period to TFTP server.
Q01777596	Once a user is blacklisted further failed attempts will not be count. Login fails even if correct credential submitted during blacklisted period. This is same with blacklisted host, i.e It does not count failed login attempts to a 'user account' from a blacklisted host. For example: If the user_attempts = 3/15m the user will be blacklisted after 3 attempts. Due to the limitation of software the third attempt recorded only when the user enters username fourth time. But it ensure that user will not be allowed to login even if he give correct credentials fourth time.
Q01754197	For installable client, even if the certificate is accepted with 'OK' not "ALWAYS", The certificate is valid with installable client till the PC gets rebooted.
Q01777631	Blacklisting does not work when trying to login with wrong credentials with interval between each attempt (but with in configured time). Workaround: Try to login with wrong credentials continuously.
Q01835093	For 802.1x authenticated sessions the port is determined from the NAS-Port RADIUS attribute sent in Access-Request from the authenticator. Since the port numbering is implemented differently on a wide variety of supported authenticators, no attempt to translate the reported NAS-Port into Unit/Port will be made.
Q01903735	SSCPLite-cisco: Reboot switch, most of ports move to green unexpectedly.

Table 9
Feature (cont'd.)

Change Request Number	Description
Q01903712	Not able to connect to cisco sscplite switch using ssh login type.
Q01903727	After software reboot, direct sessions drop and behind phone sessions stay intact.
Q01822882	Sessions got logout when failover happens.
Q01400674	The error reported by NHA, ""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	A subnet cannot be enabled unless known settings for SNAS DHCP filter mode and unknown stdopts (standard options) 51 for unknown settings are set.
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.
Q01434429	If the Action to take on NO admin rights is set to "no access", the non-admin user/device will not be give access irrespective of the enforcement type set for the group.
Q01446249	The Opera web browser cannot run the NHA applet, so the user cannot login. This is a limitation of the Opera web browser. Workaround: Use Internet Explorer or Mozilla as a web browser.
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. Workaround: Perform the commands "ipconfig/ release" and "ipconfig /renew".

Table 9
Feature (cont'd.)

Change Request Number	Description
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.
Q01418068	In a cluster, performing the /boot/delete command to delete a SNAS which handle MIP and control a switch, NHA 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.
Q01415269	To join a Multi-trunking NSNAS into a cluster unplug all unused ports when running the join wizard.
Q01427585	The Admin Rights feature may reveal the admin password to a normal user.
Q01439061	RADIUS Authentication cannot fallback to a local user.
Q01440956	Hub support cannot resist against DHCP attacks.
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 MAC database.
Q01445279	When saving trace output to an external TFTP server, the SNAS may only log the first NHA PC login.
Q01449080	NHA icon may not display properly when combined with hyperlinks.
Q01664804	NHA does not work properly after stop/start services.
Q01684744	Enhance to have user session back after switched user back to a logged user.

Nortel Health Agent known issues

Table 10
Nortel Health Agent

Change Request Number	Description
Q01755739	Real time protection or Trigger live update does not work for some of the pre-defined SRS rules.
Q01906230	Sometimes in single-sign-on environment with Nortel Health Agent and SSCP-Lite mode of enforcement, with very fast logout/logins, the machines remains with system access even though the user is logged in.

Nortel Secure Network Access Switch

Release Notes — Software Release 2.0

Printed in Canada, the United States of America, and India
Release: 2.0
Publication: NN47230-400
Document revision: 03.04
Document release date: 24 March 2009

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

www.nortel.com
LEGAL NOTICE