NØRTEL

Nortel Secure Network Access Switch

Release Notes for Software Release 1.5

NN47230-400 (320850-C)

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 User Guide for the CLI (NN47230-100)* for more information.

Nortel Networks Inc. 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 1.5

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 1.5.1 and Security & Routing Element Manager (SREM) 1.2.1.0_050.

For a list of related publications, see "Related publications" (page 24). 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 24).

These release notes cover the following topics:

Topic
"Overview" (page 8)
"New software features in this release" (page 8)
"Supported hardware and software" (page 9)
"Implementing the Nortel SNA solution" (page 13)
"Known limitations and considerations in this release" (page 15)
"Documentation additions and corrections" (page 20)
"Reading path" (page 24)
"Hard-copy technical manuals" (page 24)
"How to get help" (page 25)

The information in these release notes supersedes applicable information in other 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) is a GUI tool you can use to configure and manage the Nortel SNA switch and to monitor solution statistics.

New software features in this release

- The Secure Network Access Solution can scale to 8000 users in a single Secure Network Access Switch Cluster. A Secure Network Access Switch Cluster can contain up to 4 Secure Network Access Switches each managing up to 25 access devices.

- Support for Hubs

  Nortel Secure Network Access Solution now supports environments that have implemented hubs.

  Please see Nortel SNAS 4050 User Guide for the CLI - ***Configuring the domain - Configuring local DHCP services***

- Support for non-SSCP platforms

  Nortel Secure Network Access Solution no longer requires the network access device to support Switch-SNAS Communication Protocol (SSCP). The Nortel SNAS 4050 can now be configured to operate with all Nortel Ethernet switches and Ethernet routers, and with non-Nortel switches.

Please see Nortel SNAS 4050 User Guide for the CLI - ***Configuring the domain - Configuring local DHCP services***

- Support for WLAN 2300 series controllers

  The Nortel SNAS 4050 can interoperate with the WLAN Controllers providing both authentication and device health assessment for WLAN mobile users.

  Please see Nortel SNAS 4050 User Guide for the CLI - ***Configuring the domain - Configuring local DHCP services***

- Tunnel Guard Run-Once Agent

  The Nortel Tunnel Guard technology now includes a run-once mode of operation. After an endpoint has been successfully scanned and transitioned to the GREEN state - the Nortel Tunnel Guard agent can be shutdown. The endpoint will be trusted for the duration of the session or until the endpoint is disconnected from the network.

  Please see Nortel SNAS 4050 User Guide for the CLI - ***Configuring groups and profiles*** and ***Configuring Authentication***

- Support for MAC OS, Linux OS and Non-Interactive Devices

  Nortel Secure Network Access Solution now supports authentication of machines running Mac OS X, Linux, and passive devices such as printers, video cameras and gaming consoles.

  Please see Nortel SNAS 4050 User Guide for the CLI - ***Configuring groups and profiles - Configuring groups***

- MAC Security Policy Services

  The Nortel SNAS 4050 now supports a MAC address database to provide authentication based on the MAC address of the end point.

  Please see Nortel SNAS 4050 User Guide for the CLI - ***Configuring groups and profiles*** and ***Configuring authentication***

- Flexible Deployment Options

  An enforcement type that requires filters only has been added to release 1.5. Enforcement types supported now include VLAN + FILTER, and FILTER only.

  Please see Nortel SNAS 4050 User Guide for the CLI - ***Overview*** and ***Configuring groups and profiles***

Supported hardware and software

The Nortel SNA solution 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, ERS 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

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 1.5.1 Security & Routing Element Manager (SREM) 1.2.1.0_050
Edge switch (network access device) options:	
• Nortel Ethernet Routing Switch 5510, 5520, 5530	Nortel Ethernet Routing Switch 5500 Series, Software Release 5.0.2
• Nortel Ethernet Routing Switch 8300	Nortel Ethernet Routing Switch 8300 Series, Software Release 3.0 (Supports NSNA 1.1) Java Device Manager (JDM) 6.0.2.0 or later

Client hardware and software

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 MAC OS Linux OS Non-Interactive Devices
Browser options	Internet Explorer 6.x Mozilla Firefox 1.0.7 Netscape Navigator 8.0.x
Java Runtime Environment (JRE)	Sun JRE 1.5.0_04 (required for all browsers)

"Supported VoIP client phone models, call servers, and firmware versions" (page 11) 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

Back-end services

lists authentication and other back-end services specifications.

Authentication software and back-end services

Software	Version
LDAP authentication	Microsoft Windows 2000 SP4, 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)
DHCP	NSNAS, Microsoft Windows 2000 Server SP4, Linux Fedora
DNS	Microsoft Windows 2000 Server SP4, Linux Fedora

Delivered software images

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

Image	Image
Boot Image	NSNAS-1.5.1-boot.img
Package	NSNAS-1.5.1-upgrade_complete.pkg
SREM	srem_1.2.1.0_050.exe for Windows

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

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, 200, and 500 additional licenses are available.	2500*
Users for each Nortel SNAS 4050 cluster	8000
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 8000 concurrent user connections in a cluster. A single cluster supports a maximum of 4 Nortel SNAS 4050 devices.

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 User Guide for the CLI (NN47230-100)* or *Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*.

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 User Guide for the CLI (NN47230-100)* or the *Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*.
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 User Guide for the CLI (NN47230-100)* or the *Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*. *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 User Guide for the CLI (NN47230-100)* or the *Nortel Secure Network Access Switch 4050 User Guide for the SREM (NN47230-101)*.

—End—

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.
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.

Change Request Number	Issue
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 will be 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 PortDown 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.

Change Request Number	Issue
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.
Q01387768	The "Add MAC" option for phone devices is redundant and will be removed.
Q01390392	The SNAS may not delete an unused phone session.
Q01413600	May not show a proper error when importing or exporting incorrect info.
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.
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.
Q01441788	A improper message may appear when a user logs into a group which has no extended profile.
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.
Q01444510	There may be a hostname mismatch when obtaining a certificate from the portal.
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 extrernal TFTP server, the SNAS may only log the first TG PG login.

Change Request Number	Issue
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.
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.
Q01454814	When exporting a certificate using the wrong username or password via scp/sftp, an error message displayed with no information.
Q01463622	When using pasted configuration information an error may occur.

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.

Change Request Number	Issue
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.
Q01346043	Software Definition is deleted after user hit Esc key to cancel the deletion. Use the Cancel button instead.
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.

Documentation additions and corrections

The following information supplements or replaces existing material in the Nortel SNA documentation suite in order to accommodate new features, CR fixes, and documentation corrections. The changes will be incorporated in the next release of the documentation.

Changes in SREM documentation

The following sections detail changes to be made in SREM documentation for the NSNAS 1.5 standard release.

Managing real-time charting of statistics

SREM for NSNAS 1.5 introduces real-time charting of CPU and memory utilization performance statistics. Performance statistics are available in real-time via GUI window, or as a CSV (Comma Separated Value). To view real-time charting of performance statistics, use the following steps:

Step	Action
1	Open the SREM menu tree to **Device IP > Information**. The *Controller List* tab appears.
2	Click the **Charts** tab. The *Online charts* screen appears.
3	In the "*Active SNAS devices in cluster*" list, select the device(s) you want to monitor.
4	Click the **Start** button. The *Charts* user interface appears.
5	To stop monitoring click the **Stop** button in the *Charts* user interface. Click the **Close** button to close the interface.

—End—

Managing DHCP support

NSNAS 1.5 introduces DHCP support. The Nortel SNAS will act as a DHCP server for devices connected via hub to NSNA controlled switch ports. SNAS can also act as a DHCP server in a normal mode or to support captive portal and FILTER-ONLY mode.

To add a DHCP subnet, perform the following steps:

Step	Action
1	Open the SREM menu tree to **Device IP > Secure Access Domain > Domain > DHCP > Subnet**. The *Subnet* screen displays.
2	Click the **Add** button. The *Add Subnet* dialog box displays.
3	In the fields provided, enter the necessary information.
4	Click **Apply**.

—End—

To manage DHCP standard options, perform the followings steps:

Step	Action
1	Open the SREM menu tree to **Device IP > Secure Access Domain > Domain > DHCP > Standard Options**. The *Standard Options* screen displays.
2	To add an option, click the **Add** button, select an option ID and click **Apply**.
3	To delete an option, select it from the table and click **Delete**. Answer *Yes* to the prompt.

—End—

To manage DHCP vendor options, perform the following steps:

Step	Action
1	Open the SREM menu tree to **Device IP > Secure Access Domain > Domain > DHCP > Vendor Options**. The *Vendor Options* screen displays.
2	To add an option, click the **Add** button. The *Add Vendor option* dialog box appears.
3	In the fields provided specify the necessary information and click **Apply**.
4	To delete an option, select it from the table and click **Delete**. Answer *Yes* to the prompt.

—End—

Managing MAC Security support
The Secure Network Access Switch is capable of authenticating network access request using MAC address security. The Secure Network Access Switch maintains a list of MAC addresses for trusted and blacklisted and isolated devices and processes MAC address according to a policy. MAC addresses are maintained on the SNAS in a database allowing for flexible management. MAC security policy services allows network administrators to map a MAC address to a VLAN or filter allowing network access requests to perform DHCP, associate a MAC address to a dedicated IP address for static

IP address configuration. In addition, network administrators can specify the requirement for network access requests that are processed using the MAC security policy services to perform additional captive portal process for:

- Authentication

- End point compliance inspection using Tunnel Guard

To configure MAC Security, perform the following steps:

Step	Action
1	Open the SREM menu tree to **Device IP > Secure Access Domain > Domain > AAA > Groups > *groupname*** The **Configuration** screen is displayed.
2	Click the **MAC** tab. The MAC screen appears.
3	From the **MAC Trustlevel** dropdown, select the MAC trust level. Available options are ***bypass*** and ***none***.
4	From the **Display of MAC Registration** dropdown, select the state of display. Available options are ***true*** (display) and ***false*** (don't display).
5	From the **Set Tunnelguard mode** dropdown, select the Tunnelguard mode. Available options are ***continuous*** (always on), ***runonce*** (run this session only), and ***never*** (Tunnelguard not used).

—End—

Managing the MAC database   To manage MAC address entries, choose one of the following procedures:

Viewing and managing MAC entries   To view or add MAC entries, perform the following steps:

Step	Action
1	Open the SREM menu tree to **Device IP > Secure Access Domain > Domain > AAA > Authentication > *[authentication type]* MAC database**. The *Basic* screen appears. From this screen you can view information about current entries in the MAC database.
2	To add an entry, click the **Add** button. The *MAC Database* screen appears. In the fields provided, enter the necessary information.

3   To delete an entry, select the entry you wish to delete in the MAC
     database table and click **Delete**.

4   To clear the MAC database, click the **Clear MAC database** button
     and answer *Yes* to the prompt.

—End—

Reading path

This section lists documentation for the Nortel SNA solution, Nortel Secure
Network Access Switch Software Release 1.5. For information about
finding and accessing up-to-date documentation, see "Hard-copy technical
manuals" (page 24).

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 User Guide for the CLI
  (NN47230-100)*

- *Installing and Using the Security & Routing Element Manager (SREM)
  (NN47230-301)*

- *Release Notes for Enterprise Switch Manager (ESM), Software Release
  5.2 (209960-H)*

- *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software
  Release 5.0.2 (NN47200-400)*

- *Release Notes for the Ethernet Routing Switch 8300, Software Release
  2.2.8.1 (316811-G)*

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.com URL 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.