Part No. 320850-B
February 2006

4655 Great America Parkway
Santa Clara, CA 95054

Release Notes for Nortel Secure Network Access Solution Release 1.1

NORTEL

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* (320818-A) 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

Introduction

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 1.1.1 and Security & Routing Element Manager (SREM) 1.2.1.0.

For a list of related publications, see page 32. 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" on page 32.

These release notes cover the following topics:

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, 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 solution and to monitor solution statistics.

New software features in this release

Nortel Secure Network Access Switch Software Release 1.1.1 and SREM 1.2.1.0 provide the following new features or feature improvements:

- The Nortel TunnelGuard applet now has the ability to execute a Windows logon script. For more information, see "Using the TunnelGuard applet to run a script at logon" on page 17.

- Additional logging options. The Logs Menu (**`/info/logs`** command) now includes commands to log port, Red VLAN, switch, and client activity. For more information about the new commands, see "Additional logging options" on page 22.
- Recursive lookup for Active Directory

  A new command on the **Active Directory Settings** menu (**`/cfg/domain #/aaa/auth #/ldap/activedire/recursivem`**) specifies whether to resolve nested group names when authenticating using LDAP. For more information, see "Recursive lookup for Active Directory" on page 24.

Supported hardware and software

The Nortel SNA solution utilizes a network core router, the Nortel SNAS 4050, and Nortel SNA-enabled ports on one or more edge switches functioning as network access devices. The Nortel SNA solution secures both PC and Voice over IP (VoIP) phone clients in the network.

Switch hardware and software

Table 1 lists supported network hardware and software.

Table 1 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 1.1.1 Security & Routing Element Manager (SREM) 1.2.1.0
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 4.3.1 Nortel Ethernet Routing Switch 8300, Software Release 2.2.8.1 Java Device Manager (JDM) 5.9.5.0 or later

Client hardware and software

Table 2 lists supported PC client hardware and software.

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

Table 2 Supported PC client hardware and software

Client hardware and software	Versions
PC clients	Microsoft Windows 2000 Professional SP4 Microsoft Windows XP SP2
Browser options	Internet Explorer 6.x Mozilla Firefox 1.0.7 or later Netscape Navigator 8.0.x
Java Runtime Environment (JRE)	Sun JRE 1.5.0_04 or later (required for all browsers)

Table 3 lists supported VoIP phone models, call servers, and firmware.

Table 3 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 Phase TBD)	F/W 0621C23	F/W 0621C23	F/W 0621C23

Back-end services

Table 4 lists authentication and other back-end services specifications.

Table 4 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	Microsoft Windows 2000 Server SP4, Linux Fedora
DNS	Microsoft Windows 2000 Server SP4, Linux Fedora

Delivered software images

Table 5 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.

Table 5 Nortel SNAS 4050 software images

Image	Image
Boot Image	NSNAS-1.1.1-boot.img
Package	NSNAS-1.1.1-upgrade_complete.pkg
SREM	srem_1.2.1.0_014.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

Table 6 lists upper limit thresholds for hardware and network security software in the Nortel SNA solution.

Table 6 Hardware and software upper limit thresholds

Item	Maximum
Nortel SNAS 4050 devices in a cluster	2
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)	5
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.	800*
Users for each Nortel SNAS 4050 cluster	1500
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 800 concurrent user connections. When clustered for high availability and load balancing, the Nortel SNA solution supports 1500 concurrent user connections in a cluster. A single cluster supports a maximum of 2 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* (320818-A).

Implementation guidelines

To implement the solution, follow these general guidelines. For guideline details, see the *Nortel Secure Network Access Solution Guide* (320817-A).

1. Make a preliminary study and plan the implementation.
2. Configure the Windows server and DHCP.
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* (320818-A).
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 4.3.1* (217468-C) or *Release Notes for the Ethernet Routing Switch 8300 Software Release 2.2* (316811-D).
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* (320818-A).

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* (320818-A).

Known limitations and considerations in this release

Table 7 on page 15 lists Nortel SNAS 4050 open issues.

For Ethernet Routing Switch 5500 series issues, see *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 4.3.1* (217468-C).

For Ethernet Routing Switch 8300 series issues, see *Release Notes for the Ethernet Routing Switch 8300, Software Release 2.2.8.1* (316811-G).

Note: Ignore static client CLI commands for Nortel SNAS 4050, Ethernet Routing Switch 5500 series, and Ethernet Routing Switch 8300 switches at this time. Use dynamic client CLI commands for all operations. Static clients are not supported in this release.

Table 7 Nortel SNAS 4050 open issues

Change Request Number	Issue
Q01313825	In the SREM online Help, a number of pages do not display and you receive a “Page can not be displayed” error. To view the applicable information, refer to the equivalent pages in the *Nortel Secure Network Access Switch 4050 User Guide* (320818-A). Chapter 7, “TunnelGuard SRS Builder”: • Customizing a component, p. 324 • Adding comments, p. 348 Chapter 12, “Configuring SNMP”: • Configuring SNMP using the SREM, p. 632 • Removing SNMP targets, p. 639 • Adding monitor events, p. 648 • Removing monitor events, p.650
Q01301241	If you leave the TunnelGuard Administration applet running without any activity for more than four hours, the connection to the Nortel SNAS 4050 times out. No error message displays, and any unsaved SRS rule changes are lost. You must restart TunnelGuard Administration in order to re-establish the connection to the Nortel SNAS 4050.
Q01272433	An SSH connection can remain active through a Nortel SNAS 4050 configuration back-up and restore sequence. Follow these steps to avoid problems: 1. Before restoring a new configuration to a Nortel SNAS 4050 host, log out and then log on again as user: `admin`. 2. Keeping the current SSH session active, end all other SSH sessions. 3. Continue with the `restore` command. 4. If you are working in the SREM, use the `rediscovery` function to view the restored host as usual.
Q01272422	After a Nortel SNAS 4050 host is deleted, the SSH connection can remain active. Follow these steps to avoid problems: 1. Before deleting a Nortel SNAS 4050 host, log out and then log on again as user: `admin`. 2. Keeping the current SSH session active, end all other SSH sessions. 3. Delete the current Nortel SNAS 4050 host. 4. Configure the new Nortel SNAS 4050 host. 5. If you are working in the SREM, use the `rediscovery` function to view the new host as usual.

Table 7 Nortel SNAS 4050 open issues (continued)

Change Request Number	Issue
Q01270620	If a port goes down during a client session (for example, if a network cable is unplugged), the client will not be able to log on again successfully when the port comes back up. Workaround: When faced with a port down event, do the following: 1. Close all browser instances with an open Nortel SNAS 4050 portal page. 2. Re-establish a good network connection: – Unplug the cable connecting the PC to the network. – Wait two seconds. – Plug the network cable back in. 3. Reopen the Nortel SNAS 4050 portal page and log on again.
Q01258931	Because of the way Firefox manages its cache, the browser default web page requested through Firefox is unavailable through the Nortel SNAS 4050. Initial *and all* subsequent accesses of this URL are redirected to the portal login page specified through the Nortel SNAS 4050. Workaround: After logon, wait 30 seconds to allow the Firefox DNS cache to be released. Then open the URL as usual.
Q01256875	With Firefox and Netscape, if a user reboots a PC plugged into an IP Phone without first logging out from the portal page, the user will not be able to log on to the portal page again until the Nortel SNAS 4050 terminates the session (in accordance with the domain settings for client inactivity). To speed up the logon after rebooting, the user can issue an **`ipconfig/release`** and then an **`ipconfig/renew`** command.
Q01256113	When importing an SSH key from an Ethernet Routing Switch 5500 series edge switch, the Nortel SNAS 4050 displays the following incorrect error message if the edge switch is not available: `invalid key format`
Q01249223, Q01249387	FTP server access using the FTP link set is not currently supported. For FTP access, use an HTTP or HTTPS page with a link to the FTP server.
Q01227977	SREM attributes cannot be successfully mapped to SNMP OID values.
Q01204247-01	The `regevaltrace` CLI command function is not available in this release.

Table 7 Nortel SNAS 4050 open issues (continued)

Change Request Number	Issue
Q01200352, Q01231380, Q01210836	The SREM does not dynamically display new users through the GUI. Workaround: Perform a commit operation to display the user in the list. Perform a rediscover operation to display it in the tree. Alternatively, use the CLI and bypass the GUI to view new users.
Q01185432	`Config` check can give a misleading error message for a working RADIUS server due to a low timeout limit. To check if a configured RADIUS authentication server is working properly, add a user in RADIUS with the username “test”, password “dummy”, and then use the CLI command **`/maint/chkcfg`**.

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.

Change bars in the margin indicate new or changed information.

Using the TunnelGuard applet to run a script at logon

The following information supplements existing material about managing the end-user experience. It will be added to the chapter about configuring TunnelGuard Software Requirement Set (SRS) rules and included in the next release of the online Help.

Nortel Secure Network Access Switch 4050 User Guide (320818-A), Chapter 7, "TunnelGuard SRS Builder", p. 352

Configuring the TunnelGuard applet to execute a script at logon

You can configure the TunnelGuard applet to run an executable on the client PC after the client has been authenticated and granted access to the Green VLAN.

Software requirements

The Nortel SNA solution components require the following minimum versions of software to support this feature:

- Nortel SNAS 4050 Software Release 1.1.1
- SREM Software Release 1.2.1.0
- Ethernet Routing Switch 5500 Series, Software Release 4.3.1
- Ethernet Routing Switch 8300, Software Release 2.2.8.1

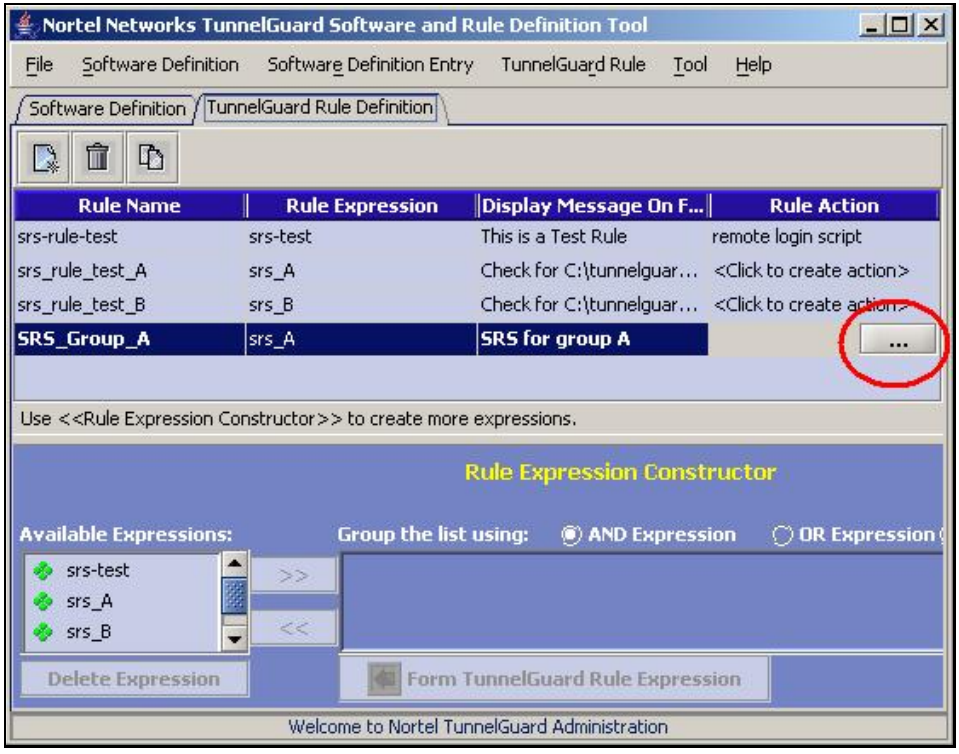
Configuring the SRS rule to run a script at logon

To configure the SRS rule to execute a script after the client successfully logs on, perform the following steps:

1. Create the script and save it on a server in the network. For more information about script requirements and a sample script, see "The executable script" on page 21.
2. Configure the SRS rule for the group and verify that the host integrity check is functioning correctly. For more information about configuring SRS rules, see "Managing TunnelGuard rules and expressions" on page 327 of *Nortel Secure Network Access Switch 4050 User Guide* (320818-A).
3. Modify the SRS rule definition for the group to specify the script:
   a. On the **TunnelGuard Rule Definition** tab, click in the **Rule Action** column of the rule associated with the group that will execute the script at logon.

      The ellipse (**...**) button appears (see Figure 1).

Figure 1 TunnelGuard Rule Definition tab



b Click the ellipse (**...**) button to edit the selected rule definition.

The **Rule Action Constructor** screen appears (see Figure 2 on page 20).

Figure 2 Rule Action Constructor

c Enter the script information in the applicable fields. Table 8 describes the Rule Action Constructor fields.

Table 8 Rule Action Constructor fields

Field	Description
Action Name	Specifies a descriptive name for the script.
Operating System	Specifies the client PC operating system. For Nortel SNAS 4050 release 1.1.1, the only option is `Windows`.
Type of Action	Specifies the executable action to be performed. For Nortel SNAS 4050 release 1.1.1, the only option is `Run Once On Success`. **Note:** With `Run Once On Success`, the script executes when the authenticated and authorized client first moves to the Green VLAN. If the client is subsequently moved to the Yellow VLAN and then back to Green, the script does not execute again. If the client is moved to the Red VLAN and then successfully reauthenticates and moves to the Green VLAN, the script will execute.
Command Type	Specifies the form in which the command is provided. For Nortel SNAS 4050 release 1.1.1, the only option is `Local Script`.
Command Text	Specifies the text of the command. For the `Local Script` type of command, specifies the path to the location where the script is stored.

d Click **OK**.

e On the **TunnelGuard Rule Definition** tab, click **File > Save** to save the modified SRS rule to the TunnelGuard server.

Note: To customize behavior for different groups on logon, create separate SRS rules and separate scripts for each group in your system. Then assign each script to the SRS rule for its group. The SRS rules for each group can all be associated with the same Software Definition if you want all the groups to satisfy the same host integrity criteria.

The executable script

The script executes as soon as the client moves to the Green VLAN, when the client DHCP request is renewed and the client obtains a new IP address. It is therefore necessary to build a small delay into the script to allow time for the client PC to establish connections to network servers (other than the domain controller) and for other PCs in the network to update their Address Resolution Protocol (ARP) cache entries with the client's new IP address. The usual way to provide such a delay is to use a sleep command or retry loop.

Figure 3 is an example of a script that uses Windows environment variables to map clients to network drives. Note the use of the sleep command.

Figure 3 Sample script to be executed at logon

```
@echo on
@echo Hello %USERNAME%, welcome to the network!
@echo You are accessing the network from %COMPUTERNAME%
@echo And you are running the %OS% os.
@echo Please wait, authenticating %USERNAME% with the % LOGONSERVER %
domain
@echo off

%LOGONSERVER%.lamly-sac.com\netlogon\sleep 2

REM Remove any local mappings to the drives that we want
NET USE H: /DELETE
NET USE G: /DELETE
NET USE P: /DELETE
NET USE Z: /DELETE

@REM Map drives that we need to
NET USE H: %LOGONSERVER%.lamly-sac.com\Share_1 /PERSISTENT:NO
NET USE G: %LOGONSERVER%.lamly-sac.com\Share_2 /PERSISTENT:NO
NET USE P: %LOGONSERVER%.lamly-sac.com\Share_3 /PERSISTENT:NO
NET USE Z: %LOGONSERVER%.lamly-sac.com\%USERNAME% /PERSISTENT:NO

@REM Launch sample application
start %LOGONSERVER%.lamly-sac.com\NETLOGON\DbgView.exe
```

Additional logging options

The following information replaces existing material about viewing log files. Equivalent information will be included in the SREM material in the chapter about system information and statistics and will be included in the next release of the online Help.

Nortel Secure Network Access Switch 4050 User Guide (320818-A), Chapter 13, "Viewing system information and performance statistics", p. 667

~~*Viewing log files using the CLI*~~

Configuring logging options and viewing log files using the CLI

You can log different types of activity on the Nortel SNAS 4050. Logging is performed by device, not for the cluster. The log will report activity for the Nortel SNAS 4050 device to which you are connected when you issue the **`/info/logs`** command. If you are logged on to the Management IP address (MIP) when you issue the command, the log will report activity for the Nortel SNAS 4050 device which is currently in control of the MIP.

To configure logging options and view and download log files, use the following command:

`/info/logs`

The **Logs** menu displays.

The **Logs** menu includes the following options:

`/info/logs` followed by:	
`list`	Displays a list of all log files.
`download <protocol> <server> <filename>`	Transmits the log file from the Nortel SNAS 4050 to a file on the specified TFTP/FTP/SFTP file exchange server. You are prompted to provide the following information: • *`protocol`* is the export protocol. Options are `tftp|ftp|scp|sftp`. The default is `tftp`. • *`server`* is the host name or IP address of the server. • *`filename`* is the name of the destination log file (*.log.x) on the file exchange server.

/info/logs followed by:	
port	Outputs all actions taken on a port. You are prompted to specify the following parameters: • switch — the switch ID • unit • port — the physical port number • MAC — (optional) the MAC address of a particular client device • user — (optional) the user name of a particular client
red	Logs port number and MAC address for clients in the Red VLAN.
switch	Shows when a switch connected to the Nortel SNAS 4050. You are prompted to specify the switch ID.
user	For a specified user, shows the user name, time logged on, and client's IP address in the Red VLAN on logon. You are prompted to specify the user name.

Figure 4 shows sample output for the **/info/logs/user** command.

Figure 4 Sample /info/logs/user output

```
>> Logs# user
User: nsna
== 20-Feb-2006::12:08:00 == INFO MSG -  <0.30449.7>
tg_ssl:135: new_session: user = nsna, client ip = 10.59.210.6

--
== 20-Feb-2006::12:18:44 == INFO MSG -  <0.31409.7>
tg_ssl:135: new_session: user = nsna, client ip = 10.59.210.6

--
== 21-Feb-2006::10:30:47 == INFO MSG -  <0.30867.3>
tg_ssl:135: new_session: user = nsna, client ip = 10.59.210.8
```

Recursive lookup for Active Directory

The following information supplements existing material about configuring LDAP authentication. Equivalent information will be included in the SREM material in the chapter about authentication and will be included in the next release of the online Help.

Nortel Secure Network Access Switch 4050 User Guide (320818-A), Chapter 6, "Configuring authentication", p. 260

Managing Active Directory passwords and recursive group lookup using the CLI

You can set up a mechanism for clients to change their passwords when the passwords expire.

1. Define a user group in the Local database for users whose passwords have expired.
2. Create a linkset and link to a site where the user can change the password (see "Configuring groups using the CLI" on page 198).
3. Map the linkset to the group (see "Mapping linksets to a group or profile using the CLI" on page 206).
4. Set the Active Directory settings using the **`/cfg/domain 1/aaa/auth #/ldap/activedire`** command.

To manage clients whose passwords have expired or who need to change their passwords, and to specify the Active Directory lookup settings for recursive group membership, use the following command:

```
/cfg/domain 1/aaa/auth #/ldap/activedire
```

The **Active Directory Settings** menu displays.

The **Active Directory Settings** menu includes the following options:

/cfg/domain 1/aaa/auth #/ldap/activedire followed by:	
`enaexpired true|false`	Specifies whether the system will perform a password-expired check. • `true` — the system performs a password-expired check against Active Directory when the client logs on • `false` — the system does not perform a password-expired check against Active Directory when the client logs on
`expiredgro <group>`	Specifies the group in which clients with expired passwords will be placed.
`recursivem true|false`	Specifies whether to resolve nested group names for recursive group membership. The options are: • `true` — If the client belongs to an Active Directory group which, in turn, belongs to another group, all groups are returned. • `false` — If the client belongs to an Active Directory group which, in turn, belongs to another group, only the first group is returned. The default value is `false`.

Ensuring all Nortel SNAS 4050 devices in a cluster will upgrade even if a device is down

The following information supplements existing material about configuring clusters. Similar notes will be included in the chapters on upgrading the software and on troubleshooting.

Nortel Secure Network Access Switch 4050 User Guide (320818-A), Chapter 2, "Initial setup", p. 61

Adding a Nortel SNAS 4050 device to a cluster

...

You can later modify settings for the cluster, the device, and the interfaces using the **`/cfg/sys/[host <host ID>/interface]`** commands.

Note: If STP is enabled on the ports to which the Nortel SNAS 4050 connects on the network access device, Nortel recommends that you enable fast start for STP on the edge switch or else disable STP on those ports. Otherwise, a future software upgrade may fail on the Nortel SNAS 4050 device if the device is down when the upgrade is performed on the rest of the cluster.

Setting status-quo and inactivity intervals to prevent Nortel SNAS 4050 transition failures

The following information supplements existing material about monitoring switch health and client activity. A similar note will be included for the SREM material in the chapter on managing the network access devices, in the Troubleshooting chapter, and in the next release of the online Help.

Nortel Secure Network Access Switch 4050 User Guide (320818-A), Chapter 3, "Managing the network access devices", p. 89

Monitoring switch health using the CLI

The Nortel SNAS 4050 continually monitors the health of the network access devices....When connectivity is re-established, the Nortel SNAS 4050 synchronizes sessions with the network access device.

The health check interval, dead count, and status-quo interval are configurable.

Note: On failure of a Nortel SNAS 4050 device in a cluster, the switch inactivity interval (interval x deadcnt) and status-quo interval (sq-int) provide a window for transferring control to the failover Nortel SNAS 4050 without disrupting existing client sessions. However, transition failures may occur if the client inactivity interval for the domain (heartbeat x hbretrycnt) expires within this window. By default, the status-quo interval is 1 minute, and the switch and client inactivity intervals are 3 minutes. If you are experiencing transition failures on failover, increase the status-quo interval for the network access device or else enable status-quo for the domain (so that client sessions continues indefinitely). For more information about setting the status-quo mode for the domain, see the **`/cfg/domain #/aaa/tg`** command on p. 132.

Note about corrupted software image downloads

The following information supplements existing material about upgrading the software.

Nortel Secure Network Access Switch 4050 User Guide (320818-A), Chapter 15, "Upgrading or reinstalling the software", p. 760

Activating the software upgrade package

The Nortel SNAS 4050 can hold up to two software versions simultaneously. To view the current software status, use the **`/boot/software/cur`** command. When a new version of the software is downloaded to the Nortel SNAS 4050, the software package is decompressed automatically and marked as *unpacked*. After you *activate* the unpacked software version (which causes the Nortel SNAS 4050 to reboot), the software version is marked as *permanent*. The software version previously marked as *permanent* is now marked as *old*.

Note: The existing *old* software version is deleted before the new version is downloaded. If the new image is corrupted during download or you attempt to activate an invalid file, the Nortel SNAS 4050 displays an error message and does not save the new image as either *unpacked* or *permanent*. The previous *permanent* software version remains unchanged, but there are no versions marked either *unpacked* or *old*.

Additional suggested items for the Exclude List

The following information supplements existing material about configuring the Nortel SNAS 4050 as a captive portal.

Nortel Secure Network Access Switch 4050 User Guide (320818-A), Chapter 9, "Customizing the portal and user logon", p. 387

Exclude List

...

By default, the captive portal Exclude List includes the following:

- windowsupdate

This will match all automatic Windows update domain names used by browsers, for example:

- windowsupdate.com
- windowsupdate.microsoft.com
- download.windowsupdate.microsoft.com

If your network includes clients using Netscape Navigator and Mozilla Firefox, Nortel recommends that you add the following entries to the Exclude List:

- For Netscape Navigator:
  - ns8-stats.netscape.com
  - home.netscape.com
- For Mozilla Firefox:
  - fxfeeds.mozilla.org

Warning about displaying the URL input field on the portal page

The following information corrects and supplements existing material about customizing the portal page. A similar note will be included for the SREM material in the chapter on customizing the portal and included in the next release of the online Help.

Nortel Secure Network Access Switch 4050 User Guide (320818-A), Chapter 9, "Customizing the portal and user logon", p. 406

Configuring the portal display using the CLI

To modify the look and feel of the portal page that displays in the client's web browser, use the following command:

```
/cfg/domain 1/portal
```

The **Portal** menu displays.

The **Portal** menu includes the following options:

/cfg/domain 1/portal followed by:	
`...`	
`linkurl on|off`	Sets the display mode for the Enter URL field on the portal Home tab. Display mode options are: • `on` — the Enter URL field is displayed • `off` — the Enter URL field is not displayed The default is `off`. When the option is enabled, a URL input field displays on the Nortel SNAS 4050 portal page for clients in the Green and Yellow VLANs. This gives clients the ability to go to any network which is reachable from the Nortel SNAS 4050 network. Potentially, therefore, it may allow clients in the Green and Yellow VLANs to bypass network restrictions. Before you enable the `linkurl` option (for example, to provide special access to a guest network), consider carefully whether your network design allows you to enable this option without compromising network security.
`...`	

Miscellaneous documentation additions and corrections

Installing and Using the Security & Routing Element Manager (SREM) (320199-B), Chapter 3, "Using SREM"

New material about the following topics has been added to the online Help and will be included in the next release of the print documentation:

- Modifying network information
- Applying and saving groups of changes
- Managing logs and statistics within the SREM

Nortel Secure Network Access Switch 4050 User Guide (320818-A), Chapter 4, "Configuring the domain", p. 134 and p. 132

In the descriptions of the TunnelGuard check settings in the online Help, the recheck and heartbeat intervals can also be expressed in days (d). The online Help has been updated and the correction will be included in the next release of the print documentation.

Nortel Secure Network Access Switch 4050 User Guide (320818-A), Chapter 9, "Customizing the portal and user logon", p. 448

New material about deleting custom content has been added to the online Help and will be included in the next release of the print documentation.

Reading path

This section lists documentation for the Nortel SNA solution, Nortel Secure Network Access Switch Software Release 1.1.1. For information about finding and accessing up-to-date documentation, see "Hard-copy technical manuals" on page 33.

Related publications

These publications are related to the Nortel SNA solution:

- *Nortel Secure Network Access Switch 4050 Installation Guide* (320846-A)
- *Nortel Secure Network Access Solution Guide* (320817-A)
- *Nortel Secure Network Access Switch 4050 User Guide* (320818-A)
- *Installing and Using the Security & Routing Element Manager (SREM)* (320199-B)
- *Release Notes for Enterprise Switch Manager (ESM), Software Release 5.1* (209960-H)
- *Release Notes for Nortel Ethernet Routing Switch 5500 Series, Software Release 4.3.1* (217468-C)

- *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:

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**.

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.