Part No. 320741-B
May 2006

Phone 1-800-4Nortel
http://www.nortel.com

# Release Notes for Nortel Real-time Threat Intelligence Sensors 3.5.1


NORTEL

Copyright © 2005–2006 Nortel Networks. All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks.

## Trademarks

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

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

The asterisk after a name denotes a trademarked item.

U.S. Government End Users: This document is provided with a “commercial item” as defined by FAR 2.101 (Oct. 1995) and contains “commercial technical data” and “commercial software documentation” as those terms are used in FAR 12.211-12.212 (Oct. 1995). Government End Users are authorized to use this documentation only in accordance with those rights and restrictions set forth herein, consistent with FAR 12.211- 12.212 (Oct. 1995), DFARS 227.7202 (JUN 1995) and DFARS 252.227-7015 (Nov. 1995).

# Contents

# Introduction

This document contains the latest information about the Nortel Real-time Threat Intelligence (RTI) Sensors Release 3.5.1.

The Nortel Real-time Threat Intelligence solution consists of the following components:

- TPS 2050 TI RTI Sensor with version 3.5.1
- TPS 2070 TI RTI Sensor with version 3.5.1
- RTI Host User license applied to the Nortel TPS 2070 Defense Center (based on the number of monitored network hosts)
- Nortel Real-time Visualizer 3.0.1 software

# Features and functionality

## TPS 2050 TI and TPS 2070 TI RTI Sensors

The TPS 2050 TI and TPS 2070 TI RTI Sensors contain the following features and functionality in release 3.5.1:

- Real-time Threat Intelligence (RTI) Visualizer 3.0.1: The Nortel RTI Visualizer client-side application generates a three-dimensional (3D) model of your network architecture based on accumulated RTI data. Used with an Event Streamer connection to a Defense Center, RTI Visualizer provides real-time depictions of variations within your network. For more information about the Real-Time Threat Intelligence Sensor Visualizer, see Table 2 (page 8), the *Real-Time Threat Intelligence Sensor Visualizer User Guide Release 3.0,* part number 322255-A and the *Real-time Threat Intelligence User Guide Release 3.5.1,* part number 320722-B.
- Statistical Network Behavior Anomaly Detection (SNBAD): RTI sensors deployed at key network intersections can create profiles of normal traffic patterns and can trigger alarms when anomalies are detected. Network Behavior Anomaly Detection (NBAD) systems monitor internal network traffic for profile deviations that indicate network misuse. SNBAD provides graphing and visual analysis of flow data to enhance NBAD.

- End Point Intelligence, Nessus Integration: The Nessus Active Scanner provides enhanced resolution of the RTI vulnerability database. Nessus is an open source vulnerability scanner that emulates attacker actions to help identify security weaknesses. The additional vulnerabilities provided by the Nessus Active Scanner can be added to a host record and leveraged for Impact Flag calculation. The Nessus vulnerabilities list can be added alone or in combination with the RTI list. Nessus scans can be initiated by a remediation module or on demand. Basic scans focussed against a range of IP addresses can be performed to provoke a response from hosts before they are completely profiled or discovered by RTI. Subsequent targeted scan responses can be detected by RTI to enhance the network map. Scan data obtained outside of the TPS system can be loaded directly into RTI.
- User Defined Host Attributes: You can add new information to an RTI host record. The new customer fields can contain numbers, text, or URLs. The data in the new customer fields can also be used as host qualifiers, used to build rules in the Policy and Response. Customer fields can include location, name of IT manager, and phone number. Lists can be created, composed from the customer fields, that are controlled by a pre-defined list of options.
- Regular Vulnerability Database Updates: When Nortel releases vulnerability database updates you can install them automatically from the RTI Sensor web interface without modifying your configuration, policies, or network settings. If you are using a Defense Center to manage your RTI Sensors you can install updates to groups of managed RTI Sensors from the Defense Center interface.
- Flow Data Visualization: You can display flow data metrics on charts and graphs and analyze traffic patterns and composition for trend analysis. Use the pre-defined charts or modify and customize graphs to change data ranges. Pre-defined charts include: Top 10 Initiators by number of flows and Top 10 Initiators by amount of traffic sent. Pie charts that show the mix of services comprising traffic are also included.
- Performance: Improved performance for RTI includes the addition of the Sfpacket Driver to RTI 2070. The Sfpacket Driver can also be applied to Intrusion Sensors running RTI software.
- Multiple detection engines and policies: One sensor can run multiple Snort instances associated with a named detection engine. The named detection engine can be associated with one or more interfaces. You can configure multiple policies on the same sensor to discover the interface where an event is detected. Events are associated with a detection engine rather than a sensor and you can create multiple virtual sensors on a single appliance. The upgrade process automatically creates a default detection engine for each upgraded sensor and converts existing policies to use the default detection engine.

## Product compatibility matrix

Table 1 indicates which version of Intrusion Sensors and RTI Sensors are compatible with each version of the Defense Center.

**Table 1** Compatibility matrix

| DC Version | IS Versions | RTI Versions |
|---|---|---|
| 4.5.1. | 4.5.1 | 3.5.1 |
| 4.1 | 4.1 | 3.1 |

# Hardware installation

There is no new hardware information for this release.

# General software information

Version 3.5.1 software, for contracted customers, is available on the Nortel Web site. For more information, see How to get help (page 24).

You can upgrade RTI appliances configured with software version 3.1.01 directly to version 3.5.1.

Separate RTI software for TPS Intrusion Sensors is no longer available. RTI for TPS IS can be activated from a Defense Center configured with Release 4.5.1. RTI licenses are separate from TPS Intrusion Sensor licenses and RTI sensors cannot be configured as Intrusion Sensors.

RTI Visualizer Release 3.0.1 software is available for download on the Nortel Web site. For more information, see Table 2 (page 8) and How to get help (page 24).

## Upgrade software

To upgrade an appliance from version 3.1.0.1 to version 3.5.1 use the RTI upgrade file **Nortel_TPS_RTI_Upgrade_3.1.0.1_to_3.5.1._Upgrade-47.sh**.

## Restore software

If an appliance configured with version 3.5.1 requires restoration, you must do the following:

1. Obtain the RTI 3.1.0 restore iso files from the Nortel Web site. See How to get help (page 24).
2. Apply the RTI 3.1.0 restore iso files.
3. Apply the 3.1.0.1 patch file.
4. Apply the upgrade to version 3.5.1 file.

### Restore iso files

The restore iso files for the RTI sensors are as follows:

- **Nortel_TPS_RTI_Sensor-2050-v3.1.0-78-Restore.iso** (TPS 2050 TI RTI Sensor)
- **Nortel_TPS_RTI_Sensor-2070-v3.1.0-78-Restore.iso** (TPS 2070 TI RTI Sensor)

## RTI Visualizer software

Table 2 lists RTI Visualizer Release 3.0 software file names.

**Table 2** RTI Visualizer software file names.

| Application | File name |
|---|---|
| RTI Visualizer 3.0 for Windows 2000 | RTIViz-3.0.1-625.win32.exe |
| RTI Visualizer 3.0 for Redhat Linux 8.0 | RTIViz-Redhat-9-3.0.1-625.i386.rpm |
| RTI Visualizer 3.0 for Redhat Linux 9.0 | RTIViz-Redhat-8-0.-3.0.1-625.i386.rpm |

To install the RTI Visualizer, see *Real-time Threat Intelligence Sensor Visualizer User Guide Release 3.0*, part number 322255-A.

## Updating software

Updates for RTI Sensor software are distributed electronically and can be downloaded from the Nortel web site. For complete instructions about performing this task, see *Nortel TPS Real-time Threat Intelligence User Guide*, part number 320722-B.

# Upgrading an RTI Sensor

This section describes upgrade prerequisites, provides important notes on the upgrade process, and presents the upgrade procedure.

## Upgrade prerequisites

You must meet the following prerequisites before upgrading your RTI appliance.

- RTI Sensor Release 3.1.0.1 is required to complete this upgrade. If you attempt to upgrade from an earlier version, the upgrade fails silently.
- You must have at least 32 MB of free space on the / partition and 97 MB of free space on the /var partition to complete this upgrade .
- Ensure that database limits for RTI events, flow data events, and policy violation events (called compliance events in Release 3.5.1) are set to 10 million or lower. If you have set the limits higher, adjust them and then wait for the database to prune itself before you begin the upgrade. Note that event processing pauses while the database is pruned. The prune is complete when the RTI Sensor begins processing events again.
- If you use a Defense Center to manage your RTI Sensors, ensure that you upgrade the Defense Center before you upgrade any sensors.

## Upgrade notes

Read the following notes before initiating the upgrade process.

- Before you begin the upgrade, Nortel recommends that you back up all event and configuration data and save it on a local computer.
- Schedule the upgrade during non-peak hours. Upgrade duration depends on the number of hosts, services, RTI events, and flow data events in the database. After the software upgrade is complete, you must wait for the vulnerability database upgrade before you begin receiving RNA events.
- If the upgrade halts do not restart it. Contact Nortel Support for more information.
- After the upgrade, the RTI Sensor reboots. Plan your upgrade for a time when it has the least impact on your deployment.
- When you upgrade to Release 3.5.1, backups stored on the RTI Sensor are not retained.
- Do not use the Web interface until the upgrade is complete and the appliance reboots.

- If you attempt to upload the upgrade script to the RTI Sensor over a slow connection, the web interface may time out before the upload is complete and the upload fails.
- During the upgrade to Release 3.5.1, the upgrade script disappears from the Updates page (on the Release 3.1.0.1 RTI Sensor). However, the upgrade installs successfully.
- If you change the management port during the initial setup for any appliance in your deployment, ensure that you change the port on all the appliances.
- If, during upgrade, you do not receive traffic on a non-bypass-enabled inline interface, ensure that the inline interface set contains the interface. If the inline interface set does not contain the interface, open the Interface Set page and manually add the interface to the interface set.
- When you start the upgrade, running tasks in the task queue are cancelled automatically, and tasks scheduled to occur during the upgrade do not run.

After you have met the prerequisites and read the upgrade notes, use the Upgrade procedure to upgrade an RTI Sensor.

## Upgrade procedure

1. Download the RTI Sensor 3.5.1 upgrade script directly from the Nortel Web site.
2. On the RTI Sensor, select **Administration**.
   The Administration page opens.
3. Select **Update**.
   The Update page opens.
4. Select **View**.
5. On the Update page, click **Browse** to navigate to the location where you saved the upgrade script.
6. Click **Upload**.
7. Under Install Update, select the upgrade.
8. Click **Install**.
9. Confirm that you want to install the upgrade and reboot the RTI Sensor.
   The upgrade is installed and the RTI Sensor automatically reboots.

To confirm the software version when the upgrade completes, follow the steps in Confirming the software version procedure (page 11).

## Confirming the software version procedure

1. Open the Operations page.
2. Select **Help**.
3. Select **About**.
   Confirm that the software version is 3.5.1.

# Restoring a Threat Intelligence Sensor

Restoration software is available for download on the Nortel web site. See Finding the latest updates on the Nortel web site (page 24).

To restore a TPS appliance to original factory settings, create a CD-ROM containing the restore files and follow the Restoration procedure in this section.

A keyboard and VGA monitor must be used, rather than the serial port, when restoring the TPS software for the TPS 2070 TI platform to its original state. Turn off the power to the TPS appliance before connecting the keyboard and monitor. Connect the keyboard and monitor. Turn on the power to the appliance and start it from the Software CD using the Restore procedure, see Step 1 of the following procedure. Follow the instructions on the monitor. When the software has been restored, see Step 4, turn off power to the appliance and disconnect the keyboard and monitor. Continue with Step 5 of the procedure.

**IMPORTANT! –** Restoring a TPS appliance results in the loss of all configuration and event data on the appliance. Nortel recommends that you back up the application before using the Restore CD-ROM.

To restore a TPS appliance to its original factory settings, use the Restoration procedure.

## Restoration procedure

1. Place the Restore CD-ROM in the CD tray and perform a safe reboot of the appliance. After the appliance reboots, you are prompted to restore the system.
2. At the prompt, type **Yes**.
3. Press **Enter**.
4. At the prompt, type one of the following:
   a. To confirm the restoration, type **Yes**.
   b. To halt the restoration, type **No**.
   **TIP**: After the system is restored, the appliance ejects the CD-ROM and reboots.
5. Connect the appliance and restore power.
6. If the Add Feature License page appears, paste the original license file into the License field.
7. Click **Submit License**.

When the restoration is complete, apply the Release 3.5.1 patch file.

# Returning a Threat Intelligence Sensor to the previous software version

**IMPORTANT! –** Contact Nortel Support before you return the RTI Sensor to the previous software version.

Use the Return to previous software version procedure to return an RTI Sensor to software release 3.1.0.1.

## Return to previous software version procedure

1. Select **Operations**.
2. Select **Update**.
   The Patch Management Update page appears.
3. Select the uninstaller that matches the upgrade you want to remove.
4. Click **Install**.
   The update is removed, the RTI Sensor is rebooted, and the RTI Sensor reverts to software release 3.1.0.1.

**IMPORTANT! –** If the operation halts, do not restart it. Contact Nortel Support for more information.

5. After the uninstall finishes and the RTI Sensor reboots, use secure shell (ssh) to log into the RTI Sensor with the root account.
6. View the following log file to check to ensure that you have enough free space on your hard drive to complete the task:

**/var/log/sf/Nortel_TPS_RTI_Upgrade_3.5.0/A_revert_prep.sh.log**

7. If the log file indicates that you have enough disk space, type **`revert`** at the command prompt.
8. Press **Enter**.

When the revert operation is complete, use the Confirming the software version procedure (page 14) to confirm the software version.

## Confirming the software version procedure

1. Log in to the RTI Sensor.
2. Select **Operations**.
3. Select **Help**.
4. Select **About**.
   Confirm that the software version is listed as 3.1.0.1.

# Resolved issues

The following issues concerning TPS 2050 TI and TPS 2070 TI RTI Sensors have been resolved in release 3.5.1:

- Destination-based remediations do not work on standalone RTI Sensors because RTI events have only source hosts transmitted in the event. Some of the included remediation modules, for example Cisco PIX Shun, Cisco IOS Null Route, and CheckPoint OPSEC SAM, provide destination-based remediations. (16149)
- Reboot the appliance if it does not restart properly after the DNS server on the Network page is changed. (16909)
- If you manually upload an update, ensure that you manually push the update to the appliance and install the update manually. If you manually upload an update and use the Task Scheduler to schedule the installation it fails. A success e-mail is sent even though the installation has failed. (17094)
- When creating a Block To/From Destination IP/Network remediation for a CheckPoint OPSEC SAM instance, the Log and Alert options are reversed. That is, selecting Log stores the remediation with the log_alert response and selecting Alert stores the remediation with the log_noalert response. (17426)
- Use Secure Copy  (remote file copy program) to copy large backup files to and from the Defense Center. Most web browsers do not support file transfers larger and 2 Gb. Ensure that you use the Access Configuration page to allow a connection between the Defense Center and the local machine where the backup files are stored. On the RTI Sensor backup files are stored in /var/sf/backup. (20061, 20064)
- File and product names used in the installation and restore processes are not rebranded. (20158, 20160)
- SSL access restriction locks out approved device. (CR Q01163853)
- The RTI/Maintenance/Task is missing. (CR Q01154875)
- Console I/O is not redirected to the serial port when using Restore or Install CD-ROMs for TPS 2070 IS, TPS 2170 IS, TPS 2070 TI, and TPS 2070 DC. (21355, CR Q01173831)
- Bookmarks cannot be saved when using Help from within the GUI. (21384, CR Q01150679)
- Sensor upgrade installation fails. If the unsupported action of uploading RTI software directly to an Intrusion Sensor, without installing the software, occurs, then an installation attempt using the Defense Center fails. (CR Q01166446)

- Local sessions no longer need to store the user name and password. (13695)
- Tasks scheduled for midnight run. (17359)
- The NOT operator ( ! ) functions correctly as shown in the examples on the Search pages. (17490)
- Performance was improved on the updates page ( Operations > Update ) (18903)
- If a user exceeds the maximum number of failed logins, the admin user can unlock the user access to the RTI Sensor by resetting to the old password from the User Management page. (20384)
- Users cannot create passwords longer than 32 characters, the maximum length allowed by the login page. (21141)
- You can remove old patch and upgrade scripts from the web interface. (22514)
- The Back button in Internet Explorer returns to the previous page. (23100)
- You can sort the list of patches and upgrades by type, version, and creation date. (23230)
- Only users with admin access can purge RTI events. (24606)
- The percentage of packets dropped by RTI is correctly reported. (24816)
- When you check the Confirm All Actions check box on the Event Preferences page, you must confirm that you want to perform an action on all the events that appear on an event view. (24893)

# Known issues

The following known limitations apply to the TPS 2050 TI and TPS 2070 TI RTI Sensors:

- When you install RTI Visualizer on Windows XP, a Security Warning appears stating that the publisher is unknown. (17210)
- When you save a graph on a RedHat 9 box the save results in a zero length file. (24092)
- You may experience small graphics issues like display distortion of the Single Query window when you drag the left border on a laptop using non-standard drivers (such as a manufacturer driver from Dell rather than the Nvidia unified driver). (24543)
- If a screen saver starts when RTI Visualizer is open, a command prompt containing errors may appear. RTI Visualizer continues to operate until you close the command prompt, at which point RTI Visualizer closes. **CAUTION**: To avoid losing your work, wait to close the command prompt until you have completed your current task. **WORKAROUND**: Disable your screensaver prior to working with RTI Visualizer. (24723)
- Selecting a domain does not give the same results as querying on the domain. Because domains may contain collapsed sub-domains, and Select Group only selects nodes that are visible, when you select a domain, the host count does not include those hidden hosts, whereas a query for a domain does. (25825)
- When you use an RTI Visualizer Version 3.0 client to query an appliance running a version of RTI prior to 3.5.1 or a version of the Defense Center prior to 4.5.1, the Sensor single query is not available. **WORKAROUND**: Run a multi query. (26678)
- The d (demo mode), r (reset view) , and w (wireframe mode) shortcut keys do not work on RedHat 9. (27344)
- On the View Schedules page ensure that the correct check boxes are selected after specifying whether the task is recurring or one time only. If the New Task option and Backup for the Job Type are selected and the Event or Configuration check boxes are selected before changing the task type between once and recurring, then the check boxes clear. (13992)
- The Scheduler page does not display an error message if an e-mail address is specified in the E-mail Status To field before setting up the mail relay host on the Configure E-mail Notification page. (14002)

- If a user account is deleted and a new account is created with the same name but differing access permissions, the new account reverts to the permissions from the deleted account. You must edit the new user account to ensure that account permissions are correct. (14037, 16291)
- The navigation menu disappears on some browsers if the Start Net Backup button on the Backup and Restore page is clicked before the name for the backup file is specified. Refresh the browser window to restore the navigation menu. (14099)
- Account privileges for users logged in as Admin may be reduced to Maintenance access. To regain Admin access log out and log in again. (14725)
- The Defense Center and managed sensors must be on the same side of a network address translation (NAT) device. If the network environment is not configured in this way, contact Nortel Support for configuration assistance. (15453)
- When a compliance policy is created based on the “a new transport protocol is detected” criterion using Transport Protocol as the condition, only the protocol abbreviation, for example UDP, can be used (and not the protocol number, for example 17). (15955)
- Configure the DHCP server to transmit the same NTP server. Otherwise, when the time is set on the sensor using the Via NTP Server option, and the DHCP server transmits a different NTP server record, the DHCP-provided NTP server is used when the sensor is rebooted. (16452)
- In High Availability environments a Defense Center must be used to collect custom fingerprints. (16809)
- The information collected is not deleted from the sensor if a managed sensor is used to collect custom fingerprints. (16809)
- The Japanese language is not supported in this release.
- The Safari web browser for Mac OS X is not supported.
- Because you can apply a system policy to any appliance model, you can use the web interface to set higher event storage database limits than the absolute maximum number of database records enforced by Nortel TPS for the appliance. When you apply the policy, the absolute limits are automatically enforced. (16603)
- If you apply multiple conflicting policies to the same sensor or detection engine while the sensor is not communicating with the Defense Center, the Defense Center may not apply the correct policy when it begins communicating again. **Workaround**: check the task queue to ensure that each policy is successfully applied before you attempt to apply a new policy of the same type. (16849)

- CPU Usage, User and CPU Usage: System performance statistics values report only the CPU usage of the thread that checks for performance data, rather than the total user and system CPU usage. (23441)
- The Defense Center automatically adjusts its local time display for daylight saving time (DST), where appropriate. However, recurring tasks that span the transition dates from DST to standard time and back do not adjust for the transition. (23732)
- Depending on the time zone setting on your RTI Sensor, including many Asian, Pacific, Indian Ocean, and South American time zone settings, you may not be able to perform or save a search for events using relative times. (25069)
- During initial setup, if you configure the system policy on your RTI Sensor to receive time through an external NTP server, then save the system policy, depending on the time served by the NTP server you may be automatically logged out of the web interface. However, all of the settings you specified are saved. Log in again to continue the setup. (25219)
- If you run dhcpd mangement_interface , where mangement_interface is the name of your management interface (for example, eth0 ), you must reboot the RTI Sensor for the new IP address to be accessible. (25253)
- If you are using Internet Explorer on a computer running Microsoft Windows XP, the page load progress bar may indicate that the page load is complete before the page has finished loading and is ready for interaction. (25892)
- If you start the local Nessus server on the RTI Sensor, then perform a backup and restore of the appliance, the Nessus server stops. To perform scans, you must restart the local Nessus server. (26853)
- Tasks in the task queue may be incorrectly nested. (26886, 27327)
- If you create a custom vulnerabilities workflow and then specify the new workflow or the predefined vulnerabilities workflow as your default, you are prompted to select a workflow when you view vulnerabilities. (26889)
- If you are not logged in as the admin user you cannot see a list of completed tasks. (26910)
- Do not use keyboard shortcuts to specify an interface set type if you use Internet Explorer. (26946)
- When you use the RTI Sensor web interface to apply a system policy to the RTI Sensor , you do not receive success confirmation and the task queue does not contain a record of the policy application. (26968)

- After the upgrade to Release 3.5.1, remediation status events are not sorted by time (the default for event views) in the remediation status table view of events. To sort the results by time, click the Time column title. (26987)
- The task queue continues to report that the scan is running when a Nessus scan finishes. **Workaround**: manually remove completed scans from the task queue. (26996)
- Editing an interface set: removing an interface from the list of available interfaces before the web interface loads all of the entire list causes the interface to disappear from view. **Solution**: Cancel the edit or wait until the web interface finishes loading. (27098)
- Multiple remote managers are not supported. Do not specify more than one remote manager for a sensor. (27123)
- When you delete a user account you are not prompted to confirm the deletion and the account is immediately deleted. (27146)
- Only the admin user can delete completed jobs, initiated by other users, from the task queue. (27158)
- The Back button in Firefox does not always return to the previous page. **Workaround**: use the menu structure. (27256)
- If you delete a sensor from the Defense Center, you must use the Task Status page to manually delete any tasks running at the time of deletion. (27260)
- You cannot use wildcards to search by MAC address for RNA-based events. (27268)
- On any RNA table view that includes the OS Version column, if you select an OS version that contains multiple versions as a constraint, and save the constraint as query, you must click Edit Query. On the Search page, you must place double quotes around the version numbers in the OS Version field before you can use the saved search. (27304)
- Avoid deleting tens of thousands of services from the services table view at once. **Workaround**: delete several thousand at once. (27312)
- If you deactivate all the vulnerabilities for a host in the host profile, you cannot reactivate any of them until a new vulnerability is detected for that host. (27350)
- The Web interface allows specification of an invalid IP address for the RTI Sensor management interface in the system settings. **Workaround**: do not specify an invalid IP address for the RTI Sensor management interface in the system settings. (27773)
- You cannot use the Analysis & Reporting, Policy & Response, or Operations menus while pages load. (27967)

- RTI Software for the Intrusion Sensor is not supported on the Service Delivery Module (SDM) 8600, although the web interface allows you to configure RNA detection engines and policies for the SDM 8600. (28048, 28700)
- If you want to use the Defense Center to serve time using Network Time Protocol (NTP), you must enable NTP in the Defense Center system policy and apply the policy to the Defense Center before you apply the policy to the sensors it manages. **Caution**: do not apply the policy to the Defense Center and the sensors at the same time. (28153)
- Nortel recommends that you do not assign a remediation as a response to an event that occurs frequently. (28338)
- If you create a compliance rule, Rule 1, based on a traffic profile change and then create another compliance rule, Rule 2, that triggers only if Rule 1 is true, Rule 2 cannot be enforced. (28459)
- If you want to bookmark a page in the online help using Firefox, do not use the bookmark icon in the online help. Use the browser bookmarking feature. (28499)
- While restoring from a backup, the restore job may appear to suspend in the task queue, even though it is complete. **Solution**: cancel the job in the task queue and reboot the RTI Sensor. (28532)
- If you are viewing the task queue for an appliance in a pop-up window you cannot view the task queue for a second appliance in a pop-up window. **Workaround**: select Operations > Monitoring > Task Status to view the task status for the second appliance. (28613)
- Although the web interface allows it, do not specify a name for a custom workflow that contains an apostrophe. You cannot choose those workflows containing an apostrophe as default workflows on the Event View Settings page. (28614)
- When configuring OPSEC remediations for Check Point Firewalls, using the web interface to set the logging level to Log actually sets the logging level to Alert . Setting the logging level to Alert actually sets the logging level to Log . (28659)
- If you upgrade your RTI Sensor to Release 3.5.1 and use the restore CD to return the appliance to a previous software version, your network and license settings are lost. Make a copy of the network and license settings settings before you initiate a restoration. (28672)
- If the detection engine column in the table view of events is blank, you cannot set attributes for hosts displayed in a custom table. **Workaround**: set the host attributes from the host profiles of the individual hosts or from the default host attributes table view of events provided with your RTI Sensor. (28675)

- Inline and Inline with Fail Open interface sets are not supported on the SDM 8600. (28676)
- You cannot create a Host Attributes report if you constrain the hosts that appear in that report based on their IP addresses. (28725)
- If you create a Host Attribute report and one of the attributes is of type List, the values assigned to each host for that attribute are rendered incorrectly. (28727)

# Known issues for RTI Visualizer

The following known limitations apply to the RTI Visualizer:

- When you install RTI Visualizer on Windows XP, a Security Warning appears that states that the publisher is unknown. (17210)
- You cannot save a graph on a Red Hat 9 computer. (24092)
- If you use  non-standard drivers you may experience display distortion of the Single Query window when you drag the left border on a laptop . (24543)
- If a screen saver starts while you have RTI Visualizer open, a command prompt containing errors may appear. RTI Visualizer continues to operate until you close the command prompt and RTI Visualizer closes. To avoid losing your work, wait to close the command prompt until you have completed your current task. **Workaround**: disable your screensaver prior to working with RTI Visualizer. (24723)
- Selecting a domain and querying on the domain do not produce the same results. Domains may contain collapsed sub-domains and Select Group only selects nodes that are visible. When you select a domain, the host count does not include hidden hosts but a query for a domain includes hidden hosts. (25825)
- When you use an RTI Visualizer Version 3.0.1 client to query an appliance running an RTI version earlier than 3.5.1 or a version of the Defense Center earlier than 4.5.1, the Sensor single query is not available. **Workaround**: run a multi query. (26678)
- The d (demo mode), r (reset view) , and w (wireframe mode) shortcut keys do not work on Red Hat 9. (27344)

# Related publications

These release notes supplement the following documents:

- *TPS 2050 and TPS 2070 Intrusion Sensor User Guide* Release 4.5.1, part number 216884-D
- *TPS 2070 Defense Center User Guide Release 4.5.1,* part number 216886-D
- *Real-time Threat Intelligence User Guide Release 3.5.1,* part number 320722-B
- Real-time Threat Intelligence Sensor Visualizer User Guide Release 3.0, part number 322255-A
- *TPS Intrusion Sensor and Defense Center Installation Guide,* part number 320737-A
- *TPS Real-time Threat Intelligence Sensor Installation Guide,* part number 320738-A
- *TPS Remediation Module for Application Switch Installation & Configuration Guide,* part number 320739-A
- *Threat Protection System 4.5.1 Release Notes,* part number 320740-B

# How to get help

This section explains how to get help for Nortel products and services.

## Finding the latest updates on the Nortel web site

The content of this documentation was current at the time the product was released. To check for updates to the latest documentation and software, click one of the following links:

| | |
|---|---|
| Latest Documentation | Takes you directly to the Nortel page for Threat Protection System documentation |
| Latest Software | Takes you directly to the Nortel page for Threat Protection System software |
| Lastest Software | Takes you directly to the Nortel page for Threat Protection System rule update software |
| Latest Documentation | Takes you directly to the Nortel page for Threat Protection System rule update documenation. |

## Getting help from the Nortel web site

The best way to get technical support for Nortel products is from the Nortel Technical Support web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

## Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

www.nortel.com/callus

## Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

## Getting help through a Nortel distributor or reseller

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.