Part No. 320741-C
January 2007

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

Release Notes for Nortel Real-time Threat Intelligence Sensors 4.0

320741-C

NORTEL

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 4.0.

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

- TPS 2050 TI RTI Sensor with version 4.0
- TPS 2070 TI RTI Sensor with version 4.0
- 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

Product compatibility matrix

You must use Release 4.6 of the Defense Center to manage Release 4.0 of the RTI Sensor.

Hardware installation

There is no new hardware information for this release.

New 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 new features and functionality in release 4.0:

- **Compliance White List**: You can now use compliance white lists to specify which operating systems, services, client applications, and protocols are allowed on all or specified hosts on your network, without having to create complex compliance rules. You can use various configuration pages or survey your network, network segment, or individual IP address to populate the white list, which you can then edit. You add a white list to a compliance policy just as you would add a compliance rule. After initial evaluation, RNA generates a white list event, which is a special kind of compliance event, when a target host violates the white list. You can view white list events in a workflow, or search for specific white list events. Finally, you can configure the RTI Sensor to trigger responses automatically when it detects a white list violation.

- **Import and export of policies**: You can export RNA detection policies, RNA appliance policies, and system policies from one RTI Sensor and then import them on another RTI Sensor. You can export a single policy or several policies at once. If you attempt to import a policy revision that already exists on an appliance, the import fails. Note that policy import and export is not intended as a backup tool, but can be used to simplify the process of adding new appliances to your Nortel Threat Protection System.
- **Nessus XML File viewing**: You can now view the results file of a Nessus scan initiated by the integrated Nessus client as a rendered XML page in a pop-up window instead of having to download the file and read the XML code in a text editor.
- **Additional default workflows and report profiles**: The RTI Sensor includes a new Host Audit report profile that you can modify and use as a template for an event report. It also includes new Client Application Summaries, Network Services by Count, Network Services by Hit, and Operating System Summary workflows, which you cannot edit, and a new Hosts with Services Default Workflow and a new Service and Host Details workflow, which you can edit.

General software information

Version 4.0 software, for contracted customers, is available on the Nortel Web site. For more information, see How to get help (page 18).

You can upgrade RTI appliances configured with software version 3.5.1 directly to version 4.0.

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 4.6. RTI licenses are separate from TPS Intrusion Sensor licenses and RTI sensors cannot be configured as Intrusion Sensors.

RTI Visualizer Release 3.01 software is available for download on the Nortel Web site. For more information, see Table 1 (page 7) and How to get help (page 18).

Upgrade files

To upgrade an appliance from version 3.5.1.3 to version 4.0, use the RTI upgrade file **Nortel_TPS_Realtime_Threat_Intelligence_Upgrade_3.5.1.3_to_4.0.0-130.sh**.

Restoration

If an appliance configured with version 4.0 requires restoration, you must do the following:

1.Obtain the RTI 4.0.0 restore iso files from the Nortel Web site. See How to get help (page 18).

2. Apply the RTI 4.0.0 restore iso files.

Restore iso files

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

- **Nortel_TPS_RTI_Sensor-2x50-v4.6.0-1145-Restore.iso** (TPS 2050 TI RTI Sensor)
- **Nortel_TPS_RTI_Sensor-2x70-v4.6.0-1145-Restore.iso** (TPS 2070 TI RTI Sensor)

NOTE – The name of the RTI Sensor restore iso files indicates the Defense Center release. When you apply the file, it will state that it is the RTI Sensor 4.0.0 file.

RTI Visualizer software

Table 1 lists RTI Visualizer Release 3.0 software file names.

Table 1 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-C.

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.

- Upgrade the Defense Center, if any, that manages the RTI sensor to Release 4.6. See the *Nortel Threat Protection System Release 4.6 Release Notes (320740-C)* for more information.
- RTI Sensor Release 3.5.1.3 is required to complete this upgrade. If you attempt to upgrade from an earlier version, the upgrade fails silently. See Finding the latest updates on the Nortel web site (page 18).
- You must have at least 90 MB of free space on the / partition and 540 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 4.0) are set to 100 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.

  The time it takes to upgrade the RTI depends on the model. Assuming you have 1 million events in the database, you will need

  - 15 mins for a TPS2x50
  - 10 mins for a TPS2x70

  Rebooting the sensor can take an additional one to two minutes.
- Once you begin the upgrade, you can monitor its progress in the task queue (**Operations** > **Monitoring** > **Task Status**). Do not use the web interface to perform any other tasks until the upgrade has completed and the RTI Sensor reboots.

IMPORTANT! – Before the upgrade completes, the RTI Sensor may log you out. If this occurs, log in to the appliance and view the task queue. If the upgrade is still running, continue to refrain from using the web interface until the upgrade has completed.

- If the task queue stops updating with current status, manually refresh your browser. If you encounter issues with the upgrade, for example, if the task queue indicates that the upgrade has failed or if a manual refresh of the task queue shows no progress, do not restart the upgrade. Instead, please contact Nortel Support.

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 4.0 upgrade script (Nortel_TPS_Realtime_Threat_Intelligence_3.5.1.3_to_4.0.0-130.sh) directly from the Nortel Web site.

Warning: Download files directly from the Nortel Technical Support site. Do not transfer them by email. If you transfer an update file by email, it may become corrupted.

2. On the RTI Sensor, select **Operations**.
The Operations page opens.

3. Select **Update**.
   The Patch Management Update page opens.

4. Select **Upload Update**.

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.

IMPORTANT! – You can monitor the upgrade's progress in the task queue (**Operations > Monitoring** > **Task Status**). Do not use the web interface to perform any other tasks until the upgrade has completed and the RTI Sensor reboots. Note that before the upgrade completes, the RTI Sensor may log you out. If this occurs, log in to the appliance and view the task queue. If the upgrade is still running, continue to refrain from using the web interface until the upgrade has completed. If the task queue stops updating with current status, manually refresh your browser. If you encounter issues with the upgrade, for example, if the task queue indicates that the upgrade has failed or if a manual refresh of the task queue shows no progress, do not restart the upgrade. Instead, please contact Nortel Support.

10. After the upgrade finishes and the RTI Sensor reboots, log into the RTI sensor.

IMPORTANT! – If you are using Firefox 2.0, you may see some javascript errors. As a workaround, force a reload of the browser by pressing Shift while clicking the reload button.

To confirm the software version when the upgrade completes, follow the steps in Confirming the software version procedure (page 10).

Confirming the software version procedure

1.Open the Operations page.

2. Select **Help**.

3. Select **About**.
   Confirm that the software version is 4.0.

After you upgrade

After you complete the upgrade, you must

- Install any patches or upgrades to the RTI Sensor that are available on the Nortel Support site.
- Update the vulnerability database (VDB) on the RTI Sensor and on the Defense Center (if any) that manages it. Note that you can use the Defense Center to push and install the VDB on the RTI Sensor.

For more information, see the RTI Sensor User Guide.

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.

You cannot uninstall major upgrades to the Nortel TPS, including the Release 4.0 upgrade: you can only uninstall patches. Uninstalling a patch removes the features and functionality included in the patch, as well as its resolved issues, while retaining your configuration and event data.

You can revert an upgraded RTI Sensor to the previously installed software version. If you revert to the previous version, it reverts to the configuration before the upgrade.

NOTE – Events generated after the upgrade are not retained in the database. Events generated before the upgrade are retained, but may have already been purged.

NOTE – You cannot revert managed sensors through the Defense Center.

Revert the RTI Sensor

1.Use secure shell (ssh) to log into the RTI Sensor with the root account.

2. Check to make sure that you have enough free space on your hard drive to complete the task. View the following log file:

/var/log/sf/Nortel_TPS_Realtime_Threat_intelligence_Upgrade_4.0.0/200_prep/
A_revert_prep.sh.log

3. If the log file indicates that you have enough disk space, type revert at the command prompt and press **Enter**.

When the revert operation is complete, use the Confirming the software version procedure (page 12) 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 3.5.1.3.

Resolved issues

The following issues concerning TPS 2050 TI and TPS 2070 TI RTI Sensors have been resolved in release 4.0:

- Fixed an issue where the system policy creation web interface did not enforce the absolute maximum limit for database records at the time of policy creation. Now, when you save the policy, if a limit is set to exceed the absolute maximum number of events allowed, the limit is reduced to a number within the allowed range when you save the policy, and a message appears indicating that the number exceeded the maximum limit. (16603)
- You now must confirm deletion when you delete a user. (27146)
- Fixed an issue where, after you deactivated all vulnerabilities for a host, the Edit button disappeared. You can now reactivate a vulnerability in the host profile, even if all vulnerabilities are currently inactive.(27350)
- Fixed an issue where unresolved IP addresses were replaced by an error message on the Flow Summary page under Analysis & Reporting > Event Summary. If an IP address cannot be resolved to a host name, the IP address now appears rather than the error message. (27836, 28282)
- Fixed an issue where right-clicking on a menu did not produce the standard popup menu. (27958)
- Fixed a problem where saving an interface with a period in the name or description field dropped all changes. You can now use periods in interface names and descriptions. (27963, 29500)
- Fixed an issue where event processing performance diminished during RNA database pruning. (28423)

- Fixed an issue where certain event view workflows incorrectly advanced to the next page on automatic refresh. (28691)
- When you edit a network interface with auto-negotiate turned on, the web interface now accurately indicates the management interface link speed and duplex settings. (29057)
- You can now view the currently applied RNA appliance policy on the Sensors page for a managed sensor or on the Apply Policy page for appliance policies. (29160)
- Fixed an issue where RNA detected a restarted service as a new service and reset all vulnerability settings for the service when it restarted. When a previously detected service restarts, RNA now maintains any updates you made to vulnerabilities for the service. (29288)
- Fixed a problem where the comments field for scheduled jobs had an overly restrictive character set. You can now enter alphanumeric characters, spaces, periods (.), commas (,), semi-colons (;), dashes (-), underscores (_), and colons (:) in the comment field when scheduling a task. (29396)
- Fixed a problem where no feedback message was provided to indicate that a system policy was applied successfully. (29503)
- Fixed a problem where compliance rules with descriptions containing double quotation marks were evaluated as invalid. (30191, 31094)
- Fixed a problem where aberrantly high TTL values could cause an inaccurate hops count for a host. The hops count for a host is now updated if the TTL value for the host changes. (30219)
- Fixed an issue that caused CISCO PIX shun remediations to fail. (30431)
- Fixed a problem with IP address sorting in the RNA network map. (30532)
- Improved RNA event processing performance. (30534)
- Fixed an issue where network configuration and licenses were lost on system restore. (30585)
- Fixed an issue with resolution of custom classification names in compliance events. The names of custom classifications used in compliance rules now appear in events based on those rules. (30727)
- Snooze and inactive periods in compliance rules that trigger on traffic profile changes now work properly. (30752)
- Fixed an issue where overlapping network definitions for auto assignment of host attributes caused attribute assignment to fail after an overlap. (30843)
- Improved handling of list type host attribute values. (31393)
- Database tables can now grow as needed, within the constraints of available disk space, to accommodate table growth within the database. (32294, 32309)

Known issues

Known Issues - Release 4.0

The following are known issues with Release 4.0:

- If you add a custom logo or image to a remote report, the images do not display or do not display correctly. As a workaround, avoid using custom logos or images in reports you plan to run remotely, or run the reports locally. (29770, 32526)
- You cannot schedule installation of a VDB update from an RTI Sensor. You must install the update manually. (31045)
- When you create a compliance event syslog alert, you cannot use a comma-separated list to specify multiple logging hosts in one alert. As a workaround, create an alert for each host where you want to log alerts. (32176)
- The first time you use one of the navigation links available on workflow table view and drill-down pages, you may not retrieve any events even if there are events for that workflow. Click the link again to refresh the view with events. (32320)
- If you select a specific detection engine while creating a report based on a custom table, an error occurs when you preview the report and the report fails if you run it. As a workaround, search for all available detection engines as part of your original event search or select All in the Detection Engines drop-down list. You cannot select a detection engine group or a specific detection engine when creating a report. (32334, 32350)
- If you schedule report creation using the pre-defined Host Audit report profile, you cannot view resulting reports because of null values in the report definition. As a workaround, select Analysis & Reporting > Reporting, click Report Profiles, then click Edit next to the report profile you want to use. On the Report Designer page, click Save Report to save the profile without the null values. (32367)
- If you click Add to add an IP address to the Access List in the system policy, then click Help, the help appears with a blank topic in the help window. As a workaround, select the table of contents for the help and locate the Configuring the Access List for the RTI Sensor topic. (32372)
- If you delete events on a workflow page and then bookmark the page, the bookmark does not retrieve events. As a workaround, after you delete events, reload the workflow page and then bookmark it. (32548)
- When running large reports, the GUI can hang due to high use of resources. (20491)
- Restoring a large backup file can cause restore to fail. (20058)

Known Issues - Prior to Release 4.0

The following open issues were identified in versions prior to Release 4.0:

- If your /var partition goes below 15% of free space while data is being replicated to a backup file, the backup may fail. If a backup fails because you have insufficient disk space or too many events to successfully create a backup, contact Nortel Support. (13712)
- When you create a report based on the events in the clipboard, the start time and end time reported in the overall summary and any page summaries reflect the current time range on the RTI Sensor, rather than the timestamps of the events used to build the report. (21215)
- The RTI Sensor 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. That is, if you create a task scheduled for 2am during standard time, it will run at 3am during DST. Similarly, if you create a task scheduled for 2am during DST, it will run at 1am during standard time. (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 event using relative times (for example, < today at 4:30pm). (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. All the settings you specified so far are saved; log in again to continue setup. (25219)
- If you run dhcpd management_interface, where management_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 complete before the page is finished loading, leading you to believe that the page is ready for your interactions when it is not. (25892)
- If you start the local Nessus server on the RTI Sensor, then perform a backup and restore of the appliance, the Nessus server is stopped. You must re-start the local Nessus server if you want to use it to perform scans. (26853)
- Sometimes, tasks in the task queue are incorrectly nested. (26886, 27327)
- If you create a custom vulnerabilities workflow and then specify either the new workflow or the predefined vulnerabilities workflow as your default, when you view vulnerabilities, you are nevertheless prompted to select a workflow. (26889)

- If you are not logged in as the admin user, jobs created by other users may not be visible. (26910)
- 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)
- Occasionally, a Nessus scan finishes, but the task queue continues to report that the scan is still running. You should manually remove these jobs from the task queue. (26996)
- When editing an interface set, removing an interface from the list of available interfaces before the web interface loads all of the available interfaces causes it to disappear from view. Either cancel the edit or wait until the web interface completes its loading. (27098)
- The task queue may contain completed jobs, such as policy applications, that were initiated by other users. You cannot delete these completed tasks; only the admin user can delete them. (27158)
- The Back button in Firefox does not always take you back to the previous page. As a workaround, use the menu structure. (27256)
- On any RNA table view that includes the OS Version column, if you select as a constraint an OS version that contains multiple versions (for example, Mac OS 10.3 and 10.4 or Linux 2.4 and 2.6) and then save the constraint as query, you must click Edit Query and, on the resulting Search page, place double quotes around the version numbers in the OS Version field before you can use the saved search. (27304)
- You should avoid deleting tens of thousands of services from the services table view at one time. As a workaround, you can safely delete several thousand at one time. (27312)
- If you create a compliance rule based on a traffic profile change (in this example, Rule1) and then create another compliance rule (Rule2) that only triggers if Rule1 is true, that is, it has as one of its necessary conditions rule Rule1 is true, Rule2 will not fire. (28459)
- In rare cases, some SNMP management systems may have an issue with the order of the variables listed in the management information base (MIB). If this is an issue for you, please contact Nortel Support. (28508)
- Although the web interface allows it, do not specify a name for a custom workflow that contains an apostrophe. You cannot choose those workflows as default workflows on the Event View Settings page. (28614)

- You cannot set attributes for hosts displayed in a custom table if the detection engine column in the table view of events is blank. As a workaround, set the host attributes in another way, for example, from the host profiles of the individual hosts, or from the default host attributes table view of events provided with your RTI Sensor (Analysis & Reporting > RNA > Host Attributes). (28675)
- RNA and compliance events are always backed up on the Defense Center regardless of the setting you select for the Backup Events option on the system Backup page. (29983)
- RNA host reports based on custom workflows may have data sorted in descending order rather than ascending order. (31567)

Related publications

These release notes supplement the following documents:

- *Intrusion Sensor User Guide Release 4.6*, (216884-E)
- *Defense Center User Guide Release 4.6,* (216886-E)
- *Real-time Threat Intelligence User Guide Release 4.0,* (320722-C)
- *Real-time Threat Intelligence Sensor Visualizer User Guide Release 3.0,* (322255-A)
- *TPS Intrusion Sensor and Defense Center Installation Guide,* (320737-A)
- *TPS Real-time Threat Intelligence Sensor Installation Guide,* (320738-A)
- *TPS Remediation Module for Application Switch Installation & Configuration Guide,* (320739-A)
- *Threat Protection System 4.6 Release Notes,* (320740-C)

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.