Part No. 320742-A
Septmber 2005

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

Release Notes for Nortel Real-time Threat Intelligence Software for TPS Intrusion Sensors 3.1

NORTEL

Originated in the U.S.A.

Contents

Introduction

This document contains the latest information about the Nortel Real-time Threat Intelligence (RTI) software for Intrusion Sensors release 3.1.

The Nortel Real-time Threat Intelligence software for Intrusion Sensors affects the following appliances:

- Nortel TPS 2050 IS Intrusion Sensor
- Nortel TPS 2070 IS Intrusion Sensor
- Nortel TPS 2070 Defense Center

NOTE – Nortel Real-time Threat Intelligence software for TPS Sensors is available for download at www.nortel.com/support. When the Technical Support page opens, from the pull-down list next to selection 1, Select from, select Product Categories. Scroll to Security & VPN in the Product Categories list box. Select Threat Protection from the list. From selection 2, ... choose a product ..., select the applicable product. From selection 3, ... and get the content., select Software. Click Go. The software page opens.

Features and functionality

RTI software for TPS 2050 IS and TPS 2070 IS Intrusion Sensors

The RTI software for TPS 2050 IS and TPS 2070 IS contains the following features and functionality in release 3.1:

- Purchase of a Real-time Threat Intelligence Feature Host license is required. For maximum performance, Nortel* strongly recommends that the RTI Feature Host License is applied on the TPS 2070 Defense Center and that RTI Sensors are managed from the TPS 2070 DC. The Feature Host license is based on the number of hosts being monitored. Once the base RTI sensors are activated, an RTI Feature Host key-code must be applied to the TPS 2070 DC designated to monitor the network. When you purchase an RTI Feature Host license, a certificate containing an

authorization serial number, instructions, and an e-mail address used to obtain an RTI Feature Host license key-code is issued. For more information, see the Nortel TPS Real-time Threat Intelligence Sensor Installation Guide, part number 320738-A.

- Network discovery events are not saved on the Intrusion Sensor because Nortel RTI for Intrusion Sensors is managed entirely by the TPS 2070 Defense Center running version 4.1.
- RTI Supported on Intrusion Sensors — RTI software is supported on the TPS 2050 IS and the TPS 2070 IS. RTI Software for TPS Intrusion Sensors is not supported on an Intrusion Sensor configured to operate in inline mode.
- RTI does not appear on the GUI — RTI does not appear on the Intrusion Sensor GUI after it has been installed. To view the RTI build number from the Intrusion Sensor select **Help,** then select **About**.

Compatibility

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
v 4.1	v. 4.1	v 3.1

Hardware installation

Refer to the appropriate installation guide for complete instructions on the installation of the TPS 2070 Defense Center, the TPS 2050 Intrusion Sensor, or the TPS 2070 Intrusion Sensor . This documentation is provided on the product Documentation and Restore CD and is also available on the Nortel Technical Support web site at www.nortel.com/support.

Software installation

This section describes the prerequisites for installing RTI software on an Intrusion Sensor and provides the procedure for installing RTI software on an Intrusion Sensor.

Prerequisites for installing RTI software on an Intrusion Sensor

Installation of RTI software on an Intrusion Sensor requires the following prerequisites:

- At least 40 Mb of free space on the root partition (/), and 78 Mb of free space is required on the /var partition
- Intrusion Sensor upgrade to version 4.1 prior to RTI software installation
- Defense Center upgrade to version 4.1 prior to managing an RTI Software Sensor

Installing RTI software on an Intrusion Sensor

Use to the following procedure to install the RTI Software on an Intrusion Sensor:

1. Go to www.nortel.com/support.
2. Select **Product Categories** from the Select from pull-down list.
3. Scroll to Security & VPN in the Product Categories list.
4. Select **Threat Protection**.
5. Select the appropriate product from ... choose a product list.
6. Select **Software** from ... and get the content list.
7. Click **Go**.
8. Download the installation file, Nortel_TPS_RTI_IS_Installer-3.1.0-78.sh.

Refer to the *Nortel RTI Software for TPS Sensor Configuration Guide Release 3.1*, Part Number 320758-A, for information about configuring the Defense Center and installing the RTI software on Intrusion Sensors.

Known issues

- The Defense Center and managed sensors must reside on the same side of the network address translation (NAT) device. If the network environment is not configured in this way, contact Nortel Technical Support for configuration assistance. (15453)
- Note that some devices marketed as hubs function as switches. If a sensor connected to a network by a hub does not produce the expected traffic, use a different hub. (16583)

- Information is not deleted from a managed sensor if the sensor is used to collect custom fingerprints. (16809)
- Use a Defense Center to collect custom fingerprints in high availability environments. (16809)
- Extra MAC-only hosts may be seen in the network map. That is, if an RTI Sensor detects a non-IP protocol for a host before it detects an IP protocol, then the host is initially listed as a MAC-only host in the network map. If an IP protocol is later detected for the host, then the MAC-only and IP-based host information is merged. However, the MAC-only host is not deleted from the network map.
- The disk can fill with RTI binary files because the LogCleaner process does not remove old RTI binary files from the Intrusion Sensor hosting the RTI software.
- The restore operation fails – When saving the backup file to the local drive, the system adds brackets, with a number, to the file name. A file with this naming format is unreadable and, if it is uploaded, the restore fails. To perform a successful restoration, remove the brackets and the number from the file name and rename the file test.tar.gz. Upload the renamed file. (CR Q01172979)
- Snort causes incorrect error for replace option (does not have quotes). CR Q01175453)
- New rule with content, without quotes, causes fatal error and snort restarts. (CR Q01171982)
- Rebranding of file and product names used in the installation and restore processes is not rebranded. (20158, 20160)
- RTI reports are not e-mailed on generate report request. (20154, CR Q01156300)
- 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)

Checking disk status

- Check the disk status from the Defense Center managing the RTI software by doing the following:
  - Select **Monitoring**.
  - Select **Status**.
  - Select **Host Statistics**.

  From the Select Devices list, do the following:
  - Select the **Intrusion Sensor** hosting the RTI software.
  - Click **Select Devices.**
  - Click the down arrow to expand Disk Usage.
  - Review the available space on the /var partition.

Related publications

These release notes supplement the following documents:

- *TPS 2050 and TPS 2070 Intrusion Sensor User's Guide* Release 4.1 (Part Number 216884-C)
- *TPS 2070 Defense Center User's Guide* Release 4.1 (Part Number 216886-C)
- *Real-time Threat Intelligence User Guide Release 3.1* (Part Number 320722-A)
- *TPS Intrusion Sensor and Defense Center Installation Guide* Release 4.1 (Part Number 320737-A)
- *TPS Real-time Threat Intelligence Sensor Installation Guide Release 3.1* (Part Number 320738-A)
- *TPS Remediation Module for Application Switch Installation & Configuration Guide* Release 4.1 (Part Number 320739-A)
- *Threat Protection System 4.1 Release Notes* (Part Number 320740-A)
- *Real-time Threat Intelligence Sensors 3.1 Release Notes* (Part Number 320741-A)
- *Real-time Threat Intelligence Software for TPS Sensor Configuration Guide* Release 3.1 (Part Number 320758-A)

Refer to the documents in the previous list for additional technical information regarding the product architecture and features. These documents are available on the Nortel Technical Support web site. To access these documents:

- Open your web browser and enter www.nortel.com/support. The Technical Support page opens.
- Select the **Browse Product Support** tab if it is not already selected.
- To go to the Threat Protection page, do the following:
  - From the pull-down list next to selection 1, Select from, select **Product Categories.**
  - Scroll to Security & VPN in the Product Categories list box.
  - Select **Threat Protection** from the list**.**
  - From selection 2, ... choose a product ..., select the applicable product.
  - From selection 3, ... and get the content., select the type of information you require. For example, select **Documentation**.
- Click **Go**. The product documentation page opens.

The User's Guide and Installation Instructions are PDF files that can be read and printed using the free Acrobat Reader® software available from Adobe Systems Incorporated at the Adobe web site. To obtain a manual in hardcopy format, contact your Nortel sales representative and order the appropriate part number.

Technical support

Technical support for your Nortel product is available through the Technical Solutions Center.

Technical Solutions Center telephone

Europe, Middle East, and Africa - 00800 8008 9009 or +44 (0) 870 907 9009

North America - (800) 4NORTEL or (800) 466-7835

Asia Pacific - (61) (2) 8870-8800

China - (800) 810-5000

Additional information about the Nortel Technical Solutions Centers is available at www.nortel.com/support.

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 an ERC for your product or service, refer to www.nortel.com/erc.