Document Number: NN47240-400
July 2008
Phone 1-800-4Nortel
http://www.nortel.com

Release Notes for Nortel Threat Protection System Release 4.7.0.5



NORTEL

Copyright © 2008 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 logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks and registered trademarks are the property of their respective owners.

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).

Export

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or reexport may be required by the U.S. Department of Commerce.

July 30, 2008

Contents

Introduction 5
Product Compatibility 5
New features and functionality 6
TPS 2070 Defense Center 8
TPS 3D Sensor 9
General software information 11
Upgrade files 11
Nortel TPS Defense Center: 11
Nortel TPS 3D Sensor (Intrusion Sensor) 12
Nortel TPS 3D Sensor (RNA Sensor) 12
Updating existing appliances and software sensors 13
Planning the update: Defense Center and 3D Managed Sensors 13
Updating the Defense Center 16
Updating 3D Managed Sensors 17
Updating unmanaged 3D sensors 19
Planning for the Update: Unmanaged or standalone sensors 20
Updating an unmanaged sensor 21
After updating your appliances 22
Uninstalling the update 23
Issues resolved in TPS Release 4.7.0.5 24
Issues resolved in both Defense Center and 3D sensors in Release 4.7.0.5 24
Known issues in TPS Release 4.7.0.5 24
Known issues in Defense Center 26
Known issues identified in Defense Center prior to Release 4.7 28
Known issues in 3D Sensor 30
Known Issues in 3D sensors identified prior to Release 4.7 31
Hardware installation 35
Defense Center 35
3D Sensors 35

Related publications 35
How to get help 36
Finding the latest updates on the Nortel web site 36
Getting help from the Nortel web site 36
Getting help over the phone from a Nortel Solutions Center 37
Getting help from a specialist by using an Express Routing Code 37
Getting help through a Nortel distributor or reseller 37

Introduction

These release notes are valid for version 4.7.0.5 of the Nortel Threat Protection System (TPS).

IMPORTANT! Beginning with Release 4.7 software, 3D Sensors refer to both Intrusion Sensors and RTI Sensors. A 3D Sensor is able to have Intrusion Sensing (IPS/IDS) and/or RTI capabilities.

The Nortel TPS is a fully integrated intrusion detection system that consists of the following:

- TPS 2070 Defense Center, which manages 3D sensors in the network environment.
- TPS 3D Sensors (TPS 2050 3D and TPS 2070 3D Sensor), which detect and track network intrusions, either independently or under the management of the TPS 2070 Defense Center.
- TPS 3D Sensors (2150 Intrusion Sensor and TPS 2170 Intrusion Sensor), which deliver fail-open functionality in Inline mode.
- Ethernet Routing Switch (ERS) 8600 Release 4.1, which supports the Service Delivery Module (SDM) that includes Threat Protection System (TPS) Release 4.6. In this configuration, TPS enables audit and alert functions independent of all other security devices deployed on a network.

Product Compatibility

You must use version 4.7.0.5 of the Defense Center to manage version 4.7.0.5 of the 3D Sensors (Intrusion Sensors, and RNA Sensors).

Version 4.7.0.5 of the Defense Center can manage:

- versions 4.7.0.1 and 4.7.0 of the 3D Sensor
- version 4.6.x.x of the Intrusion Sensor
- version 4.0.0.x of the RNA Sensor (also called the RTI Sensor)

Figure 1 Product compatibility matrix

The following table indicates the version of 3D sensors that are compatible with each version of the Defense Center. It also indicates the version of ERS 8600 Release 4.1 that is compatible with each version of the Defense Center and 3D sensors.

Table 1 Compatibility Matrix

DC Version	ISensor Versions	RTI Versions	ERS 8600
4.7.0.5	4.7.0.5	Not applicable	4.1.3.0
4.7.0.4	4.7.0.4	Not applicable	4.1.3.0
4.7.0.3	4.7.0.3	Not applicable	4.1.3.0
4.7.0.2	4.7.0.2	Not applicable	4.1.3.0
4.6	4.6	4.0	4.1.1.0
4.5.1	4.5.1	3.5.1	4.1.0.0
4.1	4.1	3.1	N/A

New features and functionality

Version 4.7.0.5 does not contain any new features or functionality. For a complete listing of the issues resolved in version 4.7.0.5 see Issues resolved in both Defense Center and 3D sensors in Release 4.7.0.5 (page 24). The following sections describe the existing features and functionality in TPS version 4.7

- TPS 2070 Defense Center (page 8)
- TPS 3D Sensor (page 9)

The following features and functionality are common to both the 2070 Defense Center and the 3D Sensors (Intrusion Sensors and RNA Sensors).

- **Improved Setup Wizard**:When you log into the web interface of your appliance for the first time, you are presented with an improved series of start-up pages. Each page takes you through a portion of the setup process for a newly installed appliance. These pages display in a logical sequence so that you can readily configure your appliance for operation. Configuration defaults and applicable online help facilitate simplified appliance setup and expedite the deployment process.

- **Nmap Integration**: You can use Nmap's active scanning capabilities on both the Defense Center and the 3D Sensor to enhance the information in your RNA network map. Because RNA passively detects information about a host by watching traffic that crosses your network, if a service does not generate traffic, RNA cannot detect it. When you scan a host, Nmap actively sends packets to ports on the host to obtain details about the host's operating system and services. It then adds that data to the host profile for the host. Nmap uses over 1500 known operating system fingerprints to determine the host operating system identity, so you can also use Nmap to discover a more specific operating system identity, which reduces the number of vulnerabilities for the host and increases the accuracy of impact correlation for events on the host. You can run Nmap scans as a task, on demand, or in response to a compliance event. If, for example, you want additional information about all the services on a host that just joined your network via a VPN, you could set up a compliance rule that detects when a new host joins that network segment, and create a compliance policy containing that rule which runs the scan as a response. You could then schedule follow-up scans to periodically refresh the information for that host.
- **Extended Flow Summary Support:** You now have the option of aggregating flows (over five-minute intervals) at the sensor level instead of sending all individual flows from 3D Sensors to the Defense Center. This is useful in low-bandwidth environments, and can also reduce the amount of space required to store flow data on the Defense Center.
- **Improved Network Map:** The network map has been improved with respect to its responsiveness and rendering speed. Also, you can now organize the network map and its hierarchy in a way that reflects your actual network construction.
- **Host Input API:** With assistance from Professional Services, you can set up a direct connection to input data into your network map from other applications on your network. For example, if you have a patch management system, you could add information about the patches applied to hosts on your network. The vulnerabilities associated with those patches are then disabled in the host profiles for those hosts, focusing impact correlation on only those vulnerabilities that actually still exist on the hosts. You can set up mappings from the names used for operating systems and services in the imported data to the names used by RNA to ensure that the data can be used for impact correlation.

  You can also create an input file containing data exported from another application that has been reformatted into the specific format required for import. The Host Input API also allows you to directly modify the operating system for a host or delete client applications and protocols through the host profile.
- **Usability Improvements:**

- **Health Monitoring Blacklist**: You can suppress health messages from appliances using blacklisting. In the course of normal network maintenance, you may want to disable appliances or make them temporarily unavailable. Because those outages are typically deliberate, you may not want to receive health events in response to them. You can set a Defense Center or a MMMMDDDDCCCC to disable all or some of theheath events generated by an appliance. For example, if you know that a segment of your network will be unavailable, you can temporarily disable health monitoring for a 3D Sensor on that segment to prevent the Defense Center from generating unnecessary health events related to the lapsed connection to the 3D Sensor.
- **Elimination of Dual Impact Flags:** Prior to Version 4.7, it was possible to see different red impact flags in the dashboard and event views due to different underlying methodologies for calculating impact values. These have been consolidated into a single impact flag.
- **SIDs in Vulnerability Database Table View:** The table view of vulnerabilities now displays the SID (Snort ID) associated with each vulnerability. Deprecation of the RNA Appliance Policy: Key features of the RNA appliance policy have been integrated into the system policy. These include database settings, event logging, and timeout values. In addition, the Combine Flows for Out-Of-Network Responders option appears in the system policy and the RNA detection policy.
- **Right-Click Actions from Event View:** You can right-click at any level of the intrusion event view to edit, enable, disable, suppress, and set thresholds for rules, view rule documentation, and for an inline deployment, set rules to Drop.
- **SEU Import Log:** The Defense Center or 3D Sensor with IPS generates a record for each SEU and local rule file that you import. Each record includes a time stamp, the user who imported the file, and a status icon indicating whether the import succeeded or failed. A detailed view for each imported SEU or local rule file provides information for each imported object, such as rule or SEU component type, rule SID, GID, and revision number, whether a rule is new, modified, or has been deleted from the rule pack, and the default rule state. You can create a custom workflow or report from the records that includes only the information that matches your specific needs, and search the log database for records matching the search criteria.

TPS 2070 Defense Center

The TPS 2070 Defense Center contains the following features and functionality in release 4.7:

- **Improved One-Click Compliance (White Lists)**
  In Version 4.6, Nortel introduced the compliance white list feature, which allows you to specify the operating systems, client applications, services, and protocols that are permitted to run on a specific subnet. You can use white lists to obtain an at-a-glance summary of the compliance of your network; you can also configure your Defense Center to alert you or to launch a remediation when RNA detects that a host is violating the white list.
  Version 4.7 introduces several improvements to the white list feature, including:
  - The ability to manually mark a host as compliant by deleting the attributes that triggered its non-compliant status. You can configure the Defense Center to alert you if RNA detects that the host becomes noncompliant again.
  - Graphs of white list compliance events over time, which allow you to track and demonstrate progress towards compliance goals.
  - Charts that show the percent of hosts in compliance for a specific white listor across all white lists in your deployment.
  - The ability to view the specific attributes that make a given host noncompliant.
- **Usability Improvements:**
  - **Prohibit Packet Transfer to the Defense Center:** Packet data is frequently important for forensic analysis. However in certain jurisdictions it is not permitted to send the details of user packet data across boarders. You can prevent packet data from leaving a sensor by simply checking a check box, for those locations. If you elect to prohibit sending packet data and you do not store events on the sensor, packet data is not retained.

TPS 3D Sensor

- **RNA Recommended Rules**: The system can recommend rule states for your intrusion policies based on RNA service and vulnerability information. You can accept or reject these recommendations and, optionally, exclude specified rules from being considered for state recommendations.
- **New Default IPS Policies**: A new set of Nortel-defined default intrusion policies is provided in SEUs as templates. While you cannot change the default policies, you can copy them and adapt them to your requirements. Current default intrusion policies include:
  - Connectivity Over Security
  - Security Over Connectivity
  - Balanced Security and Connectivity (was Suggested Inline Rules)

- **Latency Threshold**: Latency thresholds give the system administrator the option of balancing security needs with connectivity needs on inline deployments. You can configure IPS to stop inspection of a packet when the inspection time exceeds a user-configurable threshold. You can also configure IPS to suspend a rule in inline deployments for a user-configurable number of seconds when the time the rule takes to process a packet exceeds a user-configurable threshold. You can further specify that the rule be suspended only if the threshold is exceeded a user-configurable number of times.
- **NetFlow Integration:** If your organization uses NetFlow devices to collect IP traffic information, you can use the NetFlow records generated by those devices to supplement the data gathered by RNA. For example, if you have NetFlow devices deployed on networks that your 3D Sensors with RNA cannot see, you can use the data transmitted by those devices to monitor those networks.
- **Custom Service Detection:** When RNA analyzes traffic, it collects information about services used by hosts on your network by detecting service traffic in packets. RNA uses complex service detectors built into RNA to identify service traffic for commonly used services. You cannot create, modify, or delete those built-in service detectors. However, if you have custom services on your network, or if you use non-standard ports for services on your network, you can augment RNA's service detection capabilities by creating simple custom service detectors to provide RNA with the information it needs to identify non-standard services.
  You can base custom service detection on the port used by service traffic, on a pattern within the traffic, or on both the port and the pattern. Each service detector must include at least a port specification or a pattern to match. For example, if you expect traffic for a custom service to use port 1180, you can create a service detector that detects traffic on that port. If you know that the header for any packet containing service traffic has a string of ServiceName in it, you can create a service detector that registers the ASCII string of ServiceName as a pattern to be matched.
- **Real-Time User Awareness:** Nortel 3D Sensors with Real-Time User Awareness (RUA) allow your organization to correlate threat, endpoint, and network intelligence with user identity information. Running as a detection engine on your 3D Sensors but managed by the Defense Center, RUA helps to mitigate risk, block users or user activity, and take action to protect others from disruption-tightening security without hindering business operations or employee productivity by linking network behavior, traffic, and events directly to individual users. These capabilities also significantly improve your audit controls and enhance regulatory compliance.
- **Usability Improvements:**

- **Separate Indication of Blocked Events:** Prior to Version 4.7, a black impact flag in inline IPS mode indicated whether the packet had been dropped displaced other impact flags. Now a separate field indicates whether packets were dropped, so impact flags can always display the correlation between IPS data, RNA data, and vulnerability information.
- **Deprecation of the RNA Appliance Policy:** Key features of the RNA appliance policy have been integrated into the system policy. These include database settings, event logging, and timeout values. In addition, the Combine Flows for Out-Of-Network Responders option appears in the system policy and the RNA detection policy.

General software information

If you are a contracted customer, see the Nortel Support Site for version 4.7.0.5 of the software. Also, see the section How to get help (page 36) for information on TPS 2070 Defense Center and 3D Sensors (TPS 2050 3D , TPS 2070 3D Sensor, TPS 2150 3D Sensor, TPS 2170 3D Sensor, and RNA Sensor) products.

Upgrade files

The software file names for upgrade from version 4.6.0.x to version 4.7.0.x are as follows:

Nortel TPS Defense Center:

- Nortel_TPS_Defense_Center_Upgrade_4.6.0.4_to_4.7.0-376.sh

IMPORTANT! Only operate TPS on software version 4.7.0.2 or later:

The software file name for upgrade from version 4.7.0 to 4.7.0.2 is:

- Nortel_TPS_Defense_Center_Patch_4.7.0_to_4.7.0.2-1022.sh

The software file name for upgrade from version 4.7.0 to 4.7.0.3 is:

- Nortel_TPS_Defense_Center_Patch_4.7.0_to_4.7.0.3-1052.sh

The software file name for upgrade from version 4.7.0 to 4.7.0.4 is:

- Nortel_TPS_Defense_Center_Patch_4.7.0_to_4.7.0.4-1091.sh

The software file name for upgrade from version 4.7.0 to 4.7.0.5 is:

- Nortel_TPS_Defense_Center_Patch_4.7.0_to_4.7.0.5-1109.sh

Nortel TPS 3D Sensor (Intrusion Sensor)

- Nortel_TPS_Intrusion_Sensor_Upgrade_4.6.0.4_to_4.7.0-376.sh

IMPORTANT! Only operate TPS on software version 4.7.0.2 or later:

The software file name for upgrade from version 4.7.0 to 4.7.0.2 is:

- Nortel_TPS_3D_Sensor_Patch_4.7.0_to_4.7.0.2-1022.sh

The software file name for upgrade from version 4.7.0 to 4.7.0.3 is:

- Nortel_TPS_3D_Sensor_Patch_4.7.0_to_4.7.0.3-1052.sh

The software file name for upgrade from version 4.7.0 to 4.7.0.4 is:

- Nortel_TPS_3D_Sensor_Patch_4.7.0_to_4.7.0.4-1091.sh

The software file name for upgrade from version 4.7.0 to 4.7.0.5 is:

- Nortel_TPS_3D_Sensor_Patch_4.7.0_to_4.7.0.5-1109.sh

Nortel TPS 3D Sensor (RNA Sensor)

- Nortel_TPS_Realtime_Threat_Intelligence_Upgrade_4.0.0.2_to_4.7.0-376.sh

IMPORTANT! Only operate TPS on software version 4.7.0.2 or later:

The software file name for upgrade from version 4.7.0 to 4.7.0.2 is:

- Nortel_TPS_3D_Sensor_Patch_4.7.0_to_4.7.0.2-1022.sh

The software file name for upgrade from version 4.7.0 to 4.7.0.3 is:

- Nortel_TPS_3D_Sensor_Patch_4.7.0_to_4.7.0.3-1052.sh

The software file name for upgrade from version 4.7.0 to 4.7.0.4 is:

- Nortel_TPS_3D_Sensor_Patch_4.7.0_to_4.7.0.4-1091.sh

The software file name for upgrade from version 4.7.0 to 4.7.0.5 is:

- Nortel_TPS_3D_Sensor_Patch_4.7.0_to_4.7.0.5-1109.sh

You can upgrade appliances configured with software version 4.5.1.3 directly to version 4.7.

Updating existing appliances and software sensors

The following sections help you prepare for and install version 4.7 on your existing Defense Centers, 3D Sensors, and software sensors.

- Planning the update: Defense Center and 3D Managed Sensors (page 13)
- Updating the Defense Center (page 16)
- Updating 3D Managed Sensors (page 17)
- Updating unmanaged 3D sensors (page 19)
- After updating your appliances (page 22)

IMPORTANT! TPS has to be first upgraded to Release 4.7.0 software before upgrading to Release 4.7.0.5 software. Only operate TPS on software version 4.7.0.2 or later.

NOTE – For information about installing and configuring new appliances, see the installation guide on the Documentation CD that is delivered with your appliance.

Planning the update: Defense Center and 3D Managed Sensors

This section describes planning to update and updating your Defense Center and the managed 3D sensors.

NOTE – The auto update for SEUs and scheduled updates does not work. (Q01856746) For more information see Known issues in TPS Release 4.7.0.5 (page 24).

1.Update the Defense Center first.

Ensure that you update your Defense Centers to version 4.7.0.5 before you update the 3D sensors that they manage. For more information, see Updating the Defense Center (page 16).
Also, after you update the Defense Center, but before you update any 3D Sensors with IPS, you must install the latest SEU on the Defense Center and re-apply intrusion policies to your IPS detection engines.



Warning: You must apply version 4.7.0.5 to the Defense Center before updating the managed 3D sensors so that the patch process does not fail.

2. Make sure your appliances are running the correct version.

To update to version 4.7.0.5, your appliances must run atleast version 4.7.0

If you are running an earlier version, you can obtain updates from the Nortel Support Site.

IMPORTANT! When you upgrade your version 4.0.x RNA Sensors to version 4.7, the RNA web interface is replaced by a more limited interface, and you must manage the sensor with a Defense Center. If you do not currently use a Defense Center to manage your RNA Sensor, please contact your sales representative.

3. Make sure you have enough free disk space and allow enough time for the update
   For appliances with up to 10 million events, the update takes approximately 4.5 hours, so you must plan to perform the update during non-peak hours. If you are not storing events on your sensor, then the upgrade takes approximately 30 minutes.
   The following table provides guidelines for the disk space required for the version 4.7 update:

Table 0-1

Platform	Disk space on /	Disk space on /var
Defense Center	100 MB	1.035 GB
3D Sensor (Intrusion Sensor)	100 MB	760 MB
3D Sensor (RNA Sensor)	100 MB	760 MB

When you update a managed 3D sensor, the update requires additional disk space on the Defense Center's **/var** partition. The following table provides guidelines for the required disk space:

Table 0-2

Managed Sensor or software	Additional Disk space on Defense Center
Intrusion Sensor (v4.6.0.4 and later)	110 MB
RNA Sensor (v4.6.0.2 and later)	110 MB

The following table provides guidelines for the disk space and time required for the Version 4.7.0.5 update:

Table 0-3

Platform	Disk space on /	Disk space on /var	Time
Defense Center	35 MB	330 MB	15 mins
3D Sensor	35 MB	270 MB	15 mins

When you update a managed sensor, the update requires additional disk space on the Defense Center's **/var** partition. The following table provides guidelines for the required disk space:

Table 0-4

Managed Sensor	Software Additional Disk Space on Defense Center
3D Sensor version 4.7.0.4	62 MB

4. Optionally, back up your event and configuration data.
   Although the update process retains event and configuration data, Nortel strongly recommends that you back the data up to a local computer before you perform the update. See your user guide for information about backing up your appliance.

5. Perform the update, as described in Updating the Defense Center (page 16).
   In general, you can monitor its progress in the Defense Center's task queue (**Operations** > **Monitoring** > **Task Status**).

IMPORTANT! When you upgrade a Defense Center that is half of a high availability pair, the Defense Centers in the pair stop sharing configuration information until the second Defense Center is upgraded. You must upgrade both Defense Centers separately.

6. Complete any required post-update steps, as described in section: After updating your appliances (page 22).
   Nortel recommends that you check the Nortel Support Site for the latest SEU and vulnerability database (VDB) update.

7. Update any managed sensors, including software sensors, that you are managing with the Defense Center, as described in Updating 3D Managed Sensors (page 17).

Updating the Defense Center

Updating the Nortel Threat Protection System removes any update prior to version 4.7, their patch scripts, as well as their uninstall scripts from the appliance.



Warning: If you use two Defense Centers as a high availability pair, make sure that they do not have duplicated compliance policies with the same names that you manually created on each Defense Center. Duplicate compliance policies that are not the result of HA propagation will cause the update to fail in a way that is not easy to recover. (38253)

Use the following steps to update a Defense Center:

1.Download the following Nortel TPS version 4.7 Defense Center update script:
Nortel_TPS_Defense_Center_Upgrade_4.6.0.4_to_4.7.0-376.sh
from the Nortel Support Site.
Apply the following patch:
Nortel_TPS_Defense_Center_Patch_4.7.0_to_4.7.0.5-1109.sh

IMPORTANT! Download files directly from the Support Site and do not transfer them by email. If you transfer an update file by email, it may become corrupted.

2. Select **Operations** > **Update**.
The Patch Management Update page appears.

3. Click **Upload Update** to browse to the location where you saved the update script, then click **Upload**.
The update appears in the Updates list.

4. Next to the update you just uploaded, click **Install**.
The Install Update page appears.

5. Under Selected Update, select the Defense Center and click **Install**.

6. Confirm that you want to install the update and reboot the Defense Center. The update is installed and the Defense Center reboots.



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

7. After the update finishes, and the Defense Center reboots, log into the Nortel Threat Protection System.

8. Clear your browser cache and force a reload of the browser. (Otherwise, the user interface may exhibit unexpected behavior.)

9. Select **Operations** > **Help** > **About** and confirm that the software version is listed as version 4.7.0.5.

10. Verify that all managed sensors are successfully communicating with the Defense Center.

11. Continue with the tasks you need to perform after the update. For more information, see After updating your appliances (page 22).

Updating 3D Managed Sensors

You can use the version 4.7.0.5 Defense Center to update versions 4.7.0 and 4.6.0.x managed 3D Sensors (Intrusion Sensors and RNA Sensors).

NOTE – if a managed 3D Sensor uses IPS detection engines with inline interface sets, and the sensor does not have a fail-open network card, traffic is interrupted while the sensor reboots after the update has completed. If the sensor has a failopen network card, some traffic may pass through the sensor uninspected while it reboots.

Before you update managed sensors using the Defense Center, you must:

- update the Defense Center to version 4.7.0.5, making sure to complete any post-update steps, then verify that managed sensors are successfully communicating with the Defense Center
- make sure that the sensors are running the correct version of the software
- make sure that both the Defense Center and the sensors have enough free disk space to perform the update
- make sure that you have set aside adequate time to perform the update

For information on version and disk space requirements for the update, see Planning the update: Defense Center and 3D Managed Sensors (page 13).

Use the following procedure to update managed sensors:

1.Download the appropriate update script from the Nortel Support Site:

- for RNA Sensors
  Nortel_TPS_Realtime_Threat_Intelligence_Upgrade_4.0.0.2_to_4.7.0-376.sh
  Apply the following patch:
  Nortel_TPS_3D_Sensor_Patch_4.7.0_to_4.7.0.5-1109.sh.
- for the 3D Sensor
  Nortel_TPS_Intrusion_Sensor_Upgrade_4.6.0.4_to_4.7.0-376.sh
  Apply the following patch:
  Nortel_TPS_3D_Sensor_Patch_4.7.0_to_4.7.0.5-1109.sh.



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

2. Select **Operations** > **Update**.
   The Patch Update Management page appears.

3. Click **Upload Update** to browse to the update script you downloaded, then click **Upload**.
   The update script is uploaded to the Defense Center.

4. Next to the update script, click **Push**.
   The Push Update page appears.

5. Select the sensors or sensor groups that you want to update.

6. From the **Batch size for this push** list, select the number of sensors where the Defense Center should copy the update script at a time.
   For example, if you have 20 managed sensors to update, you can specify 5 as the batch size to push the updates to 5 sensors at a time, then push to the next 5 sensors.

7. Click **Push**.
   You can monitor the progress of the push in the task queue (**Operations** > **Monitoring** > **Task Status**). When the push is complete, continue with the next step.

8. Next to the update script, click **Install**.
   The Install Update page appears.

9. Select the sensors or sensor groups where you pushed the update script and click **Install**.

10. Confirm that you want to install the update and reboot the sensors.
    The update is installed and the sensors reboot.
    If a managed 3D Sensor uses IPS detection engines with inline interface sets, and the sensor does not have a fail-open network card, traffic is interrupted while the sensor reboots after the update has completed. If the sensor has a fail-open network card, some traffic may pass through the sensor uninspected while it reboots.



Warning: You can monitor the update's progress in the task queue (**Operations** > **Monitoring** > **Task Status**). If the task queue stops updating with current status, manually refresh your browser. If you encounter issues with the update, for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress, do not restart the update. Instead, contact the Nortel Support Site.

11. Select **Operations** > **Sensors** and confirm that the sensors you updated have the correct versions listed (version 4.7.0.5).

Updating unmanaged 3D sensors

The following sections describe updating unmanaged 3D sensors:

- Planning for the Update: Unmanaged or standalone sensors (page 20)
- Updating an unmanaged sensor (page 21)

Planning for the Update: Unmanaged or standalone sensors

Use this procedure to plan for the update of your standalone sensor.

IMPORTANT! A sensor is considered standalone if you do not use a Defense Center to manage it. When you upgrade your version 4.0.0.2 RNA Sensors to version 4.7.0.5, the RNA web interface is replaced by a more limited interface, and you must manage the sensor with a Defense Center. If you do not currently use a Defense Center to manage your RNA Sensor, please contact your sales representative.

1.Make sure your sensors are running the correct version.
To update to version 4.7.0.5, your sensor must be running at least the version specified below.

Table 0-5

Appliance	Minimum version
3D sensors	4.7.0
Intrusion Sensor	4.6.0.4
RNA Sensor (also called the RTI Sensor)	4.0.0.2

If you are running an earlier version, you can obtain updates from the Nortel Support Site.

2. Ensure that you have enough free disk space and allow enough time for the update.
For appliances with up to 10 million events, the update takes approximately 4.5 hours, so you should plan to perform the update during non-peak hours.
The following table provides guidelines for the disk space required for the version 4.7 update.

Table 0-6

Platform	Disk space on /	Disk space on /var
Intrusion Sensor	100 MB	760 MB
RNA Sensor	100 MB	760 MB

The disk space required for the version 4.7.0.5 update is as follows:
For appliances with up to 10 million events, the update takes approximately 15 minutes and requires 35MB on the / partition and 270MB on the **/var** partition.

3. Optionally, back up your event and configuration data.
   Although the update process retains event and configuration data, Nortel strongly recommends that you back the data up to a local computer before you perform the update. See your user guide for information about backing up your appliance.

4. Perform the update, as described in Updating unmanaged 3D sensors (page 19).
   In general, you can monitor its progress in the sensor's task queue (**Operations** > **Monitoring** > **Task Status**).

5. Complete any required post-update steps, as described in After updating your appliances (page 22).
   Nortel recommends that you check the Support web site for the latest SEU and vulnerability database (VDB) updates.

Updating an unmanaged sensor

You can update an unmanaged 3D Sensor (Intrusion Sensor or RNA Sensor) to version 4.7.0.5.

IMPORTANT! When you upgrade your version 4.0.x RNA Sensor 3D sensors to version 4.7.0.5, the RNA web interface is replaced by a more limited interface, and you must manage the sensor with a Defense Center. If you do not currently use a Defense Center to manage your RNA Sensor, please contact your sales representative.

NOTE – Updating the Nortel Threat Protection System removes any pre-version 4.7 update and patch scripts, as well as their uninstall scripts, from the appliance.

Use the following procedure to update a standalone 3D sensor.

1.Download the following Nortel TPS version 4.7 update script:
   Nortel_TPS_Intrusion_Sensor_Upgrade_4.6.0.4_to_4.7.0-376.sh
   from the Nortel Support Site.
   Also download the following Nortel TPS version 4.7.0.5 patch update script:
   Nortel_TPS_3D_Sensor_Patch_4.7.0_to_4.7.0.5-1109.sh

IMPORTANT! Download files directly from the Nortel Support Site and do not transfer them by email. If you transfer an update file by email, it may become corrupted.

2. Select **Operations** > **Update**.
   The Patch Management Update page appears.

3. Click **Upload Update** to browse to the location where you saved the update script, then click **Upload**.
   The update appears in the Updates list.

4. Next to the update you just uploaded, click **Install**.

5. Confirm that you want to install the update and reboot the 3D Sensor.
   The update is installed and the 3D Sensor reboots.

IMPORTANT! You can monitor the update's progress in the task queue (Operations > Monitoring > Task Status). Do not use the web interface to perform any other tasks until the update has completed and the 3D Sensor reboots. Note that before the update completes, the 3D Sensor may log you out. If this occurs, log in to the appliance and view the task queue. If the update is still running, continue to refrain from using the web interface until the update has completed. If the task queue stops updating with current status, manually refresh your browser. If you encounter issues with the update, for example, if the task queue indicates that the update has failed or if a manual refresh of the task queue shows no progress, do not restart the update. Instead, contact the Nortel Technical Support.

6. After the update finishes, and the 3D Sensor reboots, log into the 3D Sensor.

7. Clear your browser cache and force a reload of the browser. (Otherwise, the user interface may exhibit unexpected behavior).

8. Select **Operations > Help > About** and confirm that the software version is listed as version 4.7.0.5.

9. Continue with the tasks described in After updating your appliances (page 22).

After updating your appliances

After you complete the update, you must:

- Install any patches or updates to the Nortel Threat Protection System that are available on the Nortel Technical Support.
- Install the latest SEU and reapply intrusion policies to any IPS detection engines.

IMPORTANT! Applying an intrusion policy causes IPS detection engines to restart, which may cause a short pause in processing and for most detection engines with inline interface sets, may cause a few packets to pass through the sensor uninspected.

- Install the latest vulnerability database (VDB), then push and install the VDB update on any managed 3D Sensor with RNA.

For more information, refer to the Nortel Threat Protection System User Guide.

Uninstalling the update

Uninstalling the update results in an appliance running version 4.7.0.4. For information on uninstalling version 4.7.0.4, refer to the release notes for that version.
You cannot use the Defense Center to uninstall the update from managed sensors. Instead, you must use the sensor's web interface to uninstall the update.

IMPORTANT! If your IPS detection engines are deployed inline and your 3D Sensor does not have a fail-open network card, traffic is interrupted while the sensor reboots after the uninstallation has completed. If your 3D Sensor has a fail-open network card, some traffic may pass through the sensor uninspected while it reboots.

Use the following procedure to uninstall the update from the appliance:

1. Select **Operations** > **Update**.
   The Patch Management Update page appears.

2. Next to the uninstaller that matches the update you want to remove, click **Install**.
   On the Defense Center, the **Install Update** page appears.

3. Under Selected Update, select the Defense Center and click **Install**.
   On the 3D Sensor, there is no intervening page.

4. Confirm that you want to uninstall the update.
   The update is removed and returns to Version 4.7.0.4.



Warning: You can monitor the uninstallation progress in the task queue (**Operations** > **Monitoring** > **Task Status**). If the task queue stops updating with current status, manually refresh your browser. If you encounter issues with the uninstallation, for example, if the task queue indicates that the uninstallation has failed or if a manual refresh of the task queue shows no progress, do not restart the uninstallation. Instead, contact Nortel Technical Support.

5. Select **Operations** > **Help** > **About** after the uninstall finishes, and confirm that the software version is listed as Version 4.7.0.4.

Issues resolved in TPS Release 4.7.0.5

The following sections describe the issues resolved in TPS Release 4.7.0.5.

- Issues resolved in both Defense Center and 3D sensors in Release 4.7.0.5 (page 24)

Issues resolved in both Defense Center and 3D sensors in Release 4.7.0.5

Version 4.7.0.5 includes updated online help which addresses several documentation issues.

- Addressed an issue so that host search results containing the Last Seen field are constrained properly. (41660)
- Added a process to free disk space by pruning previously processed RNA-related files that have already been backed up and are no longer needed. (42072)
- Fixed an issue that caused search constraints to be lost when you viewed different pages within a custom workflow. (42698)
- Added a check so that if you delete a compliance white list, all the associated white list violations are also deleted. (42820)
- Updated the documentation to include improved instructions for using RUA authentication objects. (43270)

Known issues in TPS Release 4.7.0.5

The following sections describe the known issues in TPS Release 4.7.0.5:

- Known issues in Defense Center (page 26)
- Known issues in 3D Sensor (page 30)

The following known issues are common to both Defense Center and 3D sensors:

- The auto update for SEUs and scheduled updates does not work. When you click on the “Update” button, you get the following message:
“AutoUpdate failed: No valid support contract found. Contact sales or the Nortel Support Site for more information”. (Q01856746)
- Usability: “Run All Modules” under “Alert Details” doesn't start all the modules in the Health Monitor Appliance page. (37347)
- When the DR count is increased or decreased on an Inline DE, traffic is allowed for droped rule and vice versa. (38544)

- Issues with NAS Remediation. (38801)
- Unable to delete the license when trying to delete it from the currently existing license page. (38061)
- Allows to add duplicate network in Custom topology. (36171)
- Backup log file size rounded off when in MB range from Unified File List on the Backup/Restore. (36875)
- Unwanted Home Page Preferences should be removed from SDM-IS GUI and need to have only the Operations menu options as the Home Page Preferences. (37794)
- The job name is displaying the first 5 letters when the status of the task is lengthy. (38950)
- The RUA is not detecting the MSAD user name which consist of a $. (38859)
- Duplicate configuration for client applications, services and protocols are allowed for the allowed host profiles in the white list. (38951)
- When SEU Import log is selected as Report type , the report section is not changed accordingly in the Report designer page.(37764)
- Nortel SDM installation output should not go to serial. (37218)
- TPS-4.7.0 installation output redirects to serial and not to the console.(34871)
- Interface Set lists management and NAAP interface of SDM. (38460)
- Task status displays upgrade failed when doing a complete upgrade on IS 2x50. (39800)
- In Estreamer/Visualizer client, when we right click the node and select "host info in browser" it takes to 404 error : page cannot be found. (39608)
- NMAP Remediation “Port Ranges and Scan Order” field does not accept Ports in format “T:230-25 or U:51,53”. (38945)
- RNA appliance policy created in 4.6.0 is appearing in import/export page after upgraded from 4.6.0.4 to 4.7.0 - 336. (37474)
- No way to downgrade SDM-IS reduced GUI from 4.7.0.2-1022 (40015)
- Add USER_CONF variable gives snort validation failed error in 4.7.0.2 - 1022 build. (40031)
- Add SNORT_CONF variable gives snort validation failed error when DC and IS are upgraded from 4.1.0 to 4.7.0.2-1022. (40032)
- Flow Summary page does not provide activity graphs on the monitored network. (41372)
- Traffic Profile - Graph display blank. (41374)
- Report is not created for RNA Flow Data. (41375)

Known issues in Defense Center

The following is the list of known issues for the Defense Center.

- If you create a custom rule classification and use it in a local intrusion rule on an Intrusion Sensor, then import that rule on a Defense Center through the System Settings - Object Import page for the sensor, the rule classification does not import and an existing classification is automatically assigned to the rule instead. As a workaround, you can import the custom classification on the Defense Center prior to importing the rule. You could also use the **Operations > Tools > Import/Export** feature to export an intrusion policy where the rule is enabled and then import the rule (and the rule classification) to the Defense Center from the exported package. (26024, 30604)
- 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 import a rules file that includes rules with actions other than alert or pass, or that includes comments that begin with the word alert, pass, or include. (30746)
- If you back up the system for a Defense Center in a High Availability pair, then modify and apply a health policy from the Defense Center to a managed sensor, and then restore the system to the Defense Center, the name of the health policy appears in italics on the Sensors page, indicating incorrectly that the policy has been updated since it was last applied. Clicking on the policy name displays the outdated policy. You can reapply the policy to restore the non-italicized policy name and display the correct policy when you click on the policy name. (30920)
- You cannot schedule installation of a VDB update from an RTI Sensor. You must install the update manually. For a managed sensor, you can schedule VDB update installation from the managing Defense Center. (31045)
- When you view intrusion events, a browser issue that is beyond the control of Nortel might result in an unusable Open in New Window link at the bottom of the page. (31754)
- The table view of intrusion events can get in a mode where constraining to the packet view, then using the browser Back button, and then selecting the down arrow next to an event might lead to a blank packet view. To avoid this, use the links at the top of the page instead of the Back button. (31906)
- The Transparent Inline Mode check box clears if you select it when editing an inline interface set and then click either the left or right arrow button between the Available Interfaces and Selected Interfaces lists. (32171)
- For inline interface sets, but not Inline with Fail Open interface sets, the Number of Interfaces column on the Interface Sets page might list 1 instead of 1 pair. (32172)

- 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 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 Defense Center topic. (32372)
- If you apply a system policy to a managed Nortel SDM server and that policy has Via NTP from this Defense Center as the Set My Clock setting, NTP traffic is sent across unsecured network channels rather than through the secured communications tunnel and NTP does not work. This occurs because the managed SDM server is unable to resolve the Defense Center IP address. As a workaround, use the Via NTP from host option instead and specify the Defense Center IP address. (32553)
- After you restore an Intrusion Sensor backup, you must reboot the Intrusion Sensor to complete the restoration. (32583)
- The page shows "Error 500: Internal Server Error" when a misconfiguration is saved. (32409)
- Error message will appear when editing a policy to enable Opsec Sam even when operation is successful. (25873)
- When running large reports the GUI can hang due to high use of resources. (20491)
- After a backup and restore, there maybe a memory allocation issue when Detection Engines are configured from multiple management stations. (32667)
- Suppression page shows "Error 500:Internal Server Error" , when adding to a custom rule. (32824)
- Nessus 3.0 is not supported. (32823)
- There is no help for "Threshold", "Suppression" and "Rule State". (32670)
- SEU: Impossible to push SEU patch from DC to its IS. (31058)
- Currently there is no way to tell the Synchronization between rules from DC and IS. (32189)
- After installing new software to the Intrusion Sensor or Defense Center, the console asks to reboot the system rather than rebooting automatically. (32403)

Known issues identified in Defense Center prior to Release 4.7

- 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. As a workaround, check the task queue to make sure that each policy is successfully applied before you attempt to apply a new policy of the same type. (16849)
- 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 Defense Center, rather than the timestamps of the events used to build the report. (21215)
- The Defense Center will not email a copy of a report you have run remotely. (23679)
- Depending on the time zone setting on your Defense Center, 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 Defense Center 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 Defense Center for the new IP address to be accessible. (25253)
- If you have a large number of events stored on your Defense Center for the current time range, the dashboard may load slowly. (26703)
- On the Events by Impact graph in the dashboard, the Defense Center may display two bars for the red impact flag. To determine the total number of events with the red impact flag, combine the number of events from both bars. (26712, 30414)
- If you start the local Nessus server on the Defense Center, 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)
- If you delete a sensor from the Defense Center, you must use the Task Status (Operations > Monitoring > Task Status) page to manually delete any tasks that were running at the time of deletion. (27260)
- If you disable high availability between two Defense Centers, and then re-establish it, any traffic profiles, custom compliance rules, and custom compliance policies are duplicated on both Defense Centers. (27498)

- When you view an IDS event graph on your Defense Center, days containing fewer than 24 hours may not appear on the Analysis & Reporting > Event Summary > Event Graphs page. For example, in time zones that observe Daylight Savings Time, April 2, 2006 has only 23 hours because Daylight Savings Time began on the 2nd (and an hour was removed from the day by the time change). As a workaround, to view events from a time frame affected by this issue, change the time zone for your web interface to a different time zone. (28249)
- Scheduled SEU imports do not appear in the task queue. Also, the Defense Center does not notify you of scheduled SEU imports, even if you have configured it to notify you. (27144)
- 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 Defense Center (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)
- In the system policy for a Defense Center, you can configure the Health Alerts Database setting to allow up to 10,000,000 health events to accumulate in the database. However, Nortel strongly recommends that you set the limit to an amount less than or equal to the default of 100,000; higher settings may cause degradation of performance on your Defense Center. (30724)
- If you have different SEU versions on the Defense Center and the Intrusion Sensor, the web interface on the appliance with the older SEU does not display any new IDS rule categories when you are remotely viewing the (read-only) intrusion policy applied to the appliance with the newer SEU. Make sure that your appliances use the same SEU. (28569)
- If you schedule download of an SEU on a Defense Center and it fails, the task status incorrectly indicates successful completion of the download and you receive email notification of the task completion. Check /var/sf/SEU/ to see if the SEU exists on the Defense Center. (32133)
- When you disable a registered sensor on a Defense Center, health alerts for the sensor indicate that the Defense Center is not receiving heartbeats from the sensor, rather than showing a disabled status for the sensor. (32384)

Known issues in 3D Sensor

The following list contains the known issues for 3D Sensors (Intrusion Sensors and RNA Sensors).

- If you create a custom rule classification and use it in a local intrusion rule on an Intrusion Sensor, then import that rule on a Defense Center through the System Settings - Object Import page for the sensor, the rule classification does not import and an existing classification is automatically assigned to the rule instead. As a workaround, you can import the custom classification on the Defense Center prior to importing the rule. You could also use the Operations > Tools > Import/Export feature to export an intrusion policy where the rule is enabled and then import the rule (and the rule classification) to the Defense Center from the exported package. (26024, 30604)
- 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 import a rules file that includes rules with actions other than alert or pass, or that includes comments that begin with the word alert, pass, or include. (30746)
- When you view intrusion events, a browser issue that is beyond the control of Nortel might result in an unusable Open in New Window link at the bottom of the page. (31754)
- The table view of intrusion events can get in a mode where constraining to the packet view, then using the browser Back button, and then selecting the down arrow next to an event might lead to a blank packet view. To avoid this, use the links at the top of the page instead of the Back button. (31906)
- The Transparent Inline Mode check box clears if you select it when editing an inline interface set and then click either the left or right arrow button between the Available Interfaces and Selected Interfaces lists. (32171)
- For inline interface sets, but not Inline with Fail Open interface sets, the Number of Interfaces column on the Interface Sets page might list 1 instead of 1 pair. (32172)
- The White List Events table type is not a valid type when creating a custom workflow for an Intrusion Sensor. (32246)
- 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 Intrusion Sensor topic. (32372)
- After you restore an Intrusion Sensor backup, you must reboot the Intrusion Sensor to complete the restoration. (32583)

- The page shows "Error 500: Internal Server Error" when a misconfiguration is saved. (32409)
- Error message will appear when editing a policy to enable Opsec Sam even when operation is successful. (25873)
- When running large reports the GUI can hang due to high use of resources.(20491)
- After a backup and restore, there may be a memory allocation issue when Detection Engines are configured from multiple management stations. (32667)
- Suppression page shows "Error 500:Internal Server Error" , when adding to a custom rule. (32824)
- Nessus 3.0 is not supported. (32823)
- There is no help for "Threshold", "Suppression" and "Rule State". (32670)
- SEU: Impossible to push SEU patch from DC to its IS. (31058)
- Currently there is no way to tell the Synchronization between rules from DC and IS. (32189)
- After installing new software to the Intrusion Sensor or Defense Center, the console asks to reboot the system rather than rebooting automatically. (32403)

Known Issues in 3D sensors identified prior to Release 4.7

The following open issues were identified in versions prior to Release 4.7:

- In the Intrusion Sensor rule editor, if you try to save a rule that contains a syntax error, an error message appears. The contents of the rule editor are cleared and you must re-create the rule from the beginning. (11488)
- 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 for assistance. (13712)
- When you generate a report containing intrusion events, the underlying source (and destination) port query does not include event protocol. As a result, the report lists ICMP ports as source ports and combines UDP and TCP source port counts into a single result. (21060)
- 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 Intrusion Sensor, rather than the timestamps of the events used to build the report. (21215)
- If you create receive intrusion alerts more frequently than you should given the Max Alerts and Frequency settings, contact Nortel Support for assistance. (22883)

- Depending on the time zone setting on your Intrusion 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 Intrusion 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 Intrusion 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)
- Sometimes, tasks in the task queue are incorrectly nested. (26886, 27327)
- If you are not logged in as the admin user, jobs created by other users may not be visible. (26910)
- 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)
- Scheduled SEU imports do not appear in the task queue. Also, the Defense Center does not notify you of scheduled SEU imports, even if you have configured it to notify you. (27144)
- 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 Save and Add buttons in the subpages of read-only intrusion policies (that is, policies that were not authored by or imported onto the local appliance) have no effect. (27201)
- Scheduling an update of the vulnerability database has no effect, because the Intrusion Sensor has no vulnerability database. (27217)
- The Back button in Firefox does not always take you back to the previous page. As a workaround, use the menu structure. (27256)
- 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, contact Nortel Support. (28508)

- If you have different SEU versions on the Defense Center and the Intrusion Sensor, the web interface on the appliance with the older SEU does not display any new IDS rule categories when you are remotely viewing the (read-only) intrusion policy applied to the appliance with the newer SEU. Make sure that your appliances use the same SEU. (28569)
- 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)
- In the Intrusion Sensor rule editor, if you try to save a rule that contains a syntax error, an error message appears. The contents of the rule editor are cleared and you must re-create the rule from the beginning. (11488)
- 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 generate a report containing intrusion events, the underlying source (and destination) port query does not include event protocol. As a result, the report lists ICMP ports as source ports and combines UDP and TCP source port counts into a single result. (21060)
- If you create receive intrusion alerts more frequently than you should given the Max Alerts and Frequency settings, contact Nortel Support for assistance. (22883)
- 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)
- 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)
- In health alerts, the severity of the health event is reported by color instead of severity level. The alerts report Red (Critical), Yellow (Warning), Green (Normal), Blue (Disabled) and Gray (Error). (27026)

- 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)
- Scheduled SEU imports do not appear in the task queue. Also, the Defense Center does not notify you of scheduled SEU imports, even if you have configured it to notify you. (27144)
- 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 Save and Add buttons in the subpages of read-only intrusion policies (that is, policies that were not authored by or imported onto the local appliance) have no effect. (27201)
- Scheduling an update of the vulnerability database has no effect, because the Intrusion Sensor has no vulnerability database. (27217)
- 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, 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)
- RNA host reports based on custom workflows may have data sorted in descending order rather than ascending order. (31567)

Hardware installation

Warning: Prior to hardware installation, ensure that you check for product compatibility. See section "Product Compatibility" on page 5 for more information.

There is no new hardware for Release 4.7.0.5 but TPS is supported on the Ethernet Routing Switch 8600 Release 4.1 Service Delivery Module.

Defense Center

There is no new hardware for the Defense Center for release 4.7.0.5.

3D Sensors

There is no new hardware for the 3D Sensors (Intrusion Sensors and RNA Sensors) for release 4.7.0.5.

Related publications

These release notes supplement the following documents:

- *Intrusion Sensor User Guide* Release 4.6 (Part Number 216884-E)
- *Defense Center User Guide* Release 4.6 (Part Number 216886-E)
- *Real-time Threat Intelligence User Guide Release 4.0* (Part Number 320722-C)
- *Real-Time Threat Intelligence Sensor Visualizer User Guide Release 3.0* (Part Number 322255-A)
- *Real-time Threat Intelligence Sensors 4.0 Release Notes* (Part Number 320741-C)
- *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 3.1 (Part Number 320739-A)

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:

Link to	Takes you directly to the:
Latest software	Nortel page for software located at www.nortel.com
Latest documentation	Nortel page for documentation located at www.nortel.com

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

If you have any questions or require assistance with the Nortel Defense Center or 3D sensors (Intrusion Sensor, RNA Sensor, or any of the software sensors), contact Nortel Support.

- Visit the Nortel Support Site.
- Email Nortel Support at support@nortel.com.

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.

Nortel Threat Protection System Release Notes
Nortel Threat Protection System

Copyright © 2008 Nortel Networks. All Rights Reserved.

Release: 4.7.0.5
Document Number: NN47240-400
Document status: Standard
Document Version: Version 01.04
Document release date: July 2008

To provide feedback, or to report a problem in this document, go to www.nortel.com/documentfeedback.

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.

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

All other trademarks and registered trademarks are the property of their respective owners.

NORTEL