Part No. 320740-B
May 2006

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

Release Notes for Nortel Threat Protection System Release 4.5.1

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

Contents

Introduction

This document contains the latest information about the Nortel Threat Protection System (TPS) Release 4.5.1.

The Nortel Threat Protection System is a fully integrated intrusion detection system that consists of the following:

- TPS 2070 Defense Center, which manages intrusion sensors in the network environment.
- TPS 2050 Intrusion Sensor and TPS 2070 Intrusion Sensor, which detect and track network intrusions, either independently or under the management of the TPS 2070 Defense Center.
- TPS 2150 Intrusion Sensor and TPS 2170 Intrusion Sensor, which deliver fail-open functionality in Inline mode.
- Ethernet Routing Switch 8600 Release 4.1, which supports the Service Delivery Module (SDM) that includes Threat Protection System (TPS) Release 4.5.1. In this configuration, TPS enables audit and alert functions independent of all other security devices deployed on a network.

For the latest information about Real-time Threat Intelligence Sensors, see *Real-time Threat Intelligence Sensors 3.5.1 Release Notes*, part number 320741-B.

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
4.5.1	4.5.1	3.5.1
4.1	4.1	3.1

Hardware installation

There is no new hardware for Release 4.5.1 but TPS is supported on the Ethernet Routing Switch 8600 Release 4.1 Service Delivery Module.

General software information

Version 4.5.1 software, for contracted customers, is available on the Nortel web site; see How to get help (page 56) for the TPS 2070 Defense Center, TPS 2050 Intrusion Sensor, TPS 2070 Intrusion Sensor, TPS 2150 Intrusion Sensor, and TPS 2170 Intrusion Sensor products.

Upgrade files

The software file names for upgrade from version 4.1.0.2 to version 4.5.1 are as follows:

- Nortel_TPS_Defense_Center_Upgrade_4.1.0.2_to_4.5.1_Upgrade-47.sh
- Nortel_TPS_Intrusion_Sensor_Upgrade_4.1.0.2_to_4.5.1_Upgrade-47.sh

You can upgrade appliances configured with software version 4.1.0.2 directly to version 4.5.1.

Restoration

If appliances running version 4.5.1 software require restoration, you must do the following:

1. Obtain the TPS 4.1.0 restore iso files located on the Nortel Web site. See Getting help from the Nortel web site (page 56).
2. Apply the version 4.1.0.2 patch.
3. Apply the upgrade to version 4.5.1 file .

Restore iso files

The version 4.1.0 restore iso files available at time of publication are:

- Nortel_TPS_Defense_Center_2070_v4.1.0-78-Restore.iso (TPS 2070 Defense Center)
- Nortel_TPS_Intrusion_Sensor-2050-v4.1.0-78-Restore.iso (TPS 2050 Intrusion Sensor and TPS 2150 Intrusion Sensor)
- Nortel_TPS_Intrusion_Sensor-2070-v4.1.0-78-Restore.iso (TPS 2070 Intrusion Sensor and TPS 2170 Intrusion Sensor)
- Nortel_TPS_Intrusion_Sensor-SDM-v4.1.0-78-Restore.iso

Updating software

Updates for the Defense Center and Intrusion Sensor software are distributed electronically and can be downloaded from the Nortel web site for contracted customers only. Refer to the Defense Center and Intrusion Sensor User Guides for complete instructions on performing this task.. The titles and part numbers of the user guides are as follows:

- *Nortel* TPS 2070 Defense Center *User Guide,* part number 216886-D
- *Nortel Intrusion Sensor User Guide for Release 4.5.1,* part number 216884-D)
- *Nortel Real-Time Threat Intelligence Sensor Visualizer User Guide Release 3.0*, part number 322255-A

Updating intrusion rule packs and SEUs

New intrusion rule packs and Snort Engine Update (SEU) Rule Packs are occasionally made available to update existing rule packs and SEUs. New rule packs and SEUs can be downloaded from the Nortel web site under the Threat Protection System product family. The update service is provided only to customers with valid service contracts.

Auto-Update is not supported in Release 4.5.1.

Features and functionality – TPS 2070 Defense Center

The TPS 2070 Defense Center contains the following features and functionality in release 4.5.1:

- Improved Real-time Threat Intelligence (RTI) Visualizer: The enhanced RTI Visualizer represents up to 8000 concurrent devices and provides faster system manipulation. Nortel Real-time Threat Intelligence Visualizer (RTI Visualizer) is a client-side application that generates a three-dimensional (3D) model of your network architecture based on accumulated RTI data and, when using an Event Streamer connection to a Defense Center, updates to reflect real-time variations to your network, such as IDS impact changes and policy violation events. For more information about the Real-Time Threat Intelligence Sensor Visualizer, see *Real-Time Threat Intelligence Sensor Visualizer User Guide Release 3.0*, part number 322255-A, and *Threat Protection System Release 4.5.1 Defense Center User Guide*, part number 216886-D.
- End Point Intelligence, Nessus Integration: The Nessus Active Scanner provides enhanced resolution of the RTI vulnerability database. The additional vulnerabilities provided by the Nessus Active Scanner can be added to a host record and leveraged for Impact Flag calculation. The Nessus vulnerabilities list can be added alone or in combination with the RTI list. Nessus scans can be initiated by a remediation module or on demand. Basic scans focussed against a range of IP addresses can be performed to provoke a response from hosts before they are completely profiled or discovered by RTI. Subsequent targeted scan responses can be detected by RTI to enhance the network map. Scan data obtained outside of the TPS system can be loaded directly into RTI.
- User Defined Host Attributes: New information can be added to an RTI host record. The new customer fields can contain numbers, text, or URLs. The data in the new customer fields can also be used as host qualifiers, used to build rules in the Policy and Response. Customer fields can include location, name of IT manager, and phone number. Lists can be created, composed from the customer fields, that are controlled by a pre-defined list of options.
- NETBIOS Names in Host Profiles: NetBIOS information is included in the RTI host records.
- Traffic Profiling: Create traffic profiles for any host, group of hosts, subnet, or network. Configure rules to generate alerts and remediations as traffic conditions change. Configure the degree of change required to trigger rules. Configuration options include changes in standard deviations or an absolute number. Use traffic profiles in compliance policy rules to respond to traffic profile changes.

- Flow Data Visualization: Display flow data metrics on charts and graphs. Analyze traffic patterns and composition for trend analysis. Use the pre-defined charts or modify and customize graphs to change data ranges. Pre-defined charts include: Top 10 Initiators by number of flows and Top 10 Initiators by amount of traffic sent. Pie charts that show the mix of services comprising traffic are also included.
- Flow Tracker: Add flow trackers as an element of compliance policy rules. Track flow data when an Intrusion Sensor or RTI flow data event occurs.
- Improved Policy and Response: Policy and Response has been enhanced to provide inclusion of flow data events in Compliance Policy rules, grouping of rules, improved precedence operations, bucketizing of event types, change request fixes for Intrusion Sensor events, improved flow for creating rules, policies, and responses, and client data and user-defined attributes.
- Graphical User Interface (GUI) enhancements: The GUI contains a reorganized menu, and new icons and tools bars that provide improved navigation.
- Custom combined tableviews: Analyze information and create reports for Intrusion Sensors and RTI data together; including host criticality with Intrusion Sensors (IS), Intrusion Sensor events with flow data, and RTI host data with RTI service data.
- Improved backup and restore: Perform remote backups and refine the information selected for backup and restore. Use Task Scheduler, with configurable e-mail notifications, to schedule backups.
- Enterprise Policy and Metadata Synchronization: Synchronize changes made on an Intrusion Sensor with the Defense Center.
- Improved grouping of sensors: Group and view sensors by type, either RTI or IS.
- Sensor Apply and Sensor Screen enhancements: The replacement of the linear list provides more efficient scaling of devices.
- Variable Objects (Extension of Reusable Objects): Use Variable Objects, including global, policy, and sensor-specific, to create intrusion policies that accommodate larger deployments.
- Health Monitoring: Health monitoring is supported on the Defense Center but health policies can be applied from the Defense Center to Intrusion Sensors.
- Improved sensor management: All sensor management menus are accessible from the Defense Center.
- High Availability (HA) improvements: Pause a Defense Center in an HA pair. Reverse management by a second DC in an HA pair without restarting. Synchronizes HA pairs on demand.
- Data driven configuration screens: Add new detection capabilities and policy menus without performing an upgrade or implementing a patch.

- Improved error and success feedback: Backup and restore feedback is enhanced in Release 4.5.1.
- Enhanced decoders : Release 4.5.1 provides new pre-processors for SMTP, FTP, and Telnet.
- *OPSEC: OPSEC debug logging on the sensor is available from the console. The OPSEC debug logging feature is disabled by default.
- Multiple detection engines and policies: One sensor can run multiple Snort instances associated with a named detection engine which can be associated with one or more interfaces. You can configure multiple policies on the same sensor to determine the interface where an event is detected.

Upgrading an existing Defense Center

Table 1 lists the sections that provide important information about the upgrade process:

Table 1 Upgrade information

Section name	Page
Prerequisites for upgrading an existing Defense Center	10
Notes on the upgrade process	11
Upgrading a Defense Center from version 4.1.0.2 to version 4.5.1	15

For upgrade and uninstall procedures for the Defense Center, see *Nortel TPS Defense Center User Guide for Release 4.5.1,* part number 216886-D.

For upgrade and uninstall procedures for the Intrusion Sensors, see *Nortel Intrusion Sensor User Guide for Release 4.5.1,* part number 216884-D.

Prerequisites for upgrading an existing Defense Center

You must meet the following prerequisites to successfully upgrade an existing Defense Center.

- Defense Center version 4.1.0.2 is required to complete a successful upgrade to version 4.5.1. For earlier Defense Center versions you must upgrade from version 3.2 to version 4.1.0.2 before you can successfully upgrade to version 4.5.1.
- At least 32 Mb of free space is required on the root partition (/), and 97 Mb of free space is required on the /var partition.

- For Defense Centers managing Intrusion Sensors, check the sensor management page and confirm that each sensor uses a policy that the Defense Center can identify. Any policy listed as unknown must be replaced with a policy pushed from the Defense Center to the sensor before either appliance is upgraded.

IMPORTANT! Upgrade all Defense Centers before upgrading the sensors managed by the Defense Centers.

Notes on the upgrade process

This section contains important information about upgrading Nortel products. Read the entire section before starting any upgrades.

IMPORTANT! The upgrade process migrates all event and configuration data to a replacement database.

Before you begin the upgrade

- Plan the upgrade for a time when it has the least impact on your deployment because the Defense Center reboots after upgrade.
- Nortel recommends that you back up event and configuration data to a local computer.
- Delete any user-created files from /root before starting the upgrade.
- From the Nortel support site at www.nortel.com/support, obtain the upgrade software file called Nortel_TPS_Defense_Center_Upgrade_4.1.0.2_to_4.5.1._Upgrade-47.sh.

Additional upgrade notes

- Do not perform any administrative or analysis tasks during the upgrade process.
- After completion of the Defense Center upgrade, use the scheduling feature to schedule the upgrade push and installation on managed sensors. Nortel recommends that you upgrade your sensors as soon as possible after the Defense Center upgrade. For information about the scheduling feature, see the Defense Center, see the *Nortel TPS Defense Center User Guide for Release 4.5.1* (Part Number 216886-D).
- If a managed sensor upgrade process fails, it automatically restarts when using a Defense Center to push and install the upgrade. To cancel the upgrade process, click the **Cancel** button on the Task Queue page.

- To determine whether the upgrade installation is successful, view the Sensor Management page. If the version number of the sensor changes, the remote installation succeeded. Upgrade automatically reboots the sensors at the end of the upgrade process, and the Task Queue page can display a Remote Install Failed message, even in the case of a successful installation.
- If the upgrade halts for any reason, it can be restarted at the point where it stopped because the upgrade tracks its own progress. For example, in the event of a power failure during upgrade, the installation process can be restarted using the GUI. If the upgrade proceeded past the point where the GUI is accessible, edit the /etc/sf/ims.conf file and modify the SWVERSION to match the version being upgraded. For Defense Centers, this is version 4.5.1. However, if an upgrade halts for any reason, Nortel recommends that you contact Nortel Technical Support.
- The upgrade Revert feature permits restoration of an upgraded appliance to the previously-installed software version. Before using the Revert feature, the Revert process checks to ensure that there is enough free space on the hard drive to complete the task. At least 50% of the size of the event and upgrade data is required. To revert to the previous software version, log on to the Defense Center using secure shell (SSH) with the root account and type **`revert`** at the command prompt. Press **Enter**. Intrusion events in the database are not retained and RTI events generated between the upgrade and reversion are not retained. Nortel recommends that you back up all event and configuration data on a local computer before performing Revert on a Defense Center and restore events from the backup file after the reversion is complete.
- The upgrade can take several hours, depending on the number of events on the appliance, particularly on Defense Centers and the TPS 2070 IS sensor. Refresh the browser to check the status of the upgrade. When the upgrade is complete, a prompt appears instructing the user to log on to the appliance.
- When the upgrade is installed and the Defense Center is running, the new database starts to populate with old events. The population time can vary from 20 minutes, for 1 million intrusion events, to four hours for 10 million events, to 14 hours for 110 million events. Packet data is migrated after event data. You are unable to view packets associated with events until the migration is complete.
- Policy violation events generated on a version 4.5.1 secondary Defense Center, configured with custom compliance policies and rules, are identified by a number in the policy and rule columns, rather than a name, when both Defense Centers in a high availability pair are upgraded. All events generated after the upgrade exhibit the correct policy name and rule name.

- If you use the Defense Center to upgrade your Intrusion Sensors, the upgrade can interrupt traffic for up to five minutes if your Intrusion Sensor is deployed inline. Once the upgrade is complete, the Defense Center applies an updated intrusion policy to the sensors and restarts Snort. This causes an additional five to ten second interruption in traffic if your Intrusion Sensor is deployed inline.
- In Release 4.5.1, all communications between the Defense Center and its managed sensors are conducted through a single port: 8305/tcp. In previous versions, the Defense Center used a range of ports (8300/tcp through 8303/tcp) to communicate with managed sensors. If you have set up access control lists to allow traffic on these ports, you must change the access list to allow traffic on 8305/tcp. Note that an upgraded Defense Center continues to use 8300/tcp through 8303/tcp to manage sensors that are not upgraded.
- Intrusion Sensor load balancing is not supported in Release 4.5.1. If you have Intrusion Sensors in a load-balanced group, the upgrade converts the group to a non-load-balanced sensor group.
- Manually configured memcap values for preprocessors such as Stream4 and IP Defragmentation are discarded during upgrade. To support the use of detection engines in Release 4.5.1, memcaps are set dynamically based on the amount of memory and the number of detection resources on the Intrusion Sensor.
- When you upgrade to Release 4.5.1, backups stored on the Defense Center are not retained.
- During the upgrade to Release 4.5.1, the upgrade script disappears from the Updates page (on the Release 4.1.0.2 Defense Center), but the upgrade installs successfully.
- If you use an upgraded Defense Center (v4.5) to manage a legacy Intrusion Sensor (v4.1), Nortel recommends that you use only the Defense Center to manage the intrusion policies on the sensor. If you use the Intrusion Sensor web interface to apply an intrusion policy to itself, you are limited to using the functionality in v4.1.
- During the transition from v4.1.0.2 to v4.5.1, any sensor groups defined in v4.1.0.2 are automatically duplicated as detection engine groups.
- If your Defense Center is part of a high availability pair, make sure you upgrade the primary Defense Center first. After the primary Defense Center is upgraded, make sure it is communicating with all of its managed sensors. Do not change any settings on the managed sensors until after you upgrade the secondary Defense Center. Until you upgrade the secondary Defense Center, the health monitor on the primary Defense Center displays the status of the secondary Defense Center as Critical. Only after both Defense Centers are communicating with their managed sensors should you upgrade the sensors.

- You must import and apply patches and updates on both Defense Centers in a high availability pair. The second Defense Center in the pair does not receive software updates as part of the regular synchronization process.
- After the upgrade, events that reside on the clipboard are lost.
- As part of the upgrade, the Defense Center Virtual Management Network is set to 0.0.0.0/24. This disables transmission of third-party communications, such as NTP, to managed sensors and, in high availability deployments, to the Defense Center peer. To reconfigure the Defense Center Virtual Management Network setting select Operations > System Settings and click Remote Management. Nortel recommends that you use 172.16.0.0/24. After you upgrade your sensors, you must reset the Virtual Management Network to a different value (for example, 0.0.0.0/24) and click **Save** . You must then reset the value to the address range you want to use (for example, 172.16.0.0/24) and click **Save**.
- To change the management port during the initial setup for any appliance in your deployment, ensure that you change the port on all the appliances.
- If you modified the user.conf file on your Intrusion Sensor, those changes are not maintained when you upgrade the sensor to Release 4.5.1. Contact Nortel Support to recreate modifications to the user.conf file.
- If traffic is not received on a non-bypass-enabled inline interface during upgrade, determine whether the interface is part of the inline interface set. If the interface is not part of the inline interface set, open the Interface Set page and add the inline interface to the interface set manually.
- If you create identical sensor groups on a Release 4.1.0.2 Defense Center and a Release 4.5.1 Defense Center, upgrade the Release 4.1.0.2 Defense Center to Release 4.5.1, and then configure both Defense Centers as a high availability pair, each Defense Center has two sensor groups with the same name. Delete the sensors from one of the groups and then delete that group.
- Ensure that only two interfaces are connected to the network from a version 4.1 Intrusion Sensor deployed inline. If three interfaces are connected to an inline sensor, Snort fails after the upgrade.
- Running tasks in the task queue are automatically cancelled when you start the upgrade and tasks scheduled to occur during the upgrade do not run.
- Upgrade of a legacy sensor fails if the legacy sensor runs out of disk space during upgrade from the Defense Center. You must contact Nortel Support for assistance.

- If you upgrade an Intrusion Sensor managed by a pair of Defense Centers in high availability mode, and then modify the interface set configuration on the sensor, the incorrect number of Snort processes may run on the sensor. If the sensor to stops sending events to the Defense Centers, reboot the sensor.
- Health monitoring is not enabled by default after the upgrade. You must use the Defense Center to create and apply health policies to your managed sensors. For more information, refer to *Nortel TPS Defense Center User Guide for Release 4.5.1,* part number 216886-D.

Upgrade warnings

- During an installation, if the update page is refreshed, HTML code can appear. The HTML code disappears when the update is fully installed. Do not interact with the GUI until the Defense Center upgrade process is complete. (17563 and 18373)
- Allow the Defense Center to reboot unimpeded when the upgrade concludes.

Upgrading a Defense Center from version 4.1.0.2 to version 4.5.1

To upgrade to version 4.5.1 software, your system must be running version 4.1.0.2.

CAUTION—Do not use the web interface until the upgrade is complete and the appliance reboots; see Upgrade warnings.

Use the Procedure to upgrade a Defense Center to upgrade a Defense Center from version 4.1 to version 4.5.1.

Procedure to upgrade a Defense Center

1. Download the Defense Center 4.5.1 upgrade script directly from the Nortel Web site.
2. Open the Defense Center Administration menu.
3. Click **Update**.
4. Click **View**.
5. Click **Browse**.
   Navigate to the location where the upgrade script is saved.
6. Select the upgrade script.

7. Click **Open**.
   The update appears in the Upload and Update Package field.
8. Click **Upload**.
   The 4.5.1 upgrade appears in the Install update section of the page.
9. Click the button next to the upgrade.
10. Click **Install**.
    A message appears stating that the appliance will reboot automatically after the upgrade is installed.
11. Click **OK** to continue.
12. To monitor upgrade progress open the Operations page.
13. Select **Monitoring**.
    The Monitoring page appears.
14. Select **Task Status**.
    TIP: Manually refresh the browser if the task queue current status update stops.

IMPORTANT! If the upgrade halts, Nortel recommends that you do not restart it. Contact Nortel Technical Support; see How to get help (page 56).

To confirm the new software version after the upgrade is installed and the appliance is rebooted, use the Procedure to confirm the new software version.

Procedure to confirm the new software version

1. Refresh the browser.
2. Select **Operations**.
3. Select **Help**.
4. Select **About** to view and confirm the software version.

NOTE – Depending on the number of old intrusion events to be migrated into the update, it can take between 20 minutes and 14 hours for old intrusion events to appear on event views and in event statistics.

To upgrade managed sensors from a Defense Center, use the Procedure to upgrade managed sensors from a Defense Center.

Procedure to upgrade managed sensors from a Defense Center

1. Download the Release 4.5.1 upgrade script directly from the Nortel Web site.
2. On the Defense Center, select **Operations**.
3. Select **Update**.
   The Update page appears.
4. Click **Upload Update** and browse to the downloaded upgrade script.
5. Select the update.
6. Click **Upload**.
   The upload script is uploaded to the Defense Center
7. Click **Push**.
   The Push Update page appears.
8. Select the sensors or sensor groups to upgrade.
9. From the Batch size for this push list, select the number of sensors for a batch.
   For example, if you have 20 managed sensors to upgrade, you can specify 5 as the batch size to push the updates to 5 sensors at a time.
10. Click **Push**.
11. To monitor push progress, open the Operations page.
12. Select **Monitoring**.
13. Select **Task Status**.
14. When the push completes, click **Install**.
15. Confirm the installation.
    The upgrade installs, the sensor automatically reboots, and the Defense Center applies updated intrusion policies to upgraded Intrusion Sensors.
16. To confirm that the sensors are upgraded to the correct version, open the Operations page.
17. Click **Sensors**.

18. Log in to the web interface to review and accept the end user license agreement for each upgraded sensor.

Restoring a Defense Center

Restoration software is available for download from the Nortel web site; see Finding the latest updates on the Nortel web site (page 56). Create a CD-ROM containing the iso image and use the restoration procedure in this section.

A keyboard and VGA monitor must be used, rather than the serial port, when restoring the TPS software for the TPS 2070 DC platform to its original state.

Turn off the power to the TPS appliance before connecting the keyboard and monitor. Connect the keyboard and monitor. Turn on the power to the appliance and start it from the CD-ROM using the Restore procedure. Follow the instructions on the monitor. When the software has been restored, turn off power to the appliance and disconnect the keyboard and monitor. Continue with the Restore procedure.

To restore managed sensors, see Restoring an Intrusion Sensor (page 42).

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

Use the Procedure to restore a TPS appliance to its original factory settings to restore a TPS appliance to its original factory settings.

Procedure to restore a TPS appliance to its original factory settings

1. Place the Restore CD-ROM in the CD tray and perform a safe reboot of the appliance. After the appliance reboots, you are prompted to restore the system.
2. At the prompt, type **Yes**.
3. Press **Enter**.
4. At the prompt, type one of the following:
   a. To confirm the restoration, type **Yes**.
   b. To halt the restoration, type **No**.
   TIP: After the system is restored, the appliance ejects the CD-ROM and reboots.
5. Connect the appliance and restore power.

6. If the Add Feature License page appears, paste the original license file into the License field.
7. Click **Submit License**.

Downgrading the Defense Center

Ensure that you downgrade Defense Center managed sensors before you downgrade the Defense Center.

Use the Procedure to downgrade a Defense Center to downgrade the Defense Center from Release 4.5.1 to Release 4.1.0.2.

Procedure to downgrade a Defense Center

1. Open the Operations page.
2. Select **Update**.
   The Patch Management Update page appears.
3. Select the uninstaller that matches the upgrade you want to remove.
4. Click **Install**.
   The Install Update page appears.
5. Under Selected Update, select the Defense Center.
6. Click **Install**.
7. The update is removed, the Defense Center is rebooted, and the Defense Center reverts to Release 4.1.0.2.

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

8. After the uninstall finishes and the Defense Center reboots, use secure shell (ssh) to log into the Defense Center with the root account.
9. Check to make sure you have enough free space on your hard drive to complete the task by viewing the following log file:

/var/log/sf/Nortel_TPS_DC_Upgrade_4.5.0/A_revert_prep.sh.log

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

When the revert operation completes, use the Procedure to confirm the software version to confirm that the downgrade is successful.

Procedure to confirm the software version

1. Log in to the Defense Center.
2. Select **Operations** .
3. Select **Help**.
4. Select **About**.
   Confirm that the software version is listed as 4.1.0.2.

Defense Center resolved issues in version 4.5.1

The following issues concerning the TPS 2070 Defense Center are resolved in release 4.5.1:

- When using a Defense Center to manage an Intrusion Sensor with Store Events Only on DC selected, ensure that Store Events Only On DC is deselected before communication between the sensor and the DC is disabled if you decide not to manage the sensor with the DC. (15430, CR Q01142542)
- Snort does not restart after a policy is applied with a community and pass rule. (CR Q01154185)
- The DC identifies a custom-rule-based event only by rule number. (CR Q01142513)
- When a scheduled report named report/workflow emailed is created, the impact block does not appear. (CR Q01172392)
- Pushing an update to an IS that is already updated provides an unclear result. (CR Q01166435)
- Sensor current policy appears as unknown on the DC. (CR Q01142482)
- A DC/RTI custom fingerprint on the management interfaces renders the DC/RTI inaccessible. (CR Q01162947)
- Snort causes incorrect error for the replace option (does not have quotes). (CR Q01175453)
- New rule containing content, without quotes, causes fatal error and snort restarts. (CR Q01171982)
- The RTI on IS upgrade file cannot be removed from the Intrusion Sensor on the Intrusion Sensor GUI. (CR Q01175172, see also CR Q01166446)
- 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)
- False errors occur after login to TPS 2070 IS in passive or in-line mode. (21369, CR Q01149339)
- Bookmarks cannot be saved when using Help from within the GUI. (21384, CR Q01150679)
- High Availability is not supported for the Version 4.5.1 Beta release software. (23752)

- If you select Intrusion Prevention Sensor Default Policy as the basis for a new policy, the Policy Mode does not change to Intrusion Prevention Sensor. **WORKAROUND**: to create an Intrusion Prevention Policy for an Inline sensor, select Intrusion Prevention Sensor Default Policy as the basis for the new policy and set the Policy Mode to IPS (23570).
- In High Availability installations, a secondary Defense Center (DC) cannot be removed and replaced using a different Defense Center as the secondary DC. A backup of the original secondary DC must be created, and this backup must be restored on a new secondary DC. A connection is automatically made to the primary DC when the restore is complete. (13788)
- Connections can be lost before the network traffic reaches the detection engine when using an Intrusion Sensor in Inline mode in high traffic cases. The percentage of packets dropped as reported by the sensor refers to the percentage that was not processed by the detection engine. However, other packets may have been dropped before they reached the detection engine. (15898)
- Destination-based remediations do not work on standalone RTI Sensors because, in RTI events, only event source hosts are transmitted. Some of the included remediation modules, for example Cisco PIX Shun, Cisco IOS Null Route, and CheckPoint OPSEC SAM, provide destination-based remediations. (16149)
- Version 4.1 includes a new MIB, called DCEALERT.MIB, for SNMP alerting. The new MIB is available in the /etc/sf directory and supports the new compliance policy features. (16593)
- When a version 3.2.x Intrusion Sensor is added to a Defense Center, the default 4.1 intrusion policy for that sensor model is automatically pushed to the sensor. To use a different policy, the policy must be pushed to the sensor. (16667)
- Reboot the appliance if it does not restart properly after the DNS server on the Network page is changed. (16909)
- If custom compliance policies or rules are created on a Defense Center that is later added to a High Availability pair as the secondary Defense Center, then all the existing policy violation events on the secondary Defense Center are listed with numbers, rather than names, for the compliance policy and rule. As a workaround, deactivate and reactivate a single policy so that subsequent events exhibit the correct policy and rule names. (16940)
- If you manually upload an update, ensure that it is pushed manually to the appliance and installed manually. A manually uploaded update installed using the Task Scheduler fails but a success e-mail is sent. (17094)

- When creating a Block To/From Destination IP/Network remediation for a CheckPoint OPSEC SAM instance, the Log and Alert options are reversed. If you select Log, the remediation with the log_alert response is stored. If you select Alert, the remediation with the log_noalert response is stored. (17426)
- It is possible to create and save an incomplete, invalid compliance rule by incorrectly specifying a Host Profile Qualification. The rule is saved even though the GUI displays an error on save. Fix the rule or none of the compliance policies work. (18476)
- If a firewall hosts fails when OPSEC SAM responses are set to use more than one firewall host using the All option, the failure message does not indicate which host failed. Review the firewall logs of the management firewall server to determine which responses failed or succeeded. (19684)
- Use Secure Copy (remote file copy program) to copy large backup files to and from the Defense Center. Most web browsers do not support file transfers larger and 2 Gb. Ensure that you use the Access Configuration page to allow a connection between the Defense Center and the local machine where the backup files are stored. On the RTI Sensor backup files are stored in /var/sf/backup. (20061, 20064)
- File and product names used in the installation and restore processes are not rebranded. (20158, 20160)
- Local sessions no longer need to store the user name and password. (13695)
- If you are using a Defense Center to manage an Intrusion Sensor and you are storing events only on the Defense Center, you can disable the sensor connection to the Defense Center without configuring the sensor to store events locally. (15430)
- The Defense Center sends intrusion policy apply commands to the task queue, where they occur in the background. (16986)
- You can search for intrusion events by classification name. (17089)
- Tasks scheduled for midnight run. (17359)
- The NOT operator (!) functions correctly as shown in the examples on the Search pages. (17490)
- Performance is improved for display of intrusion event statistics for multiple detection engines when the there are a large number of intrusion events in the Defense Center database (10 million or more). (17503)
- You can specify a from address when configuring intrusion event e-mail alerts. (17729)

- If a user creates incident reports and that user's account is deleted from the Defense Center, the admin user can access the reports. (18305)
- Performance is improved on the updates page (Operations > Update) (18903)
- You can use spaces in the name of a custom classification. (19656)
- If you create an invalid IDS rule, the web interface does not allow you to save or apply the intrusion policy. (19999)
- If you use the web interface to begin the restore process, the process no longer times out if the backup file is large. (20058, 21393)
- If a user exceeds the maximum number of failed logins, the admin user can now unlock the user's access to the Defense Center by resetting the password for that account on the User Management page (Operations > User Management). This resets the password to the user's old password. (20384)
- Defining variables in intrusion policies works as documented. (20484)
- Intrusion Sensor performance statistics are displayed correctly. (20648)
- The performance of the scheduler is improved on systems configured to run many scheduled tasks. (21078)
- Users cannot create passwords longer than the maximum length allowed by the login page (32 characters). (21141)
- frag3: Fragmentation overlap (123:8) events display correctly on the Defense Center. (24140)
- SID 498 (Snort ID 498, "ATTACK-RESPONSES id check returned root") triggers correctly. (21818)
- If you apply a policy to a managed sensor, then modify the policy on the Defense Center, but do not apply it, the detection engines page (Operations > Configuration > Detection Engines > Detection Engines) correctly identifies the policy on the sensor as out of date. (22076)
- Intrusion event searches for negated IP addresses and CIDR blocks work correctly. (22304)
- You can remove old patch and upgrade scripts from the web interface. (22514)
- The Back button in Internet Explorer returns to the previous page. (23100)
- You can sort the list of patches and upgrades by type, version, and creation date. (23230)

- You can deactivate an intrusion rule from the packet view for custom intrusion policies. (24195)
- Only users with Admin access can purge RTI events. (24606)
- The percentage of packets dropped by RTI is reported correctly. (24816)
- When you check the Confirm All Actions check box on the Event Preferences page (Preferences > Event View Settings),you must indicate and confirm whether you want to perform an action on all the events that appear on an event view, on the clipboard, or on an incident page. (24893)
- Intrusion events stored in different database table partitions are sorted correctly in event views. (27784)

Defense Center known issues

The following list contains the known issues for the Defense Center.

- The Japanese language is not supported in this release.
- You cannot upload backup files larger than two GB. (20063)
- On a Defense Center or an RTI Sensor, the CPU Usage System values report only the CPU usage of the thread that checks for performance data. **WORKAROUND**: apply a health policy with the CPU usage module enabled to the appliance. (23441)
- If you apply two IDS policies to an Intrusion Sensor and the first policy fails but the second policy is successful, the first policy can run again and supersede the second policy. (23480)
- Saving a rule containing a syntax error in the TPS rule editor produces an error message. The contents of the rule editor are then cleared, and the rule building process must be restarted. (11488)
- Do not delete any custom rule classifications that meet the following criteria:
  - The classification was used in an intrusion policy applied to an Intrusion Sensor.
  - Any compliance policies were created using rule classifications. (11748, 14546)
- Do not delete any custom incident types assigned to an incident. (11748, 14546)
- Intrusion event reports that contain more than one million events can take several hours to generate. (13727)

- Some Intrusion Sensors added to a Defense Center can be listed as having out-of-date intrusion detection policies on the Sensor Management page. Ignore these messages. However, ensure that the sensors are updated if the policies are subsequently modified. (13965)
- If TPS e-mail alerting is set up, a recurring task named JobSFMail is added to the scheduler. The start time for the task is set for December 31, 1969 and an entry appears on the calendar for each of the recurring instances from 1969. (13978)
- On the View Schedules page, ensure that the correct check boxes are selected after specifying whether the task is recurring or one time only. If the New Task option and Backup for the Job Type are selected, and the Event or Configuration check boxes are selected before changing the task type between once and recurring, then the check boxes clear. (13992)
- The Scheduler page does not display an error message if an e-mail address is specified in the E-mail Status To field before setting up the mail relay host on the Configure E-mail Notification page. (14002)
- If a user account is deleted and a new account is created with the same name but differing access permissions, the new account reverts to the permissions from the deleted account. The new user account must be edited to ensure that account permissions are correct. (14037, 16291)
- The navigation menu disappears on some browsers if the Start Net Backup button on the Backup and Restore page is clicked before the name for the backup file is specified. Refresh the browser window to restore the navigation menu. (14099)
- The Event Summary page, on the Defense Center, can show event percentages that total more than 100 percent. (14151)
- Account privileges for users logged in as Admin can be reduced to Maintenance access. To regain Admin access, log out and log back in. (14725)
- Event searches that include all digit sensor names produce unexpected results. Avoid using all numeric characters for sensor names. (14726)
- The Defense Center and managed sensors must be on the same side of a network address translation (NAT) device. If the network environment is not configured in this way, contact Nortel Technical Support for configuration assistance. (15453)
- When a compliance policy is created based on the detected criterion “a new transport protocol is detected” using Transport Protocol as the condition, only the protocol abbreviation, for example UDP, and not the protocol number, for example 17, can be used. (15955)

- A scheduled task cannot be created using the name of the managed sensor as the job name. (16363)
- There can be a temporary pause in traffic if the Intrusion Sensor is deployed in Inline mode and the Snort process is restarted. The Snort process can be restarted when modes are switched between Passive and Inline or when the sensor is rebooted. (16514, 16516)
- The delete button on the Defense Center does not function if two or more OPSEC peers are added. (16651)
- Using a fail-open card with an Intrusion Sensor deployed in Inline mode, after a new intrusion policy is applied, causes traffic to pass through the sensor for a brief period without inspection. Uninspected traffic occurs when an intrusion policy is applied on a standalone Intrusion Sensor or when an intrusion policy is pushed to a managed Intrusion Sensor. (16702)
- It can take up to five minutes to add another managed sensor to a Defense Center having a large number of events. A large number of events can be considered five million. (16708)
- To use the rule editor to add the replace keyword to a rule, you must use quotation marks around the replacement string, for example, “replacement_string”. You must also ensure that the content keyword being replaced immediately precedes the replace keyword, which must be the last keyword in the rule. (16748, 16750).
- In High Availability environments, a Defense Center must be used to collect custom fingerprints. If a managed sensor is used to collect custom fingerprints, the information collected is not deleted from the sensor. (16809)
- If a new intrusion policy is created based on an existing policy, any settings for SNMP alerting are not copied to the new policy. As a workaround, edit the new policy and use the Alerting option to configure SNMP alerts. (16876)
- A mismatch in Snort versions between a version 4.1 Defense Center managing a version 3.2 Intrusion Sensor with a version 3.2.x patch applied can occur. The mismatch causes the Intrusion Sensor to fail to generate new events. When this happens, delete the sensor from the Defense Center and reintroduce it. When the sensor is reintroduced to the Defense Center, a new version of Snort is automatically pushed onto the sensor and the mismatch is eliminated. (16966)
- Rebooting a Defense Center while pushing a policy to a sensor causes tasks in the Task Queue to enter a state where they cannot be deleted from the Task Queue page. (19366)

- Applying any Policy from the DC causes the IS to restart the snort/interface. (CR Q01157243)
- A rule created or saved as new cannot be deleted unless the appliance is re-installed. (20009, CR Q01153219)
- Pending events cannot be removed from the queue when processing starts. Remediation events requiring completion on the Defense Center are queued and processed one at a time, resulting in a negative impact on Defense Center performance. (CR Q01202128)
- 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, 20532)
- Issues as reported in the 4.1 through 4.1.0.2 release notes that are not listed as resolved in those documents. Release notes for previous versions of the Defense Center are available on the Nortel Support Site.
- The Safari web browser for Mac OS X is not supported.
- Intrusion Sensor load balancing is not supported in Release 4.5.1.
- Because you can apply a system policy to any appliance model, you can use the web interface to set event storage database limits that are higher than the maximum number of database records enforced by Nortel TPS for the appliance. When you apply the policy, the absolute limits are automatically enforced. (16603)
- If you apply multiple conflicting policies to the same sensor or detection engine while the sensor is not communicating with the Defense Center, the Defense Center may not apply the correct policy when it resumes communicating. **Workaround**: check the task queue to ensure that each policy is successfully applied before you attempt to apply a new policy of the same type. (16849)
- When you delete a sensor from a Defense Center that is part of a high availability pair, wait until the other Defense Center deletes the sensor automatically before you attempt to re-add the sensor to either Defense Center. (17829)
- Because most web browsers do not support file transfers that are larger than 2GB, you must use scp rather than the web interface to copy large backup files to and from the Defense Center. Make sure that you use the Access Configuration page to allow a connection between the Defense Center and the local machine where you store backup files. Backup files are stored in /var/sf/backup on the Defense Center. (20063, 20066)

- If you deploy an Intrusion Sensor in inline mode, and you do not have a fail-open network card installed, you may notice a temporary pause in traffic when you apply a new intrusion policy. If you do have a fail-open network card installed, the sensor fails open while a policy is being applied. The sensor begins inspecting traffic again once the policy is applied. (20449)
- 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 Defense Center, rather than the timestamps of the events used to build the report. (21215)
- If you receive intrusion alerts more frequently than configured Max Alerts and Frequency settings, contact Nortel Support for assistance. (22883)
- The CPU Usage - User and CPU Usage - System performance statistics values only report the CPU usage of the thread that checks for performance data, rather than the total user and system CPU usage. **Workaround**: apply a health policy with the CPU usage module enabled. (23441)
- Intrusion events generated by preprocessors display a classification of "none." (24144)
- You cannot set the memcap manually for preprocessors like Stream4 and IP Defragmentation. To support the use of multiple detection engines in Release 4.5.1, memcaps are set dynamically, based on the amount of memory and the number of detection resources on the Intrusion Sensor. (24490)
- The Defense Center does not e-mail a copy of a report run remotely; that is, a report profile created on the Defense Center and run using the data on a managed sensor. (23679)
- The Defense Center automatically adjusts its local time display for daylight saving time (DST), where appropriate. However, recurring tasks that span the transition dates from DST to standard time and back do not adjust for the transition. For example, if you create a task scheduled for 2am during standard time, it will run at 3am during DST. If you create a task scheduled for 2am during DST, it will run at 1am during standard time. (23732)
- You cannot use the Defense Center to generate a remote report based on the events from a legacy sensor. (24523)

- 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 events 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 mangement_interface , where mangement_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 edit variable definitions to include port ranges in an intrusion policy, and that variable is used by many rules (for example, if you set $HTTP_SERVERS to 80:81), the Defense Center uses excessive memory when you validate or apply the policy. **Workaround**: duplicate the rules and use a different port for the duplicated rules. (25735)
- If you use Internet Explorer in a Microsoft Windows XP environment, the page load progress bar may indicate that the page is finished loading and ready for interaction when it is not. (25892)
- Intrusion event thresholding applies to each detection engine, instead of to each sensor. If your Intrusion Sensor is configured with a detection engine that has multiple resources and your intrusion policy contains rules that use the threshold keyword to limit event logging, you may receive more events than expected. (25957, 25992)
- Custom classifications assigned to intrusion rules created on managed sensors are not maintained if you import intrusion rules into the Defense Center from the managed Intrusion Sensor. (26024)
- If you run ifconfig from the command line on Ethernet Routing Switch 8600 Service Delivery Module (SDM) inline and inline with fail-open appliances, your session suspends. **Workaround**: terminate the session and log in again. (26076)
- When you view intrusion event graphs for the detection engine on a legacy Intrusion Sensor, you must reselect the detection engine to view a different graph for the same detection engine. (26359)

- Intrusion policies and detection policies are not listed for your managed sensors on the Sensors page because policies are applied to detection engines in Release 4.5.1. (26393)
- If you apply an IPS Policy to a passive detection engine on a legacy sensor, the web interface does not alert you . If you apply an IPS policy to a passive detection engine, drop rules do not drop packets or block attacks and drop rules do not alert you when malicious packets are detected. (26496, 26885, 27225)
- If you have a large number of events stored on the 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 same impact flag. However, the sum of the number of events is correct. (26712)
- In a high availability pair, each Defense Center is not aware of sensors the other is monitoring but health policies are shared. (26826)
- If you start the local Nessus server on the Defense Center, then perform a backup and restore of the appliance, the Nessus server stops. If you want to use the local Nessus server to perform scans you must restart it. (26853)
- Tasks in the task queue can be incorrectly nested. (26886, 27327)
- If you create a custom vulnerabilities workflow, and then specify the new workflow or the predefined vulnerabilities workflow as your default, when you view vulnerabilities you are prompted to select a workflow. (26889)
- If you are not logged in as the admin user, jobs are automatically removed from the task queue when they finish running and you cannot see a list a completed tasks. (26910)
- If you configure your Defense Center to alert you when health events are pruned from the database, the alert specifies incorrectly that the audit log is pruned. Note that health events are pruned as specified despite the alert. (26917)
- If you are using Internet Explorer, do not use keyboard shortcuts to specify an interface set type. (26946)
- You can create multiple intrusion policies with the same name. **Workaround**: choose unique names for policies. (26950)
- When you use the Defense Center web interface to apply a system policy to the Defense Center you do not receive confirmation and the task queue does not contain a record of the policy application. (26968)

- After the upgrade to Release 4.5.1, remediation status events are not sorted by time (the default for event views) in the remediation status table view of events. **Workaround**: click the Time column title to sort the results by time. (26987)
- If the task queue reports that a Nessus scan is running after it finishes, you must manually remove the job from the task queue. (26996)
- Health event severity, in health alerts, is reported by color as follows: red indicates critical, yellow indicates warning, green indicates normal, blue indicates disabled, and gray indicates an error. (27026)
- When editing an interface set, if you remove an interface from the list of available interfaces before the web interface loads all of the available interfaces, the interface you remove disappears from view. **Workaround**: cancel the edit or wait until the web interface is loaded. (27098)
- Release 4.5.1 does not support multiple remote managers but you can specify more than one remote manager on the web interface on the Defense Center. **Workaround**: do not specify more than one remote manager for a sensor. (27123)
- When you delete a user account, the Defense Center does not prompt you to confirm the deletion and the account is immediately deleted. (27146)
- You cannot edit network interfaces on legacy sensors. If you are using the Defense Center to manage legacy sensors and attempt to edit the default network interface settings for the sensors, the Defense Center displays an error stating that it cannot load the network interfaces. Disregard the error message. (27152)
- The task queue may contain completed jobs, such as policy applications, initiated by other users. Only the admin user can delete these completed tasks. (27158)
- Each registered sensor must have a unique IP address. A sensor cannot register with the Defense Center if an address is not available in the virtual management network. If you attempt to register more sensors than available addresses, contact Nortel Support. (27187, 27188)
- If you configure the virtual management network so that there are less available IP address than sensors registered to the Defense Center, some sensors may share virtual IP addresses. **Solution**: increase the number of available IP addresses in the virtual management network so that each sensor receives a unique IP address. (27195)
- The Save and Add buttons in the subpages of read-only intrusion policies (that is, policies that were not authored by the local appliance) do not function. (27201)
- The Back button in Firefox does not always take you back to the previous page. **Workaround**: use the menu structure. (27256)

- If you delete a sensor from the Defense Center, you must use the Task Status (Operations > Monitoring > Task Status) page to manually delete tasks that were running at the time of deletion. (27260)
- You cannot use wildcards when you are searching by MAC address for RTI-based events (network discovery events, hosts). (27268)
- Queries: On any RTI table view that includes the OS Version column, if you select an OS version that contains multiple versions as a constraint and then save the constraint as a query, before you can use the saved search you must click **Edit Query** and, on the resulting Search page, place double quotes around the version numbers in the OS Version field. (27304)
- Do not delete tens of thousands of services from the services table view at one time. **Workaround**: delete several thousand at one time. (27312)
- If you deactivate all the vulnerabilities for a host in the host profile, you cannot reactivate any of the host vulnerabilities until a new vulnerability is detected for that host. (27350)
- When you upgrade a legacy managed Intrusion Sensor to Release 4.5.1, backlogged events may display sensor IDs as "unknown" on the sensor web interface. **Workaround**: apply a new intrusion policy to the detection engines on the sensor. (27395)
- 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)
- The Help > About page on a legacy sensor managed by a Release 4.5.1 Defense Center may display a software error. Disregard the message. **Workaround**: Nortel recommends that you upgrade your legacy sensors. (27518)
- You can specify an invalid IP address for the Defense Center on the web interface. Do not specify an invalid IP address for the Defense Center management interface in the system settings. (27773)
- You cannot use the Analysis & Reporting, Policy & Response, and Operations menus while pages load. (27967)
- You can configure RTI detection engines and policies for an Intrusion Sensor on the SDM 8600 web interface. NOTE: RTI Software for the Intrusion Sensor is not supported on the SDM 8600. (28048, 28700)

- If want to use the Defense Center to serve time using NTP, you must enable NTP in the Defense Center system policy and apply the policy to the Defense Center before you apply the policy to the sensors it manages. Do not apply the policy to the Defense Center and the sensors at the same time. (28153)
- Do not assign a remediation as a response to an event that occurs frequently. The remediation can fail or Defense Center performance can decrease. (28338)
- If you create a compliance rule, Rule 1, based on a traffic profile change, and then create another compliance rule, Rule 2, that triggers only if Rule1 is true, Rule 2 does not activate. (28459)
- If you write an intrusion rule to search packet payloads for content using Perl-compatible regular expressions (PCRE), and you use the hash mark, semicolon, vertical bar, single quote, and colon characters, the rule editor may display a truncated version of the rule, even though the rule is correctly stored in the database. (28473)
- If you use Firefox as your browser, use the browser bookmark feature to bookmark a page in the online help. Right-click the frame that contains the content you want to bookmark and select This Frame > Bookmark This Frame. (28499)
- When you use the rule editor to create a replace rule, ensure that the content you use to replace the detected malicious content contains the exact number of characters as the malicious content. Snort fails if you enter new content that does not match the number of characters for the original malicious content. (28591)
- While restoring from a backup, the restore operation may appear to hang in the task queue, even though it has completed successfully. **Workaround**: cancel the job in the task queue and reboot the Defense Center. (28532)
- If SEU versions differ between 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 remotely view the (read-only) intrusion policy applied to the appliance with the newer SEU. **Workaround**: ensure that your appliances use the same SEU. (28569)
- You can view the task queue for only one appliance at a time in a popup window. **Workaround**: view the task status for another appliance by selecting Operations > Monitoring > Task Status. (28613)
- Do not specify a name containing an apostrophe for a custom workflow. You cannot select workflow names containing an apostrophe as default workflows on the Event View Settings page. (28614)

- If you install a new SEU and then attempt to apply an invalid intrusion policy to a detection engine, the detection engine stops examining network traffic. **Solution**: correct the errors in your intrusion policy and reapply it. (28636)
- Configuring OPSEC remediations for Check Point Firewalls: If you use the web interface to set the logging level to Log, the level is actually set to Alert . Setting the logging level to Alert actually sets the logging level to Log . (28659)
- Network and license settings are lost if you use the restore CD to restore a Defense Center previously upgraded to Release 4.5.1 **CAUTION**: Ensure that you keep a copy of network and license settings before you restore the appliance. (28672)
- If the detection engine column in the table view of events is blank, you cannot set attributes for hosts displayed in a custom table. **Workaround**: set the host attributes from the host profiles of the individual hosts or from the default host attributes table view of events provided with your Defense Center. (28675)
- Inline and Inline with Fail Open interface sets are not supported on the SDM 8600. (28676)
- The web interface indicates that transparent mode is enabled for Inline and Inline with Fail Open interface sets, even if it is not enabled. **Workaround**: to ensure that transparent mode is set correctly, edit the interface set accordingly and click **Save**. (28724)
- You cannot create a Host Attributes report if you constrain the hosts that appear in that report based on their IP addresses. (28725)
- If you create a Host Attribute report, and one of the attributes is of type List, the values assigned to each host for that attribute are rendered incorrectly. (28727)

Features and functionality – TPS 2050 IS, TPS 2150 IS, TPS 2070 IS, and TPS 2170 IS Intrusion Sensors

The TPS 2x50 IS and TPS 2x70 IS Intrusion Sensors contain the following features and functionality in release 4.5.1:

- Enhanced decoders: Release 4.5.1 provides new pre-processors for SMTP, FTP, and Telnet.
- Multiple detection engines and policies: One sensor can run multiple Snort instances associated with a named detection engine. The named detection engine can be associated with one or more interfaces. You can configure multiple policies on the same sensor to discover the interface where an event is detected.
- Graphical User Interface (GUI) enhancements: The GUI contains a reorganized menu, and new icons and tools bars that provide improved navigation.
- *OPSEC: OPSEC debug logging on the sensor is available from the console. The OPSEC debug logging feature is disabled by default.

Upgrading existing Intrusion Sensors

Table 2 lists the sections that provide important information about the upgrade process:

Table 2 Upgrade information

Section name	Page
Prerequisites for upgrading Intrusion Sensors	37
Notes on the upgrade process	37
Upgrading an Intrusion Sensor from version 4.1.0.2 to version 4.5.1	40
Procedure to reapply the current intrusion policy	41

To install a new Intrusion Sensor version 4.1 appliance, follow the instructions provided in the *Nortel TPS Sensor/DC Installation Guide, Release 4.1*, Part Number 320737-A, which is provided on the Intrusion Sensor Documentation and Restore CD. The guide is also available on the Nortel Technical Support site at www.nortel.com/support.

Prerequisites for upgrading Intrusion Sensors

The following prerequisites must be met before existing Intrusion Sensors are upgraded to version 4.5.1:

- Intrusion Sensor version 4.1.0.2 is required to complete a successful upgrade to version 4.5.1.
- At least 108 Mb of free space is required on the root partition (/), and 11 Mb of free space is required on the /var partition.
- For Defense Centers managing Intrusion Sensors, check the sensor management page and confirm that each sensor uses a policy that the Defense Center can identify. Any policy listed as unknown must be replaced with a policy pushed from the Defense Center to the sensor before either appliance is upgraded.
- Upgrade all Defense Centers before upgrading sensors managed by the Defense Centers.

Notes on the upgrade process

This section contains important information about upgrading Nortel products. Read the entire section before beginning any upgrade.

IMPORTANT! The upgrade process migrates all event and configuration data to a replacement database.

- Intrusion Sensor load balancing is not supported in Release 4.5.1. The upgrade process converts Intrusion Sensors in a load-balanced group to a non-load-balanced sensor group.
- Plan the upgrade for a time when it has the least impact on your deployment because the Defense Center reboots after upgrade.
- Nortel recommends that you back up event and configuration data to a local computer.
- Delete any user-created files from /root before starting the upgrade.
- Do not perform any administrative or analysis tasks during the upgrade process.
- After completion of the Defense Center upgrade, obtain the upgrade software file called Nortel_TPS_Intrusion_Sensor_Upgrade_4.1.0.2_to_4.5.1_Upgrade-47.sh from the Nortel support site at www.nortel.com/support.
- Backups stored on the Intrusion Sensor are not retained when the Sensor is upgraded to Release 4.5.1.

- Use the scheduling feature to schedule the upgrade push and installation on managed sensors. For information about the scheduling feature, see the *Nortel TPS Defense Center User Guide*, Part Number 216886-D.
- If the upgrade halts for any reason, it can be restarted at the point where it stopped because the upgrade tracks its own progress. For example, in the event of a power failure during upgrade, the installation process can be restarted using the graphical user interface (GUI). If the upgrade proceeded past the point where the GUI is accessible, edit the /etc/sf/ims.conf file and modify the SWVERSION to match the version being upgraded. For Defense Centers this is version 4.1.0.2. However, if an upgrade halts for any reason, Nortel recommends that you contact Nortel Technical Support.
- The upgrade Revert feature permits restoration of an upgraded appliance to the previously installed software version. Before using the Revert feature, the Revert process checks to ensure that there is enough free space is available on the hard drive to complete the task. At least 50 percent of the size of the event and upgrade data is required. To revert to the previous software version, use secure shell (ssh) with the root account to log into the Intrusion Sensor, type **`revert`** at the command prompt and press **Enter**. Nortel recommends that all event and configuration data is backed up on a local computer before performing the Revert operation because intrusion events in the database are not retained. After the Revert operation is complete, restore the events from backup file to the Intrusion Sensor.
- Intrusion events on the clipboard, or marked as reviewed, are lost when the appliance is rebooted at the end of the upgrade procedure.
- The upgrade can take several hours, depending on the number of events on the appliance, particularly on Defense Centers and the TPS 2070 IS sensor. Refresh the browser to check the status of the upgrade. When the upgrade is complete, a prompt appears instructing the user to log into the appliance.
- E-mail alerting must be reconfigured after the upgrade is complete because settings for e-mail alerting on intrusion rules are not preserved as part of the upgrade. The configuration requirement applies to Defense Centers managing Intrusion Sensors.
- The version number on the login page is not updated after the Upgrade. To confirm that the new version is installed, select **Help**. Then select **About** and review the value in the Software Version field.
- If you set the memcap value manually for preprocessors such as Stream4 and IP Defragmentation, those values are discarded during upgrade. To support the use of detection engines in Release 4.5.1, memcaps are set dynamically based on the amount of memory and the number of detection resources on the Intrusion Sensor.

- If you use an upgraded Defense Center to manage a legacy Intrusion Sensor, Nortel recommends that you use the Defense Center to manage the intrusion policies on the sensor. If you use the Intrusion Sensor web interface to apply an intrusion policy to the Intrusion Sensor, you are limited to using the functionality in version 4.1.
- If you attempt to upload the upgrade script to the Intrusion Sensor over a slow connection, the web interface may time out before the upload is complete and the upload fails.
- During the upgrade to Release 4.5.1, the upgrade script disappears from the Updates page (on the Release 4.1.0.2 Intrusion Sensor), but the upgrade installs successfully.
- If you change the management port during the initial setup for any appliance in your deployment, make sure you change the port on all appliances.
- If you modified the user.conf file on your Intrusion Sensor, those changes are not maintained when you upgrade the sensor to Release 4.5.1. Contact Nortel Support to recreate modifications.
- During upgrade, if traffic is not received on a non-bypass-enabled inline interface, check to see if the interface was added to the inline interface set. If it was not, you can manually add the inline interface to the interface set from the Interface Set page.
- Ensure that a version 4.1 Intrusion Sensor, deployed inline, is connected to the network by only two interfaces. Snort fails after the upgrade if there are more than two interfaces connected on an inline sensor.
- Running tasks in the task queue ware automatically cancelled when you start the upgrade. Tasks scheduled to occur during the upgrade do not run.
- If you upgrade an Intrusion Sensor that is managed by a pair of Defense Centers in high availability mode, and then modify the interface set configuration on the sensor, the incorrect number of Snort processes may run on the sensor and the sensor may stop sending events to the Defense Centers. If the sensor stops sending events to the Defense Centers, reboot the sensor.

Upgrading an Intrusion Sensor from version 4.1.0.2 to version 4.5.1

Use the Procedure to upgrade an Intrusion Sensor to upgrade an Intrusion Sensor from version 4.1 to version 4.5.1.

CAUTION—Do not use the web interface until the upgrade is complete and the appliance reboots; see Upgrade warnings (page 15).

Procedure to upgrade an Intrusion Sensor

1. Download the Intrusion Sensor 4.5.1 upgrade script.
2. Open the Intrusion Sensor Administration page.
3. Select **Update**.
4. Select **View**.
5. Click **Browse**.
   Navigate to the location where the upgrade script is saved.
6. Select the upgrade script.
7. Click **Upload**.
8. Click **Open**.
   The update appears in the Upload and Update Package field.
9. Click **Upload**.
   The 4.5.1 upgrade appears in the Install Update section of the page.
10. Select the button next to the upgrade.
11. Click **Install**.
    A message appears stating that the appliance will reboot automatically after the upgrade is installed.
12. Click **OK** to confirm and continue.
13. Reapply the current intrusion policy; see Procedure to reapply the current intrusion policy (page 41).

IMPORTANT! If the upgrade halts, Nortel recommends that you do not restart it. Contact Nortel Technical Support.

To reapply the current intrusion policy, use the Procedure to reapply the current intrusion policy.

Procedure to reapply the current intrusion policy

1. Select **Detection**.
2. Select **Policy**.
3. Select **Apply**.
4. Select the name of the current policy.
5. Click **Apply**.
   TIP: There can be a brief pause while the new version of Snort restarts on an Intrusion Sensor deployed in Inline mode.

To confirm the new software version after the upgrade is installed and the appliance is rebooted, use the Procedure to confirm the new software version.

Procedure to confirm the new software version

1. Refresh the browser.
2. Select **Help**.
3. Select **About** to view and confirm the software version.

Migrating event and packet data to the new database

After the upgrade process concludes the system populates the new database with the old intrusion events. The event data migration time can vary from 20 minutes, for 1 million intrusion events, to four hours for 10 million events, to 14 hours for 110 million events.

Old intrusion events do not appear on the event views or in the event statistics until population of the new database completes. You cannot view packets associated with events until the migration completes because packet data migrates after event data.

Restoring an Intrusion Sensor

Restoration software files are available for download from the Nortel web site; see Finding the latest updates on the Nortel web site (page 56).

Create a CD-ROM containing the iso image and follow the restoration procedure in this section.

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

You cannot use the Defense Center to uninstall the upgrade from managed sensors.

A keyboard and VGA monitor must be used rather than the serial port when restoring the TPS software for the TPS 2070 IS and TPS 2170 IS platforms to its original state. Turn off the power to the TPS appliance before connecting the keyboard and monitor. Connect the keyboard and monitor. Turn on the power to the appliance and start it from the Software CD using the Restore procedure, see step 1 of the following procedure. Follow the instructions on the monitor. When the software has been restored, turn off power to the appliance and disconnect the keyboard and monitor. Continue with Step 5 of the procedure.

Use the Procedure to restore a TPS appliance to its original factory settings to restore a TPS appliance to its original factory settings.

Procedure to restore a TPS appliance to its original factory settings

1. Place the Restore CD-ROM in the CD tray and perform a safe reboot of the appliance.
   After the appliance reboots, you are prompted to restore the system.
2. At the prompt, type **Yes**.
3. Press **Enter**.
4. At the prompt, type one of the following:
   a. To confirm the restoration, type **Yes**.
   b. To halt the restoration, type **No**.
      TIP: After the system is restored, the appliance ejects the CD-ROM and reboots.
5. Connect the appliance and restore power.

6. If the Add Feature License page appears, paste the original license file into the License field.
7. Click **Submit License**.

Downgrading an Intrusion Sensor

When you downgrade an Intrusion Sensor from Release 4.5.1 to a previous release take note of the following:

- Contact Nortel Support before you downgrade the Intrusion Sensor.
- When you downgrade the Intrusion Sensor, events generated after the upgrade are not retained in the database. Events generated before the upgrade are retained, but they may already have been purged.

IMPORTANT! Ensure that you downgrade Defense Center managed sensors before you downgrade the Defense Center.

Use the Procedure to downgrade an Intrusion Sensor to downgrade an Intrusion Sensor from Release 4.5.1 to a previous release.

Procedure to downgrade an Intrusion Sensor

1. Select **Operations**.
2. Select **Update**.
   The Patch Management Update page appears.
3. Select the uninstaller that matches the upgrade you want to remove.
4. Click **Install**.
   The update is removed, the Intrusion Sensor reboots, and the Intrusion Sensor reverts to Release 4.1.0.2.

   CAUTION: If the uninstall halts, do not restart it. Contact Nortel Support for more information.
5. After the uninstall finishes and the Intrusion Sensor reboots, use secure shell (ssh) to log into the Intrusion Sensor with the root account.
6. To ensure that you have enough free space on your hard drive to complete the task view the following log file:

/var/log/sf/Nortel_TPS_IS_Upgrade_4.5.0/A_revert_prep.sh.log

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

To confirm the software version use Procedure to confirm the software version.

Procedure to confirm the software version

1. Log in to the Intrusion Sensor.
2. Select **Operations**.
3. Select **Help**.
4. Select **About**.
   Confirm that the software version is 4.1.0.2.

Intrusion Sensors resolved issues in version 4.5.1

The following issues concerning Intrusion Sensors are resolved in release 4.5.1:

- When using a Defense Center to manage an Intrusion Sensor with Store Events Only On DC selected, if you decide not to manage the sensor with the DC, ensure that Store Events Only On DC is deselected before communication between the sensor and the DC is disabled. (15430, CR Q01142542)
- Connections can be lost before the network traffic reaches the detection engine when using an Intrusion Sensor in Inline mode in high traffic cases. The percentage of packets dropped, as reported by the sensor, refers to the percentage not processed by the detection engine. However, other packets may have been dropped before they reached the detection engine. (15898)
- Destination-based remediations do not work on standalone RTI Sensors because, in RTI events, only source hosts are transmitted. Some of the included remediation modules, for example Cisco PIX Shun, Cisco IOS Null Route, and CheckPoint OPSEC SAM, provide destination-based remediations. (16149)
- Version 4.1 includes a new MIB, called DCEALERT.MIB, for SNMP alerting. The new MIB is available in the /etc/sf directory and supports the new compliance policy features. (16593)
- When a version 3.2.x Intrusion Sensor is added to a Defense Center, the default 4.1 intrusion policy for that sensor model is automatically pushed to the sensor. To use a different policy, the policy must be pushed to the sensor. (16667)
- Reboot the appliance if it does not restart properly after you change the DNS server on the Network page. (16909)
- If you manually upload an update, ensure that it is pushed manually to the appliance and installed manually. A manually uploaded update installed using the Task Scheduler fails but a success e-mail is sent. (17094)
- Rebooting a Defense Center while pushing a policy to a sensor causes tasks in the Task Queue to enter a state where they cannot be deleted from the Task Queue page. (19366)
- If a firewall hosts fails when OPSEC SAM responses are set to use more than one firewall host using the All option, the failure message does not indicate which host failed. Review the firewall logs of the management firewall server to determine which responses failed or succeeded. (19684)

- Use Secure Copy (remote file copy program) to copy large backup files to and from the Defense Center. Most web browsers do not support file transfers larger and 2 Gb. Ensure that you use the Access Configuration page to allow a connection between the Defense Center and the local machine where the backup files are stored. Only the RTI Sensor backup files are stored in /var/sf/backup. (20061, 20064)
- File and product names used in the installation and restore processes are not rebranded. (20158, 20160)
- Intrusion Sensors in Inline mode process traffic flow unlike Intrusion Sensors in Passive mode. On the Performance Status page, Intrusion Sensors in Passive mode cannot report the percentage of packets dropped. (14719)
- Local sessions no longer need to store the user name and password. (13695)
- If you are using a Defense Center to manage an Intrusion Sensor, and you are storing events only on the Defense Center, you can disable the sensor connection to the Defense Center without first configuring the sensor to store events locally. (15430)
- You can search for intrusion events by classification name. (17089)
- Tasks scheduled for midnight run. (17359)
- The NOT operator (!) functions correctly as shown in the examples on the Search pages. (17490)
- You can specify a "from" address when configuring intrusion event e-mail alerts. (17729)
- If a user creates incident reports and then that user account is deleted from the Intrusion Sensor, the admin user can access the reports. (18305)
- The Updates page performance is improved. (18903)
- You can use spaces in the name of a custom classification. (19656)
- If you create an invalid IDS rule, you cannot save or apply the intrusion policy on the web interface. (19999)
- Using the web interface to begin the restore process no longer times out if the backup file is large. (20058, 21393)
- If a user exceeds the maximum number of failed logins, the admin user can unlock the user access to the Intrusion Sensor by resetting the password for that account on the User Management page. This resets the user password to the old password. (20384)
- Defining variables in intrusion policies works as documented. (20484)
- Intrusion Sensor performance statistics are displayed correctly. (20648)

- Users cannot create passwords longer than the maximum length, 32 characters, allowed by the login page. (21141)
- SID 498 (Snort ID 498, "ATTACK-RESPONSES id check returned root") triggers correctly. (21818)
- If you apply a policy to a managed sensor, then modify the policy on the Defense Center but do not apply it, the detection engines page correctly identifies the policy on the sensor as out of date. (22076)
- Intrusion event searches for negated IP addresses and CIDR blocks work correctly. (22304)
- You can remove old patch and upgrade scripts from the web interface. (22514)
- The Back button in Internet Explorer returns to the previous page. (23100)
- You can sort the list of patches and upgrades by type, version, and creation date. (23230)
- Deactivating an intrusion rule from the packet view works correctly for custom intrusion policies. (24195)
- When you check the Confirm All Actions check box on the Event Preferences page, you must confirm that you want to perform an action on all the events that appear on an event view, on the clipboard, or on an incident page. (24893)
- Intrusion events are sorted correctly in event views if they are stored in different database table partitions. (27784)

Intrusion Sensors known issues

The following list contains the known issues for Intrusion Sensors.

- Snort does not restart after a policy is applied with a community and pass rule. (CR Q01154185)
- When a scheduled report named report/workflow emailed is created, the impact block does not appear . (CR Q01172392)
- Snort restarts at midnight. Snort restart affects TPS 2070 IS in Inline mode, build 235, and TPS 2050 IS, build 289. In Inline mode, Snort restarting causes the link to cycle and causes failover in a redundant scenario. When Snort is restarted it loses session and state information.(CR Q01158292)
- A TPS 2070 IS in Inline mode permits load balance configuration. (CR Q01159577

- Saving a rule containing a syntax error in the IDS rule editor produces an error message. The contents of the rule editor are cleared and the rule-building process must be restarted. (11488)
- Do not delete any custom rule classifications under the following conditions:
  - the classification in an intrusion policy is used and applied to the Intrusion Sensor
  - any compliance policies are created using rule classifications (11748, 14546)
- Do not delete any custom incident types assigned to an incident. (11748, 14546)
- Intrusion event reports containing more than 1 million events can take more than one hour to generate. (13727)
- Some Intrusion Sensors added to a Defense Center can be listed on the Sensor Management page as having out-of-date intrusion detection policies. Ensure that the sensors are updated if the policies are modified. (13965)
- The start time for IDS e-mail alerting is set for December 1969 and an entry appears on the calendar for each recurring instance back to 1969. The task in the scheduler is named JobSFMail. (13978)
- On the View Schedules page, ensure that the correct check boxes are selected after specifying whether the task is recurring or one time only. If the New Task option and Backup for the Job Type are selected, and the Event or Configuration check boxes are selected before changing the task type between once and recurring, then the check boxes clear. (13992)
- The Scheduler page does not display an error message if an e-mail address is specified in the E-mail Status To field before setting up the mail relay host on the Configure E-mail Notification page. (14002)
- If a user account is deleted and a new account is created with the same name but differing access permissions, the new account reverts to the permissions from the deleted account. The new user account must be edited to ensure that account permissions are correct. (14037, 16291)
- The navigation menu disappears on some browsers if you click the Start Net Backup button on the Backup and Restore page before you specify the name for the backup file. Refresh the browser window to restore the navigation menu. (14099)
- The Event Summary page, on the Defense Center, can show event percentages that total more than 100 percent. (14151)
- Account privileges for users logged in as Admin can be reduced to Maintenance access. To regain Admin access, log out and log back in. (14725)

- Event searches that include all digit sensor names produce unexpected results. Avoid using all numeric characters for sensor names. (14726)
- The Defense Center and managed sensors must reside on the same side of a network address translation (NAT) device. If the network environment is not configured in this way, contact Nortel Technical Support for configuration assistance. (15453)
- A scheduled task cannot be created using the name of the managed sensor as the job name. (16363)
- There can be a temporary pause in traffic if the Intrusion Sensor is deployed in Inline mode and the Snort process is restarted. The Snort process can be restarted when modes are switched between Passive and Inline or when the sensor is rebooted. (16514, 16516)
- Using a fail-open card with an Intrusion Sensor deployed in Inline mode, after a new intrusion policy is applied, causes traffic to pass through the sensor for a brief period without inspection. Uninspected traffic occurs when an intrusion policy is applied to a standalone Intrusion Sensor or when an intrusion policy is pushed to a managed Intrusion Sensor. (16702)
- It can take up to five minutes to add another managed sensor to a Defense Center having a large number of events. A large number of events can be considered five million. (16708)
- To use the rule editor to add the replace keyword to a rule, you must use quotation marks around the replacement string, for example, “replacement_string”. You must also ensure that the content keyword being replaced immediately precedes the replace keyword, which must be the last keyword in the rule. (16748, 16750).
- If a new intrusion policy is created based on an existing policy, any settings for SNMP alerting are not copied to the new policy. As a workaround, edit the new policy and use the Alerting option to configure SNMP alerts. (16876)
- A mismatch in Snort versions between a version 4.1 Defense Center managing a version 3.2 Intrusion Sensor with a version 3.2.x patch applied can occur. The mismatch causes the Intrusion Sensor to fail to generate new events. When this happens, delete the sensor from the Defense Center and reintroduce it. When the sensor is reintroduced to the Defense Center, a new version of Snort is automatically pushed onto the sensor and the mismatch is eliminated. (16966)
- The Japanese language is not supported in this release.
- 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)

- A rule created or saved as new cannot be deleted unless the appliance is re-installed. (20009, CR Q01153219)
- False errors occur after login to TPS 2070 IS in passive or in-line mode. (21369, CR Q01149339)
- Bookmarks cannot be saved when using Help from within the GUI. (21384, CR Q01150679)
- When you enter a hostname on the Network Configuration page the user interface inserts a dot character at the end of the hostname. The dot produces the following error: alert not sent, socket refused and the Intrusion Sensor does not send a response. To allow OPSEC to operate correctly Nortel recommends that you configure the Intrusion Sensor with a Hostname and Domain name. (CR Q01209729)
- The Safari web browser for Mac OS X is not supported.
- Intrusion Sensor load balancing is not supported in Release 4.5.1.
- Because you can apply a system policy to any appliance model, you can use the web interface to set event storage database limits that are higher than the maximum number of database records enforced by Nortel TPS for the appliance. However, when you apply the policy, the absolute limits are automatically enforced. (16603)
- If you apply multiple conflicting policies to the same sensor or detection engine while the sensor is not communicating with the Defense Center, the Defense Center may not apply the correct policy when it restarts communication. **Workaround: check** the task queue to ensure that each policy is successfully applied before you attempt to apply a new policy of the same type. (16849)
- Because most web browsers do not support file transfers that are larger than 2GB, you must use scp rather than the web interface to copy large backup files to and from the Intrusion Sensor. Use the Access Configuration page to connect the Intrusion Sensor and the local machine where backup files are stored. Backup files are stored in /var/sf/backup on the Intrusion Sensor. (20063, 20066)
- If you deploy an Intrusion Sensor in inline mode, and you do not have a fail-open network card installed, there may be a temporary pause in traffic when you apply a new intrusion policy. If you have a fail-open network card installed, it fails open while a policy is being applied and the sensor begins inspecting traffic again once the policy is applied. (20449)
- When you generate a report containing intrusion events, the underlying source and destination port query does not include event protocol. 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, not the timestamps of the events used to build the report. (21215)
- If you receive intrusion alerts more frequently than the Max Alerts and Frequency settings, contact Nortel Support for assistance. (22883)
- CPU Usage, User and CPU Usage: System performance statistics values report only the CPU usage of the thread that checks for performance data, not than the total user and system CPU usage. (23441)
- Intrusion events generated by preprocessors display a classification of "none." (24144)
- You cannot manually set the memcap for preprocessors such as Stream4 and IP Defragmentation. To support the use of multiple detection engines in Release 4.5.1, memcaps are set dynamically, based on the amount of memory and the number of detection resources on the Intrusion Sensor. (24490)
- The Defense Center automatically adjusts its local time display for daylight saving time (DST), where appropriate. However, recurring tasks that span the transition dates from DST to standard time and back do not adjust for the transition. For example, if you create a task scheduled for 2 a.m. during standard time, it will run at 3 a.m. during DST. Similarly, if you create a task scheduled for 2 a.m. during DST, it will run at 1 a.m. during standard time. (23732)
- 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 events using relative times (for example, < today at 4:30 p.m.). (25069)
- During initial setup, if you configure the system policy on your Intrusion Sensor to receive time through an external NTP server and 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 mangement_interface , where mangement_interface is the name of your management interface (for example, eth0), you must reboot the Intrusion Sensor or the new IP address is not accessible. (25253)

- If you edit variable definitions to include port ranges in an intrusion policy, and that variable is used by many rules (for example, if you set $HTTP_SERVERS to 80:81), the Intrusion Sensor uses excessive memory when you validate or apply the policy. **Workaround**: duplicate the rules and use a different port for the duplicated rules. (25735)
- If you are using Internet Explorer in a Microsoft Windows XP environment, the page load progress bar indicates that the page load is complete before the page is loaded. The page is not ready for interaction. (25892)
- Intrusion event thresholding applies to each detection engine, not each sensor. If your Intrusion Sensor is configured with a detection engine that has multiple resources and your intrusion policy contains rules that use the threshold keyword to limit event logging, you may receive more events than expected. (25957, 25992)
- If you create and assign an intrusion rule on a managed Intrusion Sensor and import the intrusion rule into a Defense Center from the managed Intrusion Sensor, any custom classification assigned to the rule is not maintained. (26024)
- When you view intrusion event graphs for the detection engine on a legacy Intrusion Sensor, you must reselect the detection engine to view a different kind of graph for the same detection engine. (26359)
- The web interface does not alert you if you apply an IPS Policy to a passive detection engine on a legacy sensor. If you apply an IPS policy to a passive detection engine, drop rules do not drop packets or block attacks, and drop rules do not alert you when malicious packets are detected. (26496, 26885, 27225)
- tasks in the task queue may be nested incorrectly. (26886, 27327)
- Because jobs are removed automatically from the task queue on completion, you cannot view a list a completed tasks unless you are logged in as the admin user. (26910)
- If you are using Internet Explorer, do not use keyboard shortcuts to specify an interface set type. (26946)
- Although you can create multiple intrusion policies with the same name, you must choose unique names for policies to avoid confusion. (26950)
- When you use the Intrusion Sensor web interface to apply a system policy to the Intrusion Sensor, you do not receive confirmation of success and the task queue contains no record of the policy application. (26968)

- Editing an interface set: if you remove an interface from the list of available interfaces before the web interface has loaded all of the available interfaces, the removed interface disappears from view. **Solution**: cancel the edit or wait until the web interface is loaded. (27098)
- Multiple remote managers are not supported although the web interface on the sensors allows you to specify more than one remote manager (Defense Center). Do not specify more than one remote manager for a sensor. (27123)
- When you delete a user account, the Intrusion Sensor does not prompt you to confirm the deletion. The account is immediately deleted. (27146)
- The task queue may contain completed jobs, such as policy applications, that were initiated by other users. 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 the local appliance) do not function. (27201)
- Because the Intrusion Sensor has no vulnerability database you cannot schedule an update of the vulnerability database. (27217)
- The Back button in Firefox does not always return to the previous page. **Workaround:** use the menu structure. (27256)
- If you delete a sensor from the Defense Center, you must use the Task Status page to manually delete any tasks running at the time of deletion. (27260)
- When you upgrade a legacy managed Intrusion Sensor to Release 4.5.1, backlogged events may display unknown Sensor IDs on the sensor web interface. **Workaround**: apply a new intrusion policy to the detection engines on the sensor. (27395)
- Do not specify an invalid IP address for the Intrusion Sensor management interface in the system settings. (27773)
- You cannot use the Analysis & Reporting, Policy & Response, and Operations menus while pages load. (27967)
- If want to use the Defense Center to serve time using NTP, you must enable NTP in the Defense Center system policy and apply the policy to the Defense Center before you apply the policy to managed sensors. Do not apply the policy to the Defense Center and the sensors at the same time. (28153)

- The About page displays version information for the version of Snort that is currently installed on the Intrusion Sensor. However, the sensor detection engines can use the Defense Center version of Snort if you used a Defense Center with an SEU that differs from the Intrusion Sensor to apply an intrusion policy to the detection engines on the sensor. (28388)
- The rule editor may display a truncated version of the rule if you use the hash mark, semicolon, vertical bar, single quote, or colon characters and Perl-compatible regular expressions (PCRE) to write an intrusion rule to search packet payloads for content. However, the rule is stored correctly in the database. (28473)
- If you want to bookmark a page in the online help using Firefox, do not use the bookmark icon in the online help. Use the browser bookmarking feature. (28499)
- When you use the rule editor to create a replace rule, ensure that the content you use to replace the detected malicious content contains the same number of characters as the malicious content or Snort fails to start. (28591)
- While restoring from a backup, the restore operation may appear to suspend in the task queue even though it has completed successfully. **Solution**: cancel the job in the task queue and reboot the Intrusion Sensor. (28532)
- Ensure that Defense Centers and Intrusion Centers use the same SEU. If the SEU version on the Defense Center and Intrusion Sensor differ, the web interface on the appliance with the older SEU does not display any new IDS rule categories when you remotely view the intrusion policy applied to the appliance with the newer SEU. (28569)
- You cannot view the task queue for more than one appliance in a pop-up window. For example, if you are upgrading an appliance and you click the Task Status link on the Patch Management Update page you cannot view the task queue for a second appliance in a pop-up window. **Workaround**: view the task status for one of the appliances by selecting Operations > Monitoring > Task Status. (28613)
- Do not specify a name containing an apostrophe for a custom workflow, although the web interface does not prevent apostrophe use, because you cannot choose those workflows as default workflows on the Event View Settings page. (28614)
- If you install a new SEU and then attempt to apply an invalid intrusion policy to a detection engine, the detection engine stops examining network traffic. **Solution**: correct the errors in your intrusion policy and reapply it. (28636)
- If you use the restore CD to downgrade an upgraded Intrusion Sensor, your network and license settings are lost. Make a copy of network and license settings before initiating downgrade activity. (28672)

- The web interface indicates that transparent mode is enabled for Inline and Inline with Fail Open interface sets, even if it is not. To ensure that transparent mode is set correctly, edit the interface set and click **Save**. (28724)

Related publications

These release notes supplement the following documents:

- *TPS 2050 and TPS 2070 Intrusion Sensor User Guide* Release 4.5.1 (Part Number 216884-D)
- *TPS 2070 Defense Center User Guide* Release 4.5.1 (Part Number 216886-D)
- *Real-time Threat Intelligence User Guide Release 3.5.1* (Part Number 320722-B)
- *Real-Time Threat Intelligence Sensor Visualizer User Guide Release 3.0* (Part Number 322255-A)
- *Real-time Threat Intelligence Sensors 3.5.1 Release Notes* (Part Number 320741-B)
- *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

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.