

Nortel Intrusion Sensor

Release 4.5.1.2 Release Notes

September 12, 2006

Issues Resolved in Release 4.5.1.2

The following issues are resolved in Release 4.5.1.2:

- Fixed an issue where an upgrade might fail because of insufficient disk space.
- Fixed a problem where the web interface improperly handled flow depths of 0 for the HTTP inspection preprocessor.
- Fixed an issue where, while restoring from a backup, the restore job might appear to hang in the task queue, even though it had completed successfully.
- Fixed an issue where intrusion event email alerts may have included incorrect messages.
- Intrusion rule messages longer than 64 characters are no longer truncated in the web interface and alerts
- Fixed a problem where editing an network interface may stop traffic from being processed by the detection engines.
- Applying an intrusion prevention policy to an inline Intrusion Sensor no longer causes the sensor to drop packets while detection engines are restarted.
- Fixed an issue where intrusion event email alerts would stop being sent after an error occurred.
- Improved latency on low-traffic networks being monitored by Intrusion Sensors deployed inline.
- Fixed an issue where the packet views for intrusion events generated by unknown rules and intrusion agents were not correctly displayed.
- Fixed an issue where RTI Software on Intrusion Sensors consumed excessive resources and stopped processing traffic.

Upgrading Existing Intrusion Sensors

This section outlines how to plan and perform the upgrade of your Intrusion Sensor.

To plan your upgrade, read the following steps:

1. Prepare for the upgrade. Make sure that:

- you upgrade the Defense Center, if any, that manages the Intrusion Sensor to Release 4.5.1.2
- your Intrusion Sensor is running the correct version (4.5.1 or 4.5.1.1) of the Nortel TPS software

If you are running an earlier version, you can obtain upgrades from the [Nortel Customer Support](#) site.

- you have enough free disk space

You must have at least 8 MB of free space on the / partition and 52 MB of free space on the /var partition to complete this upgrade successfully.

- you plan your upgrade for a time when it will have the least impact on your deployment; be sure to schedule the upgrade during non-peak hours

2. Optionally, back up your event and configuration data and save it to a local computer.

Although the upgrade process retains event and configuration data, Nortel strongly recommends that you back the data up yourself before you perform the upgrade.

3. Perform the upgrade, as described in [Upgrading the Intrusion Sensor](#).

Once you begin the upgrade, you can monitor its progress in the task queue (**Operations > Monitoring > Task Status**). Do **not** use the web interface to perform any other tasks until the upgrade has completed and the Intrusion Sensor reboots.

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

Note that if your Intrusion Sensor is deployed inline and does not have a fail-open network card, traffic is interrupted while the sensor reboots after the upgrade has completed. If your Intrusion Sensor has a fail-open network card, some traffic may pass through the sensor uninspected while it reboots.

4. Complete any required post-upgrade steps, as described in [After You Upgrade](#).

Upgrading the Intrusion Sensor

You can use the Defense Center to upgrade Intrusion Sensors. For more information, refer to the release notes for the Defense Center.

To upgrade an Intrusion Sensor:

1. From the [Nortel Customer Support](#) site, download zip file: TPS_IS_DC_4_5_1_2.zip.

2. Extract the Intrusion Sensor 4.5.1.2 upgrade script (Nortel_TPS_Defense_Center_Patch_4.5.1.1_to_4.5.1.2_Upgrade-34.sh).

WARNING! Download files directly from the [Nortel Customer Support](#) site and do not transfer them by email. If you transfer an update file by email, it may become corrupted.

3. Select **Operations > Update**.

The Patch Management Update page appears.

4. Click **Upload Update** to browse to the location where you saved the upgrade script, then click **Upload**.

The upgrade appears in the Updates list.

5. Next to the upgrade you just uploaded, click **Install**.

6. Confirm that you want to install the upgrade and reboot the Intrusion Sensor.

The upgrade is installed and the Intrusion Sensor reboots.

WARNING! You can monitor the upgrade's progress in the task queue (**Operations > Monitoring > Task Status**). Do **not** use the web interface to perform any other tasks until the upgrade has completed and the Intrusion Sensor reboots. If the task queue stops updating with current status, manually refresh your browser. If you encounter issues with the upgrade, for example, if the task queue indicates that the upgrade has failed or if a manual refresh of the task queue shows no progress, do **not** restart the upgrade. Instead, please contact Nortel Support.

7. After the upgrade finishes and the Intrusion Sensor reboots, log into the Intrusion Sensor.

8. Select **Operations > Help > About** and confirm that the software version is listed as 4.5.1.2.

After You Upgrade

After you complete the upgrade, you **must** install the latest SEU on the Intrusion Sensor and on the Defense Center that manages it (if any) and reapply intrusion policies to your detection engines.

For more information, refer to the Intrusion Sensor User Guide.

Uninstalling the Upgrade

Regardless of where you started, uninstalling the upgrade results in a Intrusion Sensor running Release 4.5.1.1. For information on uninstalling Release 4.5.1.1, refer to the notes for that release.

Note that if your Intrusion Sensor is deployed inline and does not have a fail-open network card, traffic is interrupted while the sensor reboots after the uninstallation has completed. If your

Intrusion Sensor has a fail-open network card, some traffic may pass through the sensor uninspected while it reboots.

You **cannot** use the Defense Center to uninstall the upgrade from Intrusion Sensors.

To uninstall the upgrade from the Intrusion Sensor:

1. Select **Operations > Update**.

The Patch Management Update page appears.

2. Next to the uninstaller that matches the upgrade you want to remove, click **Install**.

3. Confirm that you want to uninstall the upgrade and reboot the Intrusion Sensor.

The upgrade is removed, the Intrusion Sensor reboots, and the Intrusion Sensor reverts to Release 4.5.1.1.

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

4. After the uninstall finishes and the Intrusion Sensor reboots, log into the Intrusion Sensor.

5. Select **Operations > Help > About** and confirm that the software version is listed as Release 4.5.1.1.

Known Issues

The following are known issues with Release 4.5.1.2:

- Issues as reported in the 4.5 through 4.5.1.1 release notes that are not listed as resolved in any of those documents, or in this document. Release notes for previous versions of the Intrusion Sensor are available on the [Nortel Customer Support](#) site.

Product Compatibility

You must use Release 4.5.1.2 of the Defense Center to manage Release 4.5.1.2 of the Nortel Intrusion Sensor.

For Assistance

If you have any questions or require assistance with the Nortel Defense Center, Intrusion Sensor, RTI Sensor, or any of the software sensors, please contact Nortel Support.

- Visit the [Nortel Customer Support](#) site.

- Email Nortel Support at support@nortel.com.

Thank you for using Nortel products.