NORTEL THREAT PROTECTION SYSTEM RELEASE NOTES

Release 4.6.0.4

August 24, 2007

For the Nortel Defense Center Release 4.6.0.4, the Nortel Intrusion Sensor Release 4.6.0.4, and the Nortel Intrusion Sensor on SDM Release 4.6.0.4, these release notes describe:

Issues Resolved in Release 4.6.0.4

The following issues are resolved for the Nortel Defense Center, the Nortel Intrusion Sensor, and the Nortel Intrusion Sensor on SDM Release 4.6.0.4:

- You can now set the Flow Depth field on the HTTP Inspection page of an intrusion policy to 0 and successfully save and apply the policy. (33817)
- **Defense Center Only** Applying a health policy to a managed sensor from a Defense Center now consistently succeeds in Microsoft Internet Explorer version 6.0 service pack 2. (34005)
- **Defense Center Only** Resolved an issue where a report was sometimes automatically deleted after completion. (34062)
- **Defense Center Only** You can now disable the management virtual network by entering 0.0.0.0/24 or 0.0.0.0/0 in the Management Virtual Network field

of the Remote Management page in the System Settings on the Defense Center. (34152)

- **Defense Center Only** Resolved an issue where SNMPv3 traps for health monitoring were not encrypted or authenticated even if you selected encryption and authentication during alert configuration. (34386)
- **Defense Center Only** Resolved an issue where communications to a single sensor stop when the Defense Center is heavily loaded. (34419)
- The number of connections for the Stream4 preprocessor is now dynamically set based on available resources. (34442)
- **Defense Center Only** Resolved an issue by expanding the table used to store traffic profile flow summaries in the database. (34616)
- The SFDataCorrelator can now restart without affecting transmission of intrusion events to the Defense Center from a managed sensor. (34623)
- **Defense Center Only** When configuring an LDAP server for login authentication, you can now include the special characters '#' and '&' in the test user password. (34732)
- **Defense Center Only** Resolved an issue where policy apply jobs would stop and prevent further policy apply jobs from starting. (34936)
- **Defense Center Only** Defense Center sessions now time out as configured if the interface is left unattended. (35009)
- **Defense Center Only** When you disable the management virtual network by entering 0.0.0.0/0 in the Management Virtual Network field of the Remote Management page in the System Settings on the managing Defense Center, you are not locked out of managed sensors. (35395)

Upgrading Existing Appliances and Software Sensors

Planning for the Upgrade: Defense Center and Managed Sensors

This section outlines how to plan for the upgrade of your Nortel Defense Center.

1. **Patch the Defense Center First**

   Make sure you upgrade your Defense Centers to Release 4.6.0.4 before you upgrade the Intrusion Sensors that they manage.

   Also, after you upgrade the Defense Center, but **before** you upgrade any Intrusion Sensors, you must install the latest SEU and re-apply intrusion policies to your detection engines.

2. **Make Sure Your Appliances are Running the Correct Version**

   To upgrade to Release 4.6.0.4, your Intrusion Sensor must be running at least Version 4.6.0.

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

3. **Make sure you have enough free disk space and allow enough time for the upgrade**

   You must have at least 3 MB of free space on the `/` partition and 6 MB of free space on the `/var` partition to complete this upgrade successfully. You should plan to perform the upgrade during non-peak hours.

   The following table provides guidelines for the disk space and time required for the upgrade.

Platform	Disk Space on /	Disk Space on /var	Time
Defense Center	3MB	9.5MB	5 minutes
Intrusion Sensor	6MB	9.8MB	10 minutes

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

Managed Sensor/ Software	Additional Disk Space
Intrusion Sensor	1.8MB

4. **Optionally, Back up Your Event and Configuration Data**

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

5. **Perform the upgrade, as described in Upgrading the Defense Center**

   In general, you can monitor its progress in the Defense Center's task queue (**Operations > Monitoring > Task Status**).

6. **Complete any required post-upgrade steps, as described in After You Upgrade**

   Nortel recommends that you check the Nortel Support web site for the latest SEU and vulnerability database (VDB) update.

7. Upgrade any managed sensors that you are managing with the Defense Center, as described in Upgrading Managed Sensors.

Planning for the Patch: Unmanaged Intrusion Sensors

This section outlines how to plan for the upgrade of your standalone Intrusion Sensor.

IMPORTANT! A Intrusion Sensor is considered a standalone sensor if you do not use a Defense Center to manage it.

1. **Make Sure Your Sensors are Running the Correct Version**

   To upgrade to Release 4.6.0.4, your Intrusion Sensor must be at least Version 4.6.0.

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

2. **Make sure you have enough free disk space and allow enough time for the upgrade**

   You must have at least 8 MB of free space on the `/` partition and 8.6 MB of free space on the `/var` partition to complete this upgrade successfully.

   You should 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.

3. **Optionally, Back up Your Event and Configuration Data**

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

4. **Perform the upgrade, as described in Upgrading an Unmanaged Sensor**

   In general, you can monitor its progress in the Intrusion Sensor's task queue (**Operations > Monitoring > Task Status**).

5. **Complete any required post-upgrade steps, as described in After You Upgrade**

   Nortel recommends that you check the Nortel Support web site for the latest SEU and vulnerability database (VDB) updates.

Upgrading the Defense Center

To upgrade the Defense Center:

1. Download the Nortel Defense Center Release 4.6.0.4 upgrade script (`Nortel_TPS_Defense_Center_Patch_4.6.0_to_4.6.0.4-24.sh`) from the Nortel Support Site.

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

2. Select **Operations > Update.**

   The Patch Management Update page appears.

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

   The upgrade appears in the Updates list.

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

   The Install Update page appears.

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

6. Confirm that you want to install the upgrade.

   The installation process begins.

   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 Support.

   IMPORTANT! You can monitor the upgrade's progress in the task queue (**Operations > Monitoring > Task Status**). Do **not** use the web interface to perform any other tasks until the upgrade has completed. 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 Support.

7. After the upgrade finishes, clear your browser cache and force a reload of the browser.

   Reloading the browser can prevent the web interface from exhibiting unexpected behavior.

8. Select **Operations > Help > About** and confirm that the software version is listed as 4.6.0.4.

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

10. Continue with the tasks you need to perform after the upgrade.

    For more information, see After You Upgrade.

Upgrading Managed Sensors

You can use the Release 4.6.0.4 Defense Center to upgrade managed Intrusion Sensors.

BEFORE YOU UPGRADE

Before you upgrade managed sensors using the Defense Center, you **must:**

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

For information on version and disk space requirements for the upgrade, refer to Upgrading Existing Appliances and Software Sensors.

To upgrade managed sensors:

1. Download the Intrusion Sensor Release 4.6.0.4 upgrade script (`Nortel_TPS_Intrusion_Sensor_Patch_4.6.0_to_4.6.0.4-24.sh`) from the Nortel Support Site.

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

2. Select **Operations > Update.**

   The Patch Update Management page appears.

3. Click **Upload Update** to browse to the upgrade script you downloaded, then click **Upload.**

   The upgrade script is uploaded to the Defense Center.

4. Next to the upgrade script, click **Push.**

   The Push Update page appears.

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

6. From the **Batch size for this push** list, select the number of sensors where the Defense Center should copy the upgrade script at a time.

   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, then push to the next 5 sensors.

7. Click **Push.**

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

8. Next to the upgrade script, click **Install.**

   The Install Update page appears.

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

10. Confirm that you want to install the upgrade.

    The upgrade is installed.

WARNING! You can monitor the upgrade's progress in the task queue (**Operations > Monitoring > Task Status**). If the task queue stops updating with current status, manually refresh your browser. If you encounter issues with the 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 Support.

---

11. Select **Operations > Sensors** and confirm that the sensors you upgraded have the correct versions listed (Release 4.6.0.4).

Upgrading an Unmanaged Sensor

You can upgrade an unmanaged Nortel Intrusion Sensor to Release 4.6.0.4.

To upgrade a standalone Intrusion Sensor:

1. Download the Intrusion Sensor Release 4.6.0.4 upgrade script (`Nortel_TPS_Intrusion_Sensor_Patch_4.6.0_to_4.6.0.4-24.sh`) from the Nortel Support Site.

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

---

2. Select **Operations > Update.**

   The Patch Management Update page appears.

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

   The upgrade appears in the Updates list.

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

   The upgrade is installed.

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

5. After the upgrade finishes, log into the Intrusion Sensor.
6. Select **Operations > Help > About** and confirm that the software version is listed as Release 4.6.0.4.
7. Continue with the tasks you need to perform after the upgrade, including:

- applying any available upgrades or patches to the Intrusion Sensor
- installing the latest SEU and reapplying intrusion policies to IPS detection engines

After You Upgrade

After you complete the upgrade, you **must:**

- install any patches or updates to the Intrusion Sensor that are available on the Support Site
- install the latest SEU and reapply intrusion policies to any IPS detection engines

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

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

Uninstalling the Upgrade

Uninstalling the upgrade results in an Defense Center running 4.6.0. For information on uninstalling 4.6.0, refer to the release notes for that version.

You **cannot** use the Defense Center to uninstall the upgrade from managed sensors. Instead, you must use the sensor's web interface to uninstall the upgrade.

To uninstall the upgrade from the Defense Center:

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.**

IMPORTANT! In this version of the uninstaller, the release numbers in the Task Description have been transposed.
`Nortel_TPS_Defense_Center_Patch_Uninstaller_4.6.0_to_4.6.0.4-#.sh`
should be

`Nortel_TPS_Defense_Center_Patch_Uninstaller_4.6.0.4_to_4.6.0-#.sh`
and
`Nortel_TPS_Defense_Center_Patch_Uninstaller_4.6.0_to_4.6.0.2-#.sh`
should be
`Nortel_TPS_Defense_Center_Patch_Uninstaller_4.6.0.2_to_4.6.0-#.sh`

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

3. Confirm that you want to uninstall the upgrade.

   The upgrade is removed, and the Defense Center returns to 4.6.0.

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

   ---

4. After the uninstall finishes, select **Operations > Help > About** and confirm that the software version is listed as 4.6.0.

Product Compatibility

You must use Release 4.6.0.4 of the Defense Center to manage Release 4.6.0.4 of the Intrusion Sensor.

Release 4.6.0.4 of the Defense Center can manage:

- versions 4.5.1 through 4.5.x and versions 4.6 through 4.6.0.x of the Intrusion Sensor
- versions 3.5.0 through 3.5.x and versions 4.0.0 through 4.0.0.x of the RTI 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 Support Site at http://support.nortel.com/.
- Email Nortel Support at support@nortel.com.

Thank you for using Nortel products.

Legal Notices

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Nortel, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of oninfringement or the implied warranties of merchantability or fitness for a particular purpose.

U.S. Government End Users

This document is provided with a “commercial item” as defined by FAR 2.101 (Oct 1995) and contains “commercial technical data” and “commercial software documentation” as those terms are used in FAR 12.211-12.212 (Oct 1995). Government End Users are authorized to use this documentation only in accordance with those rights and restrictions set forth herein, consistent with FAR 12.211- 12.212 (Oct 1995), DFARS 227.7202 (JUN 1995) and DFARS 252.227-7015 (Nov 1995).

Nortel Networks reserves the right to change any products described herein at any time, and without notice. Nortel Networks assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Nortel Networks. The use and purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Nortel Networks.

Export

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