

Nortel Defense Center

Release 4.6.0.2 Release Notes

February 19, 2007

For the Nortel Defense Center Release 4.6.0.2, these release notes describe:

[Issues Resolved in Release 4.6.0.2](#)

[Upgrading Existing Defense Centers](#)

[Uninstalling the Upgrade](#)

[Product Compatibility](#)

II Issues Resolved in Release 4.6.0.2

The following issues are resolved in Release 4.6.0.2:

Fixed an issue where (null) appeared in place of the number of records in the title of an email alert. The correct number of records now appears. (32398)

Fixed an issue where you could select a specific detection engine in a report based on a custom table, which caused the report to fail. If you select a custom table as the basis of a report, the report now automatically includes all detection engines. (32457)

Fixed an issue where users with Admin access assigned to their accounts could not view all tasks in the task status queue. (32528)

Fixed an issue where connections to managed sensors lapsed and were not re-established because no packets were sent to maintain the connection. (32858)

Fixed an issue where changes to the remote management port did not update the iptables rules, causing connections from the sensor to be blocked. (32912)

Fixed an issue where older log files were not automatically pruned. (32934)

Fixed an issue where log files were not pruned after upgrade. (32826)

Fixed an issue where users with Data access assigned to their accounts could set suppression options in all local policies through the packet view. (33243)

II Upgrading Existing Defense Centers

This section outlines how to plan and perform the upgrade of your Defense Center and any sensors that it manages.

To plan your upgrade, read the following steps:

1. Prepare for the upgrade. Make sure that:

your Defense Center is running the correct version (4.6.0) of the Nortel TPS software

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

your managed sensors are running versions of the Nortel TPS software that can be managed by a Release 4.6.0.2 Defense Center, as detailed in [Product Compatibility](#).

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

you have enough free disk space

You must have at least 3 MB of free space on the / partition and 5 MB of free space on the /var partition to complete this upgrade successfully.

Nortel recommends that you use the Defense Center to upgrade your managed sensors. Depending on the sensors in your deployment, you must have additional space free on Defense Center's /var partition, as follows:

1 MB for Intrusion Sensors

1 MB for RTI Sensors

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 Defense Center](#).

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.

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.

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

5. Upgrade any sensors that you are managing with the Defense Center, as described in [Upgrading Managed Sensors](#).

Upgrading the Defense Center

To upgrade a Defense Center:

1. Download the Defense Center Release 4.6.0.2 upgrade script (`Nortel_TPS_Defense_Center_Patch_4.6.0_to_4.6.0.2-#.sh`) from the [Nortel Support Site](#).

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

2. Select **Operations > Update**.

The Patch 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**.

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 Nortel Support.

6. After the upgrade finishes, clear your browser cache and force a reload of the browser. (Otherwise, the user interface may exhibit unexpected behavior.)

7. Select **Operations > Help > About** and confirm that the software version is listed as 4.6.0.2.

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

9. Continue with the tasks you need to perform after the upgrade, including:

applying any available upgrades or patches to the Defense Center

installing the latest SEU and reapplying intrusion policies to IDS/IPS detection engines

upgrading managed sensors

For more information, see the sections that follow.

Upgrading Managed Sensors

You can use the Defense Center to upgrade managed Intrusion Sensors. 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 Nortel 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 the sensor release notes.

To upgrade managed sensors:

1. Download the appropriate upgrade script from the [Nortel Support Site](#).

for the RTI Sensor, `Nortel_TPS_RNA_Patch_3.5.1.3_to_4.0.0_Upgrade-#.sh`

for the Intrusion Sensor, `Nortel_TPS_IS_Patch_4.6.0_to_4.6.0.1-#.sh`

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

2. Select **Operations > Update**.

The Patch Update Management page appears.

3. Click **Upload Update** to browse to the 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.

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 Nortel Support.

10. Select Operations > Sensors and confirm that the sensors you upgraded have the correct versions listed.

for Intrusion Sensors, 4.6.0.2

for RTI Sensors, 4.0.0.2

After You Upgrade

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

install the latest SEU and reapply intrusion policies to any IDS/IPS detection engines you configured on managed Intrusion Sensors

Note that applying an intrusion policy causes IDS/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 *Defense Center User Guide*.

II Uninstalling the Upgrade

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

You **cannot** use the Defense Center to uninstall the upgrade from managed sensors. For information on how to uninstall the upgrade from a sensor, refer to the sensor release notes.

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**.

The Install Update page appears.

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

The upgrade is removed and the Defense Center returns to Release 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 Nortel Support.

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

II Product Compatibility

Release 4.6.0.2 of the Defense Center can manage:

versions 4.5.0 through 4.5.1.3 and versions 4.6.0 and 4.6.0.2 of the Intrusion Sensor

versions 3.5.0 through 3.5.1.3 and versions 4.0.0 and 4.0.0.2 of the RTI Sensor

versions 3.5.0 through 3.5.1.3 and versions 4.0.0 of RNA Software for Intrusion Sensors

II 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://www.nortel.com/support>.

Email Nortel Support at support@nortel.com.

Thank you for using Nortel products.

Legal Notices

© 2007 Nortel Networks, 4655 Great America Parkway, Santa Clara, CA 95054, USA. All rights reserved.

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, Inc. reserves the right to change any products described herein at any time, and without notice. Nortel, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Nortel, Inc. 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, Inc.

Portions of this manual are © 2006 Sourcefire, Inc. All Rights Reserved. Any other trademarks appearing in this manual are owned by their respective companies.

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.