

Nortel Defense Center

Release 4.5.1.5 Release Notes

February 27, 2007

For the Nortel Defense Center Release 4.5.1.5, these release notes describe:

[New Features and Functionality](#)

[Issues Resolved in Release 4.5.1.5](#)

[Upgrading Existing Defense Centers](#)

[Uninstalling the Upgrade](#)

[Known Issues](#)

[Product Compatibility](#)

You can use this patch to upgrade from version 4.5.1 through version 4.5.1.3 to version 4.5.1.5.

II New Features and Functionality

Release 4.5.1.5 of the Nortel Defense Center does not include any new features or functionality. However, this release is cumulative from version 4.5.1, so be sure to review the release notes for previous releases for any new features they may have introduced.

II Issues Resolved in Release 4.5.1.5

The following issue is resolved in Release 4.5.1.5:

Addressed an issue regarding the change to Daylight Savings Time in the United States and other countries.

IMPORTANT! This release is cumulative from version 4.5.1, so be sure to review the resolved issues in the release notes for previous releases.

II Upgrading Existing Defense Centers

This section offers some suggestions for planning and performing the upgrade of your Defense Center and any sensors that it manages.

WARNING! As part of the installation process, your Defense Center is automatically rebooted. If you are installing the patch upgrade on a managed sensor, the sensor is also automatically rebooted as part of the installation.

To plan your upgrade, read the following steps:

1. Prepare for the upgrade. Make sure that:

your Defense Center is running one of the supported versions for the upgrade (that is, versions 4.5.1 through 4.5.1.3)

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

you have enough free disk space

The amount of free space required by the upgrade depends on the version you are upgrading from. For example, to upgrade from version 4.5.1, you must have at least 27 MB of free space on the / partition and 125 MB of free space on the /var partition to complete this upgrade successfully. To upgrade from version 4.5.1.3, you must have 15 MB of free space on the / partition and 50 MB of free space on the /var partition. If you plan to use the Defense Center to upgrade managed sensors, you must have additional space free on the /var partition, as follows:

43 MB for Intrusion Sensors

43 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](#).

After 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 Defense Center 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, contact Nortel Support.

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

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

Upgrading the Defense Center

After you upgrade the Defense Center, you can use it to upgrade the sensors that it manages.

To upgrade a Defense Center:

1. Download the Defense Center 4.5.1.5 upgrade script (Nortel_TPS_Defense_Center_Patch_4.5.1.3_to_4.5.1.5_Upgrade-#.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 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 and reboot the Defense Center.

The upgrade is installed and the Defense Center 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 Defense Center 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, contact Nortel Support.

7. After the upgrade finishes and the Defense Center reboots, log into the Defense Center.

8. Select **Operations > Help > About** and confirm that the software version is listed as 4.5.1.5.

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, including:

- upgrading managed sensors

- installing the latest SEU and reapplying intrusion policies to detection engines on your Defense Center and any managed Intrusion Sensors

- updating the vulnerability database (VDB) on the Defense Center and any RTI Sensors or RTI Software that it manages

For more information, see [After You Upgrade](#).

Upgrading Managed Sensors

You can use the Defense Center to upgrade managed sensors.

Note that if your managed 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 sensor has a fail-open network card, some traffic may pass through the sensor uninspected while it reboots.

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

- upgrade the Defense Center and verify that the sensors are successfully communicating with it

- make sure that the sensors are running the correct version of the Nortel TPS software

- make sure that both the Defense Center and the sensors have enough free disk space to perform the upgrade

For information on these requirements, 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_Real time_Intrusion_Patch_3.5.1.3_to_3.5.1.5_Upgrade-#.sh

- for the Intrusion Sensor,
Nortel_TPS_Intrusion_Sensor_Patch_4.5.1.3_to_4.5.1.5_Upgrade-#.sh

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 to which 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 to which you pushed the upgrade script and click **Install**.

10. Confirm that you want to install the upgrade and reboot the sensors.

The upgrade is installed and the sensors reboot.

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.

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

for RTI Sensors, 3.5.1.5

for Intrusion Sensors, 4.5.1.5

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

installing the latest SEU and reapplying intrusion policies to detection engines on your Defense Center and any managed Intrusion Sensors

updating the vulnerability database (VDB) on the Defense Center and any RTI Sensors or RTI Software that it manages

For more information, continue with [After You Upgrade](#).

After You Upgrade

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

download and import the latest SEU

reapply intrusion policies to any IDS/IPS detection engines you configured on managed Intrusion Sensors

Note that you **must** reapply intrusion policies regardless of whether you had to import a new SEU. 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.

download and install the latest vulnerability database (VDB), then push and install the VDB update on any managed RTI Sensors or RTI Software.

For more information, refer to the Defense Center User Guide.

II Uninstalling the Upgrade

Regardless of where you started, uninstalling the upgrade results in a Defense Center running Release 4.5.1.3. For information on uninstalling Release 4.5.1.3, 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**.

4. Confirm that you want to uninstall the upgrade and reboot the Defense Center.

The upgrade is removed, the Defense Center reboots, and the Defense Center reverts to Release 4.5.1.3.

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.

5. After the uninstall finishes and the Defense Center reboots, log into the Defense Center.

6. Select **Operations > Help > About** and confirm that the software version is listed as Release 4.5.1.3.

II Known Issues

There are no new known issues with Release 4.5.1.5. However, this release is cumulative from version 4.5.1, so be sure to review the known issues in the release notes for previous releases.

II Product Compatibility

Release 4.5.1.5 of the Defense Center can manage:

versions 4.1.x and 4.5.0 through 4.5.1.5 of the Intrusion Sensor

versions 3.1.x and 3.5.0 through 3.5.1.5 of the RTI Sensor

versions 3.1.x and 3.5.0.1 of Nortel RTI Software for Red Hat Linux

IMPORTANT! Although you can use a version 4.5.1.5 Defense Center to manage version 4.1.x Intrusion Sensors and version 3.1.x RTI Sensors, the sensors themselves cannot be patched for the daylight savings time issue. Nortel **strongly recommends** that you upgrade your sensors to a supported version as soon as possible.

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 noninfringement 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.