Nortel Defense Center

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 a problem where the web interface did not display the source or destination IP address nor the source or destination port for compliance events generated from RTI flows.
- Fixed a problem where compliance rules would not fire when matching the IDS event message using the **is** or **is not** constraint.
- Fixed an issue where intrusion event email alerts may have included incorrect messages.
- Fixed a problem where syslog alerts for compliance events based on RTI flow data events did not include IP address information.
- Intrusion rule messages longer than 64 characters are no longer truncated in the web interface and alerts.
- Fixed a problem that occasionally caused poor network map performance.
- Fixed a problem where editing an network interface may stop traffic from being processed by the detection engines.
- Fixed an issue that prevented intrusion rules from propagating from the primary to the secondary Defense Center in a high availability configuration.
- 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.

- Increased the length of intrusion event message names forwarded to Event Streamer clients to 256 characters.
- 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 the Defense Center occasionally ran out of memory in large-scale deployments.
- Fixed an issue where the data correlator consumed excessive CPU resources.
- Fixed an issue where RTI would generate a service event every time an ftp connection used EPSV to transfer data.
- Fixed an issue where RTI Software on Intrusion Sensors consumed excessive resources and stopped processing traffic.

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 (4.5.1 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

- you have enough free disk space

  You must have at least 10 MB of free space on the `/` partition and 52 MB of free space on the `/var` partition to complete this upgrade successfully.

  If you plan to use the Defense Center to upgrade managed sensors, you must have additional space free on the `/var` partition, as follows:

  - 14 MB for Intrusion Sensors
  - 13 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 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, please 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. From the Nortel Customer Support site, download zip file: TPS_IS_DC_4_5_1_2.zip.

2. Extract the Defense Center 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.**

   The Install Update page appears.

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

7. 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, please contact Nortel Support.

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

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

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

11. 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
- updating the vulnerability database (VDB) on the Defense Center and any RTI Sensors or RTI Software that it manages

For more information, see the sections that follow.

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 Customer Support site.

- for the RTI Sensor, `Nortel_Realtime_Intrusion_Patch_3.5.1.1_to_3.5.1.2_Upgrade-34.sh`
- for the Intrusion Sensor, `Nortel_TPS_Intrusion_Sensor_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.

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, and 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, 3.5.1.2
- for Intrusion Sensors, 4.5.1.2

After You Upgrade

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

- install the latest SEU and reapply intrusion policies to the detection engines you configured on managed Intrusion Sensors
- update the vulnerability database (VDB) on the Defense Center and any RTI Sensors or RTI Software that it manages

Note that updating the VDB takes a variable amount of time depending on how many hosts are in your network map. For example, updating the VDB when your network map includes 10,000 hosts takes approximately 10 minutes, while updating the VDB when your network map contains 170,000 hosts can take up to 3.5 hours.

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

Uninstalling the Upgrade

Regardless of where you started, uninstalling the upgrade results in a Defense Center running Release 4.5.1.1. For information on uninstalling Release 4.5.1.1, 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 4.5.1.1.

   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.

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 4.5.1.1.

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 Defense Center are available on the Nortel Customer Support site.
- If you modified the `user.conf` file on your Release 4.1.x Intrusion Sensor, those changes are not maintained when you apply an intrusion policy to the sensor using a Release 4.5.1.2 Defense Center. If you need to recreate those modifications, contact Nortel support.
- In high-availability environments, sensors in groups may be duplicated on the Sensors page (**Operations > Sensors**).

Product Compatibility

Release 4.5.1.2 of the Defense Center can manage:

- versions 4.1.x and 4.5.0 through 4.5.1.2 of the Intrusion Sensor
- versions 3.1.x and 3.5.0 through 3.5.1.2 of the RTI Sensor
- versions 3.1.x and 3.5 of Nortel RTI Software for Intrusion Sensors

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

- Email Nortel Support at support@nortel.com.

Thank you for using Nortel products.