Cambium Network Updater Tool

Release Notes

System Release 4.13.3

Cambium Networks™

Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Cambium Networks assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party Software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement. See the legal notices and license agreement section of the Network Updater on-line help document.

© 2019 Cambium Networks, Inc. All Rights Reserved.

Table of Contents

1 Overview

The Network Updater Tool is a free-of-charge tool that applies packages to upgrade various device types. Because this tool is available, an operator does not need to visit each module in the network or even each AP where they would otherwise use the SM Autoupdate capability of the radios.

Certain devices such as ePMP Series and some backhauls do not support the SM Autoupdate feature. For these cases, Network Updater reports to the user that this feature does not apply. However, user can directly upgrade the SMs using the CNUT.

1.1 Support added in this release

Network Updater Release 4.13.3 contains the below enhancements or fixes from earlier versions.

1. Warning message about the existence of PMP430 SM when trying to upgrade an AP to 16.1 or later firmware versions added

2. Warning message about PMP 450/450i/450b SMs running 15.1.5 or earlier software versions added

3. Added support for PTP550 and ePMP3000 device upgrade

4. Added showwarnings option in CLI so that the warning message appears in CLI and not in the GUI

5. Corrected the command line for External Tools

6. Restricted the size of External Tool name to 50 characters

7. Fixed the issue of device type format getting changed when the network is saved

8. "Invalid upgrade image" error message changed to "Incorrect upgrade image attempted for specified device Or Failed to set max file size(status:256)".

9. Updated the Introduction in the installer

10. Fixed the issue of the warning message 'SMs running on Firmware version 15.1.5 or lower do not register to AP running 16.1 or higher' popping up even when the AP was on 16.1 or higher while trying to upgrade the AP to 16.1.1 or higher version

1.2 Limitations

This release has following limitations:

1. Due to memory limitation on AP devices, it is recommended to select at only one SM type at a time for Autoupdate, when using The Access Point as File Server, especially in case of PMP 450 AP.

2. CNUT will continue to monitor the status of all connected SMs (irrespective of SM type selected). However, the SM types that are not selected, will not be upgraded and error message for such SMs will be "Incorrect upgrade image attempted for specified device Or Failed to set max file size(status:256)."

3. When using CNUT HTTP as File Server for Autoupdate of SMs, irrespective of SM type selected, CNUT will continue to Autoupdate all SMs that are connected to the AP device.

1.3   Network Elements support already available in CNUT

The Network Updater tool is a free-of-charge application that applies packages to upgrade the following device types:

- ePMP Access Point (AP)
- ePMP SM (STA)
- PMP 100 Access Point Authentication Server (APAS)
- PMP 100 Access Point CAP 110 (APL)
- PMP 100 Subscriber Module (SM)
- PMP 450 Access Point (AP)
- PMP 450 Subscriber Module (SM)
- PMP 450b Subscriber Module (SM)
- PMP 450i Access Point (AP)
- PMP 450i Subscriber Module (SM)
- PMP 450m Access Point (AP)
- PMP 450b Access Point (AP)
- PMP 450b Subscriber Module (SM)
- PMP 400/430/500 Access Point (AP)
- PMP 400/430/500 Subscriber Module (SM)
- PMP 320 Access Point (PMP)
- PMP 320 Subscriber Module (CPE)
- PTP 120 Ethernet Bridge 10 Mbps (BH)
- PTP 130/200 Ethernet Bridge 20 Mbps (BH20)
- PTP 110 Ethernet Bridge 2 Mbps (BH2)
- PTP 110 Ethernet Bridge 4 Mbps (BH4)
- PTP 230 Ethernet Bridge Unlimited Mbps (BHUL)
- PTP 230 Ethernet Bridge 10 Mbps (BH10)
- Cluster Management Module micro (CMM)
- Cluster Management Module-4 (CMM4)
- Cluster Management Module-4 14 Port Switch (CMM4-ES14)
- Cluster Management Module-4 8 Port Switch (CMM4-ES8)
- PTP 400 Ethernet Bridge
- PTP 300 Ethernet Bridge
- PTP 450 Ethernet Bridge
- PTP 450i Ethernet Bridge
- PTP 450b Ethernet Bridge

- PTP 500 Ethernet Bridge
- PTP 600 Ethernet Bridge
- PTP 650 Ethernet Bridge
- PTP 670 Ethernet Bridge
- PTP 700 Ethernet Bridge
- PTP 800 Ethernet Bridge
- Element Group (Folder)

Users can upgrade to this release only from its previous release that is CNUT 4.12.8.

1.4 Product and Documentation Links

For links to products and documents about supported network elements, visit the following web pages:

- Network Updater latest-issue documentation at http://www.cambiumnetworks.com/products/software-tools/cambium-network-updater-tool/
- PMP450m, PMP 450b, ePMP Force 190 and other products http://www.cambiumnetworks.com/products/

2 Dependencies of Network Updater

2.1 Supported Operating Systems

This Network Updater release is supported on following OS:

- Windows Platforms
  - Windows Server 2012 R2 Standard Edition[2]
  - Windows 7
  - Windows 10
- Red Hat Enterprise Linux (32/64-Bit OS)
  - Version 6.7 32-bit ES (not AS)
  - For 64-Bit Server, following 32-Bit libraries need to be installed on RHEL 6.7 before installing CNUT
    - glibc
    - libXtst
- CentOS
  - Version 6.x 32-bit (64-bit)
  - For 64-Bit Server, following 32-Bit libraries need to be installed on CentOS 6.7 before installing CNUT
    - glibc
    - libXtst

2.2 Required Ports

This Network Updater release requires the following ports to be open on the host device:

- ftp, Ports 20 and 21 for active; Port 21 for passive
- tftp, Port 69 in UDP
- telnet, Port 23 in TCP
- http, Port 80 in TCP
- https, Port 443 in TCP
- snmp, Port 161 in UDP
- enabling/disabling SM autoupdate, Port 2501 in UDP

2.3 Java Runtime Environment

Since the external tools in this release require that JRE Version 1.5 or later is running on the host machine, the installation tool for this release loads a proper version of JRE.

2

3 Network Updater Software Installation

The installation tool for this release successfully runs on either a machine without Network Updater or a machine that has a previous version of it installed with the following preconditions.

- Installation directory can be chosen by user only in case of fresh installation. In case of migration, the installation takes place at the location of previously installed Network Updater.

- In case user wants to migrate, it is recommended to migrated from CNUT 4.12.8 to 4.13.3

3.1 General Installation Information

The installation of this release is a single-file Bitrock InstallBuilder process. The installation file can be downloaded from http://www.cambiumnetworks.com/support/management-tools/cnut.
The operator downloads either the Windows version (`.exe`) or the Red Hat Linux version (`.run`) of the installer. When the operator double-clicks on the installation file, the wizard assists the operator through the installation. The installation tool automatically detects whether a previous release of Network Updater is already installed and, if it detects one, prompts the operator to upgrade the Network Updater installation on their computer. This is the recommended installation practice, because the tool in this case automatically imports existing preferences and external tools that were associated with the previous release into the installation of the new release.

Important ....Operators who are still running CNUT 4.8 or below should uninstall it before installing this Network Updater release or go through the sequential upgrades.

Full details about installation are provided under the section titled "Installation" in *Cambium Network Updater On-Line Help* that supports this release.

3.2 Launching Installation or Upgrade on Windows

To run the installation on any supported Windows platform, download the file **CNUTInstaller – 4.13.3-windows-installer.exe** to your Network Updater computer and double-click on the file name to execute it.

3.3 Launching Installation or Upgrade on Red Hat Linux

To run the installation on any supported Linux platform, download the file CNUTInstaller-4.13.3-linux-installer.run to your Network Updater computer. Before running the installer in Linux, change the permissions on the downloaded setup file by executing the following command:

chmod +x CNUTInstaller-4.13.3-linux-installer.run

Then, to run the installer, execute the following command:

./CNUTInstaller-4.13.3-linux-installer.run

4   Issues in Network Updater Operation

4.1   Issues resolved with this software release

Issue	Description of Resolved Issue	Item ID
The command line for external tools shows null	After selecting a jar in 'Launch External Tool' null was passed as the argument. This issue has been resolved The CNUTInitRadio.jar is not supported in CNUT and PMP450BWUpdaterTool.jar is replaced by BWUpdaterTool.jar	CNUT-1046
If the incorrect upgrade image is selected for the upgrade, "Invalid upgrade image" message was displayed	"Invalid upgrade image" error message changed to "Incorrect upgrade image attempted for specified device Or Failed to set max file size(status:256). SM:(MAC=0A003E453183)"	CNUT-1074
Device type format changes when a network is saved.	The device type format changed when a network was saved. This issue has been resolved.	CNUT-1052
There was no restriction for the character size of the Name field in 'Add External Tool' in previous releases	With this release there is a restriction of 50 characters on the size of External Tool name	CNUT-1093
Add the support for PTP 550 and ePMP 3000 devices	Added the support for PTP 550 and ePMP 3000 devices	CNUT-1057

Issue	Description of Resolved Issue	Item ID
CNUT 16.1 support [15.1.5 and 430SM] warning messages are not shown for PMP 450m device type	Warning - about the existence of PMP430 SM when trying to upgrade an AP to 16.1 or later firmware versions This warning indicates that upgrading the AP to 16.1 or later firmware versions will result in loosing access to the 430 SMs If [Yes] is selected for this Warning pop-up, the upgrade is proceeded, and the devices are upgraded successfully. If [No] is selected in this Warning pop-up, the upgrade is cancelled Warning - about PMP 450/450i/450b SMs running 15.1.5 or earlier software versions This warning indicates that SMs running 15.1.5 or lower firmware versions do not register to an AP running 16.1 or later firmware versions If [Yes] is selected in this Warning pop-up, the upgrade is proceeded, and the devices are upgraded successfully. If [No] is selected in this Warning pop-up, the upgrade is cancelled	CNUT-1071
To suppress warnings in CLI when PMP 450 AP devices are upgraded to 16.1 or higher and SMs are running on 15.1.5	Added another parameter in the CLI command i.e showwarnings. The decision whether to suppress the warning or not is left entirely to the user. If showwarnings:true , the warning message pops up ,the next course of action depends on the option selected by the user. If showwarnings:false, the upgrade continues without any warnings. If this parameter is not included, then by default it takes false as the value.	CNUT-1104

4.2   Issues acknowledged with this software release

The following issues are acknowledged in this release:

Issue	Description of Acknowledged Issue	Item ID
Canopy PMP 450i SM and PMP 450b SM cannot be auto updated using PMP 450 AP and using AP as file server	As of Software Release 16.2 and later, CNUT Autoupdate using PMP 450 AP as the File Server no longer supports update of 450b and 450i SMs. Use cnMaestro or CNUT HTTP File Server option to upgrade these SMs.	CNUT-1017
Auto Update using CNUT HTTP as file server doesn't restrict to selected Auto Update SM Type	Even if user selects only one of the SM Types, CNUT will perform Autoupdate of all SMs connected to AP device when File Server Type is selected as CNUT HTTP Workaround: Use AP as File Server to upgrade a single SM Type	CNUT-1022
Channel Bandwidth Tool takes null argument in command line	If user manually tries to add Channel Bandwidth Updater tool, Channel Bandwidth Tool takes null argument in command line Workaround: Use default settings to run Channel Bandwidth Updater tool.	CNUT-987
Issues with CNUT Gather Support tool	This works only with IE (and not on Chrome)	CNUT-986
On Linux, the migration doesn't detect if CNUT tool is already running	The migration doesn't fail. Also, it doesn't warn the user that the tool is running and doesn't save the active network. Note: Workaround is to close the tool and save the network before starting the migration scenario on Linux.	CNUT-977
Events are not recorded while Autoupdate is enabled.	No messages are added to the log until Auto update is disabled.	CNUT-828
Updates of PMP-430 APs by a PMP-450 package fail.	While PMP-430 SMs under the AP are successfully updated by the PMP-450 package, the PMP-430 AP is not. Please uncheck PMP 430 SMs while upgrading PMP 450 devices using PMP 450 packages	CNUT-851
Web browsers are not displaying device information from SM auto-discovery.	Regardless of OS platform, data collected through the **Gather SM Passwords and Extract IP Address and SNMP Settings** auto-discovery option is viewable in only the latest version of web browser (latest of Firefox or latest of Internet Explorer). Latest version of Firefox performs best, regardless of OS.	CNUT-574 0019269
For PMP 430 devices, Network Updater disregards the setting in the General Configuration block.	Even if the check box for **Enable SM Autoupdate when an Access Point is Updated** is checked (**Continue updating child elements if parent element fails to update is unchecked**), Network Updater will push the new package to the SMs even if the attempt to push the new package to the AP fails (for example, when the AP package contains an image that is not valid for the AP).	CNUT-211 0021158

Issue	Description of Acknowledged Issue	Item ID
The Create New Folder option is unavailable for saving a network archive file.	As a result of a known issue in Java 1.4 through 1.6 (Bug #4847375), the Create New Folder button in the Windows Save dialog is grayed out (☐) • While **Save In** is set to **My Documents**. • When **Save In** has been set to **My Documents** and then changed to **Desktop**.	CNUT-103 0009787
The encryption type not available from certain SMs.	Network Updater relies on the link table in the radio to *display* the encryption type of the radio. Certain SMs (for example, those that operate on System Release 9.0) do not include this as a field in their link tables. The workaround for this problem is to upgrade the system release in these radios to the current release. However, there is no risk that Network Updater would *upgrade* such a radio with the wrong encryption package, because it correctly discovers the encryption type as it discovers the SM through its IP address.	CNUT-100 0008122
The maximized Network Updater GUI obscures the Windows task bar.	As a result of known issues in Java (Bug #4737788 and 4472411), the GUI overlays and hides the Windows task bar until the GUI is resized (restored) to its last previous size.	CNUT-82 0002321
The Restore (resize) function sometimes does not work on the maximized state of the Network Updater GUI.	As a result of known issues in Java (Bug #4737788 and 4472411), the GUI sometimes cannot be restored to its last previous size from the maximized state. When this occurs, you may move the maximized window by a distance that is sufficient to allow manually resizing it.	CNUT-68 0000971
HTTP or HTTPS server may fail to start.	See Busy Port Will Prevent HTTP or HTTPS Server Start.	CNUT-58 0018693
[CNUT as HTTP file server]: Upgrading device setup is successful but updated status is seen only on manual refresh	The devices get upgraded , but sometimes the updated status is seen only after manually refeshing the devices.	CNUT-1068
[PTP 450 AP : CNUT shows null error when PTP 450 AP and SM are upgraded at the same time. Though the upgrade is successful	The devices get upgraded. But this can be observed on some setups at times. Verification failed: Could not connect to device in order to verify status/version unknown. Please try to manually refresh the NE and verify its status/version. Error occurred while updating device: null .	CNUT-1069
The command line in External Tools shows null for CNUTHwScheduler.jar	CNUTHwScheduler.jar is not supported in External tools, but this jar is still used by Configure Advantage scheduler, so could not be removed from Tools.	CNUT-1046

Issue	Description of Acknowledged Issue	Item ID
[PTP 700]:Devices have telnet enabled but still CNUT gives error as "Message: Error Connecting to device via telnet interface"	This issue has been observed sometimes.	CNUT-1080

4.3   Caveats That Apply to This Software Release

The following caveats apply to or continue to apply in this release.

4.3.1   SMs That Do Not Update

An operator whose autoupdate job includes both P10 and P11 firmware may find that P11 SMs are not being auto updated to a package for Release 11.2 or later. This can occur when the sequence of pushing packages is ordered to allow the P10 SMs to be updated before the P11s, as in the default order.

Where this problem has been observed, the following workaround will resolve it:

1. From the main menu in Network Updater, select **Update→Configure**.
2. In the SM Autoupdate Configuration tab of the Update Configuration dialog, find the Auto Update SM Type table.
3. Click to highlight the row of P11 SM.
4. If this is below the row of P10 SM, click the **Move Up** button to juxtapose these rows, such that P11 SM is above P10 SM.
5. Click **OK** to save this sequence and dismiss the dialog.

4.3.2   Busy Port Will Prevent HTTP or HTTPS Server Start

If another process is using Port 80 when the HTTP or HTTPS server attempts to start, the start will fail, and the following Start HTTP[S] Server error will pop up as the top window in the Network Updater GUI:

```
Failed to start HTTP_or_HTTPS Server:
[...]on port80_or_443 already in use.
```

This message is also thrown to the log as a SEVERE event. Although you can resolve the barrier to launch, a hasty response can have consequences. It is strongly recommended that, when you have identified the process that is blocking by using the port, you research any adverse effects of killing that process before you kill it.

To find the process

- in Windows, open a Command Prompt window (from Accessories) and enter **`netstat -ano|findstr :`*`80_or_443`***.

- in Linux, at the OS command prompt, enter **`netstat -ano|grep :`*`80_or_443`***.

For either case, the system returns a tabular line that includes a Local and Foreign IP address (with `:`*`port_number`* appended) and whose last column is populated by the *`process_ID`*, which typically is a numeric string of four or fewer characters. Carefully research the source of that process, particularly to find out whether stopping that process will have effects that are adverse.

If you are certain that the effects would be benign, then you can kill the process as follows:

- In Windows, perform the following steps:

    1. Right-click in an unoccupied area of the task bar at the bottom of the desktop.

    2. From the resulting drop-down list of options, select **Task Manager**.

    3. In the Windows Task Manager window, click the Processes tab.

    4. From the main menu of this window, select **View**➔**Select Columns**.

    5. In the Select Columns window, check the check box of **PID (Process Identifier)**.

    6. Click **OK**.

    7. Scroll to find the PID that is using the port (Port 80 or 443).

    8. Click to highlight the row of that process.

    9. Research whether and how the process may be essential and/or should not be interrupted. For example, you can perform an Internet search on the executable file name and study remarks from the returned results.

    10. If you are certain that the process can be stopped without consequences that are damaging, click the **End Process** button at the bottom of the Windows Task Manager window.

        If you are uncertain, allow the process to run until its completion.

- In Linux, perform the following steps:

    1. Search the Internet for the string **PID** *n*, where *n* is the string that you saw in the PID column.

        Research whether and how the process may be essential and/or should not be interrupted. For example, you can perform an Internet search on the executable file

    2. name (that the PID search results associated with the PID) and study remarks from the returned results.

    3. If you are certain that the process can be stopped without consequences that are damaging, enter **`kill`** *`PID`*.

        If you are uncertain, allow the process to run until its completion.

4.3.3   Auto Update logs not shown on CNUT UI until it is disabled

If auto update status is not updated on CNUT UI and logs but the connected SM are getting auto updated, exit CNUT and re launch the application.

4.3.4   HTML Entity Symbols Problematic

Because of how Network Updater processes passwords, HTML entity symbols (special characters such as, but not limited to ~,!, and @, °, ª, á, é, í, ó, and ú) as characters in configured passwords typically prevent the associated user from logging into Network Updater. Although a particular symbol may not prevent log in, all operators are advised to ensure that none of the passwords associated with users, even the root user, contain any of the entity symbols.

Similarly, the inclusion of these special characters in the values of the **Site Name**, **Site Location**, and **Site Contact** fields typically causes processing problems for Network Updater storage as XML data and should be avoided.

4.3.5   Semicolons Problematic in External Tools and Radios Passwords

Network Updater's external tool interface uses a semicolon delimited list to pass input parameters to the external tools. One of the input parameters is the radio password. If a radio password contains a semicolon, and that element is selected to be manipulated by an external tool (either a customer supplied external tool or one of the tools included with the Network Updater installation), issues may be encountered in the proper processing of the tool and/or element. To work around this issue where External Tools usage is desired, the user should change the passwords on the network elements, such that they *do not* contain semicolons.

4.3.6   CNUT Failed to extract SM information for 13.3 firmware

If the canopy devices are on 13.3 firmware version, even if the SMs are set to discover by their public IP during auto-discovery, they may get discover without their public IPs. This is a firmware issue. However, we can access the SM device directly using its public IP and perform actions like upgrading/downgrading/refresh directly.

4.3.7 CNUT logs may sometimes show SEVERE exceptions due to low network connectivity, but upgrades are successful

While device is upgrading, the CNUT logs sometimes show **"SEVERE Exception: response headers not sent yet"** but still device is able to upgrade successfully. This behavior is random in nature and may be due to slow network connectivity. Ignore this exception, as the device is properly getting upgraded"

4.3.8 CNUT logs show SNMPIOException if the device is set to SNMP Read-Only.

Set the device to SNMP read-write to avoid this error.

4.3.9 CNUT GUI or CNUT through CLI randomly gives Invalid File Image (Status 211) error though rerunning the same process, upgrade happens successfully.

This is a random behavior that CNUT upgrade using GUI or CLI gives Invalid File Image (Status 211). We need to either reboot the device or rerun the upgrade process. After this the upgrade is successful from GUI and CLI as well.

Resources for Support

Network Updater Help

These release notes call attention to changes in the Network Updater tool. The effects of these changes are fully described in the document *Cambium Network Updater On-Line Help* for this release. The user should search that document for information before consulting other sources of information. From the Network Updater application main menu, select **Help☐Contents** to open that resource.

Community Forum

The technical support Community Forum is part of the support web site and can be used for asking questions directly to the support team. Questions and answers are accessible to all so that any customer can benefit from the same dialogue. To access this forum, visit http://community.cambiumnetworks.com. This forum requires authentication for posting.

Technical Support

You can obtain support Network Updater from any or all of the following sources:

- *Cambium Network Updater On-Line Help*, and release notes. See http://www.cambiumnetworks.com/support/management-tools/cnut.
- Cambium Networks support web page: http://www.cambiumnetworks.com/support/
- This page provides links to information on all products and tools, as well as access to customer support materials and interactive support forums. Some of these resources are restricted to registered users and channel partners.
- The Community Forum Page http://community.cambiumnetworks.com/
- Direct contact with Cambium Networks Technical Support. This contact is available 7 days a week, 24 hours a day. To find the appropriate phone number based on your country or region, visit http://www.cambiumnetworks.com/support/contact-support.
- A technical support case, which you can open at http://www.cambiumnetworks.com/support/open-a-support-case. The case captures basic information about answers you are seeking or the problem that your network is experiencing and provides this to the support team, who are available 7 days a week, 24 hours a day, and will respond. They will also provide a case number by which you and they can continue to track progress on issues that require deeper investigation.