

# **Cambium Network Updater Tool**

## **On-Line Help**

**System Release  
5.0.2 and Later  
Issue 1**



August 2021  
© 2021 Cambium Networks. All Rights Reserved.

August 2021

## **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 [Legal Notices and License Agreement](#).

August 2021

# Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>9</b>
1.1	About the Network Updater Tool .....	9
1.2	About this Help Document .....	9
1.2.1	New in This Issue .....	9
1.2.2	Intended Use .....	10
1.2.3	Terminology .....	10
	Highlighted Element.....	10
	Selected Element .....	10
	Modules vs. Radios .....	10
1.2.4	Related Documentation .....	11
1.2.5	Feedback .....	11
	Feedback on Network Updater Tool .....	11
	Feedback on Help File .....	11
1.3	Recommended Minimum Computer Configuration.....	11
<b>2</b>	<b>Key Network Updater Concepts.....</b>	<b>12</b>
2.1	Auto Discovery .....	12
2.2	Back Office .....	13
2.3	SM Autoupdate Feature .....	13
2.4	Network .....	15
2.5	Network Element Addressing – IP Addresses and Hostnames.....	16
2.6	Image Package Files .....	16
2.7	Element Groups (Folders) .....	16
2.8	Installation Package .....	17
2.9	Network Layers and Orders of Updating Equipment .....	17
2.10	Upgrading High-speed Backhauls .....	18
2.11	Time Duration Estimates to Complete a Network Upgrade.....	19
2.12	Script Engine .....	20
2.13	Subscriber Modules Accessibility: Routable IPs versus AP LUIDs.....	21
<b>3</b>	<b>Installation .....</b>	<b>21</b>
3.1	Uninstalling Network Updater .....	21

August 2021

3.2	Installing Network Updater on Red Hat Linux .....	22
3.2.1	Assumptions .....	22
3.2.2	Instructions.....	22
3.2.3	Program Usage .....	23
3.2.4	Caveats .....	23
3.3	Installing Network Updater on Windows .....	23
3.3.1	Assumptions .....	23
3.3.2	Instructions.....	24
3.3.3	Program Launch .....	31
3.4	Installation Restriction .....	31
<b>4</b>	<b>Configuration and Settings .....</b>	<b>32</b>
4.1	Security of Tool and Data.....	32
4.2	Configuration Files and Directories .....	32
4.2.1	Archived Log Files .....	32
4.2.2	Network Archive Files.....	32
4.2.3	Preference File .....	33
4.3	Network Communications .....	33
4.4	Tool Dependencies .....	34
4.4.1	Operating Systems Supported .....	34
4.4.2	Java .....	34
4.4.3	Release Supported .....	34
4.5	External Tools Included.....	34
4.5.1	Custom Local Tools.....	35
4.5.2	Configure Advantage Platform Scheduler .....	36
	Features .....	37
	Specific Operations .....	37
	GUI .....	39
	Running Parallel Instances of Tool .....	40
4.5.3	Gather Customer Support Information.....	41
	Features .....	41
	Specific Operations .....	41
	<i>Generating a Report File involving several Elements in a Network Updater Archive.....</i>	<i>41</i>
	<i>Extracting and Viewing the Contents of a Report File .....</i>	<i>43</i>
4.5.4	Reboot Unit .....	43
4.5.5	Set Access Point Authentication Mode .....	45
4.5.6	Set Autoupdate Address on APs.....	46
4.5.7	Set SNMP Accessibility .....	48

August 2021

4.5.8	Set SM/CPE Security .....	49
4.5.9	Bandwidth Updater .....	52
	Adding the Bandwidth Updater Tool .....	53
	Command Line .....	54
	Example .....	54
4.5.10	Using the Bandwidth Updater Tool .....	55
<b>5</b>	<b>Network Updater Operations.....</b>	<b>56</b>
5.1	Quick Start Examples .....	56
5.1.1	Upgrading a Single Radio before Deployment .....	56
	Assumptions.....	56
	Steps to Perform a Single Radio Local Upgrade .....	57
5.1.2	Upgrading a Single AP and its Associated SMs.....	57
	Assumptions.....	58
	Steps to Perform a Single AP Sector Upgrade .....	58
5.1.3	Minimum Actions to Perform Future Network Upgrades.....	59
5.2	Detailed Procedural Operations .....	59
5.2.1	Creating a New Network Archive File .....	59
5.2.2	Adding Network Elements.....	60
5.2.3	Detecting SMs in Network.....	63
5.2.4	Viewing Current Versions .....	64
5.2.5	Current State Information on Network Elements .....	65
5.2.6	Identifying Installation Package for Performing Upgrades .....	65
5.2.7	Ensuring the Network is configured for Using SM Autoupdate .....	66
5.2.8	Determining Where SMs Will Obtain Package Files.....	67
5.2.9	Initiating or Discontinuing a Network Upgrade .....	67
5.2.10	Scheduling an Upgrade for a Future Time .....	69
5.2.11	Examining the Network for Straggler Elements to be upgraded.....	69
5.2.12	Disabling Autoupdate after all SMs have been upgraded .....	69
5.2.13	Saving Status Information in the Network Archive File .....	70
5.2.14	Refreshing the Status Information upon Start-Up.....	70
5.2.15	Package cannot be removed while devices are in upgrade state.....	71
5.2.16	Using Network Updater to Run Auxiliary Scripts against your Network .....	71
5.2.17	Improved Update Tracking .....	72
5.2.18	Improved Auto-Update Tracking .....	72
5.3	GUI Menu Operations .....	72
5.3.1	File Menu.....	72
	File→New Network Archive .....	72
	File→Load Network Archive.....	73

August 2021

File→Save Network Archive .....	73
File→Save Network Archive As .....	73
File→ <i>any of five most recent files</i> .....	73
File→Exit .....	74
<b>5.3.2 Edit Menu .....</b>	<b>74</b>
Edit→Preferences .....	74
Edit→Show/Hide Extended Element Information .....	77
Edit→Manage Subscriber Module Password List.....	79
Edit→Add Elements to Highlighted Element .....	79
Edit→Add Elements to Network Root.....	81
Edit→Remove Selected Elements .....	82
Edit→Modify Selected Network Element Access .....	82
Edit→Change Network Element Type.....	85
Edit→Move Selected Network Elements .....	86
Edit→Open Highlighted Network Element Web Page .....	86
Edit→Undo Network Changes .....	86
Edit→Find.....	86
Edit→Cancel Current tasks.....	86
<b>5.3.3 View Menu .....</b>	<b>87</b>
View→Refresh/Discover Entire Network.....	87
View→Refresh/Discover Selected Network Elements .....	87
View→Refresh/Discover Selected Network Branches .....	87
View→Continuous Refresh .....	87
View→Clear History Log Window .....	88
View→Show Full History Log .....	88
View→Debug on .....	89
View→Horizontal Scroll Deep Tree .....	89
<b>5.3.4 Update Menu .....</b>	<b>89</b>
Update→Configure .....	90
<i>SM Autoupdate Configuration Tab</i> .....	92
<i>HPAP Channel Bandwidth Tab</i> .....	94
Update→Http Server Configure .....	98
Update→Manage Packages .....	100
Update→Update Entire Network Root .....	104
Update→Update Selected Network Elements.....	104
Update→Update Selected Network Branches .....	105
Update→Enable/Disable APs for SM Autoupdate .....	105
Update→TimeOut Configurations .....	105
Update→Schedule Network Update.....	107
Upgrades are non-blocking .....	109
Update→Upload Certificate to Selected Elements .....	110
Update→Upload Certificate to Selected Branches .....	111
<b>5.3.5 Tools Menu.....</b>	<b>111</b>

August 2021

Tools→Add External Tool to Menu .....	111
Tools→Edit External Tool Menu.....	113
Tools→Launch External Tool.....	113
Included Network Updater External Tools .....	114
<b>5.3.6 Help Menu .....</b>	<b>114</b>
Help→Contents.....	114
Help→Tools→ <i>ToolName</i> .....	114
Help→About .....	115
<b>5.4 User Convenience Actions .....</b>	<b>115</b>
5.4.1 Right click to manipulate selected element .....	115
5.4.2 Double click to modify element .....	115
5.4.3 Select all Elements of a branch .....	115
5.4.4 Sorting Network Elements by Column Values.....	116
5.4.5 Change Order of Columns Displayed .....	116
5.4.6 Change Display Size of Column Displayed.....	116
5.4.7 Last Settings on External Tools Remembered .....	116
5.4.8 Mouse-Over Display of Tree Contents .....	116
<b>6 Command Line Operations .....</b>	<b>117</b>
6.1 Introduction .....	117
6.2 Usage for Direct Update of device.....	117
6.3 Usage for SM Autoupdate of PMP450 devices.....	118
<b>7 Building Custom External Tools.....</b>	<b>123</b>
7.1 Parameters Passed to External Tools .....	123
Host Address.....	123
ESN (Element Serial Number) .....	123
MAC Address .....	123
Element Type .....	124
Encryption Type .....	124
SNMP Community String .....	124
Device Login ID/Password .....	125
Software Version String .....	125
Software Boot String .....	125
FPGA Version String .....	125
Site Name .....	125
Site Contact .....	125
Site Location .....	125
Detected Parent .....	125
Detected Parent Password .....	125

August 2021

7.2	External Tool Help.....	126
7.3	External Tool Extended Attributes.....	126
7.3.1	Java Extended Manifest Attributes .....	126
<b>Acronyms and Abbreviations .....</b>		<b>127</b>
<b>Legal Notices and License Agreement.....</b>		<b>129</b>
<b>Troubleshooting .....</b>		<b>134</b>
	Autoupdate source address is not set on APs .....	134
	An error is thrown when I try to enable SM Autoupdate on an AP .....	134
	Update of network elements works, but SM Autoupdate never activates on APs.....	135
	Network Updater server IP address changed, and SM Autoupdate no longer works .....	135
	SM Autoupdate with external TFTP server is not working .....	135
	AP telnet Interface shows Autoupdate disabled after Network Updater enables it .....	136
	Network Updater tries to update an already updated SM when using SM Autoupdate.....	136
	Update of radio devices works fine, but updates of CMM micro platforms fail.....	136
	I am applying an update to an unsupported release .....	136
	Network Updater does not discover or update SMs .....	136
	An AP goes down during an update .....	137
	If my radio web interface is locking up, will Network Updater still work? .....	137
	I cannot downgrade my R8.x radios to R7.x .....	137
	An HSBH link dropped during an upgrade, and the far-end HSBH does not respond .....	137
	Network Updater hangs loading packages or performing an update.....	138
<b>Resources for Support.....</b>		<b>138</b>
	Network Updater Help.....	138
	Community Forum .....	138
	Technical Support .....	140



# 1 Introduction

## 1.1 About the Network Updater Tool

The Network Updater Tool is a free-of-charge tool that applies packages to upgrade the device types that the release notes for the release that you are using list as supported. 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 PMP 320 Series APs and SMs 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.

## 1.2 About this Help Document

### 1.2.1 New in This Issue

Network Updater Release 4.12.8 contains the below enhancements or fixes from earlier versions.

1. Upgrade of devices when DNS Name is used in place of IP address and HTTPS server
2. CNUT should remove the requirement for encryption type in the package name
3. CNUT hang issue addressed when AES-128 disabled downgrades are performed
4. Vulnerability Issues in CNUT addressed.
5. CNUT transfers all files to 450i/450m AP regardless of SM Autoupdate Configuration issue addressed.
6. CNUT cannot Auto upgrade PMP 450i SM and PMP 450b SM, registered to PMP450 AP issue addressed.

August 2021

7. Support added for PTP 670 devices
8. Auto Update using new Auto Update SM Types supported using CLI
9. CLI working for Auto Upgrade using CNUT as file server (HTTP)
10. Customer Reports CNUT 4.11.2 Hangs on SM Update issue is addressed.
11. Support of 3G 450m device type

## 1.2.2 Intended Use

This Help documentation should be used with the Network Updater tool. The audience for this tool and document includes system operators and network administrators.

These help files cover the entire graphical user interfaces of the tool, as well as the supporting concepts and configurations required ensuring proper operation of the tool. In addition to detailed functional descriptions of each feature found under [GUI Menu Operations](#), this help file provides [Detailed Procedural Operations](#) for performing network upgrades and provide a set of [Quick Start Examples](#) on how to use the tool. Troubleshooting and support information is included at the end of the help file.

## 1.2.3 Terminology

### Highlighted Element

When this document mentions the highlighted element, it refers to moving your mouse over any portion of its row and clicking on it such that the row becomes highlighted. This action is typically used when you are manipulating a single network element.

### Selected Element

When this document or a GUI option mentions the selected element, it refers to clicking in the check box at the front of a network element line such that a check mark appears in that box. This method is used to specify one or more network elements upon which to perform a complex operation, such as initiating an update to, launching an external tool on, or performing mass changes to elements.

### Modules vs. Radios

These help files make use of the term *modules* when referring to all network components, such as APs, SMs, BHs, and CMMs. When a comment only applies to the RF portions of the network, the term *radios* is used. In this context the term radios can be considered a subset of modules.

August 2021

## 1.2.4 Related Documentation

The user may find other documentation useful in understanding concepts or manipulating the network in conjunction with the Network Updater tool; in particular

- system release notes (on the radios)
- Cluster management module (CMM) user guides (on manually updating a CMM).
- Release-specific system user guides and their successor, *Fixed Wireless Broadband IP Networks User Guide: PMP 100 PMP 400/430 PTP 100 PTP 200*, (on manually updating an AP, configuring an AP for network communications and management control, and the SM Autoupdate feature).
- *Prizm Release 3.3 User Guide* (on network discovery).

## 1.2.5 Feedback

Cambium Networks welcomes and encourages feedback on our products and our documentation. Please feel free to make use of these mechanisms for letting us know your thoughts and inputs on the Network Updater tool.

### Feedback on Network Updater Tool

If you have input on how Network Updater tool is working or need to report a problem with the tool, we encourage you to send those to technical support at the email address listed under [Technical Support](#) for your region.

### Feedback on Help File

We welcome your feedback on documentation, including feedback on structure, content, accuracy, completeness, or other comments you have. Please send your feedback to <http://www.cambiumnetworks.com/>

## 1.3 Recommended Minimum Computer Configuration

The following should be considered when selecting a computer to run the Network Updater tool.

The Network Updater tool supports either Windows or Red Hat Enterprise Linux platforms.

This Network Updater release supports

- Windows Platforms

August 2021

- Windows Server 2012 R2 Standard Edition<sup>1</sup>
- 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 CNUIT
    - 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 CNUIT
    - glibc
    - libXtst

The computer will need network access to connect to the devices being upgraded.

The computer should also have sufficient memory to run the application as well as load the various software packages that will be used to upgrade the devices. A minimum of 512 MB of RAM is recommended, though depending on your network size and number of unique types of devices, you may be able to get away with less RAM. See the topic [Network Updater hangs loading packages or performing an update](#) in the troubleshooting section for more information on memory restriction

## 2 Key Network Updater Concepts

### 2.1 Auto Discovery

Auto Discovery is the capability for the Network Updater tool to automatically populate its network component list with the SMs that are in your network. This information is automatically pulled from the APs, thus saving the network administrator the trouble of entering all of that information, and helping to ensure consistence and accuracy of the network components being manipulated. It should be noted that auto-discovered SMs are referenced through the AP LUID capability instead of through a direct IP address to the SM. Because of this fact, auto discovered SMs must be updated using the SM Autoupdate capability of the system. See [SM Autoupdate Feature](#) for more details.

---

<sup>1</sup>

August 2021

## 2.2 Back Office

The Back Office is the location(s) the network operator runs support infrastructure for their network that does not need to be located at either the CPE or the base station locations. Such support infrastructure may include Billing and Provisioning, Network Monitoring, Network firewall, Mail servers, Internet interconnection equipment, etc.

## 2.3 SM Autoupdate Feature

The radios in series other than PMP 320 have a feature called Autoupdate, which allows an AP to instruct an SM to perform a software upgrade. We will use the term **SM Autoupdate** in this document to clarify that this Autoupdate operation only affects SMs in the network. The AP examines the current software version and FPGA versions on the SM to determine if an update is required, and if required it gives the command to the SM to perform the appropriate update. As a part of the command, the AP tells the SM where it can obtain the latest software and firmware. Options include from

- The AP.
- A specified CNUT HTTP server.
- A specified local TFTP server.

**note** ..... Network Updater only uses TFTP in conjunction with SM Autoupdate if it is located on the same network computer that the Network Updater program is running on.

This feature reduces the amount of individual radio manipulation that is required to upgrade an entire network, but on its own does not prevent the network administrator from individually accessing AP and BH radios and manually performing upgrades of these radios. The Network Updater Tool extends the capabilities provided by the SM Autoupdate features to make a one-touch network upgrade possible.

SM Autoupdate can make upgrading of a network both fast and efficient but, for auto discovered SMs, is the only mechanism to automatically upgrade the software and FPGA on the SMs. This is because, without a direct IP address, the Network Updater cannot directly communicate with an SM, and therefore must rely on the virtual proxy capability through the AP provided by the SM Autoupdate feature to initiate upgrades of these SMs.

**important** ..... SM Autoupdate is supported for SMs whose **Network Accessibility** parameter (in the IP tab of the SM's Configuration management web page) is set to **Local**, not **Public**. Even where Network Updater can discover SMs as children of their APs, if their **Network Accessibility** is set to **Public**, then Network Updater *must* discover them directly.

Network Updater initiates and terminates the SM Autoupdate mode within APs by using the HTTP, HTTPS, or TFTP protocol. The SM Autoupdate mode in an AP remains active only until the user turns it off (manually or through another command that Network Updater sends) or the AP reboots. For security purposes, the AP accepts this command from a single IP address, which is specified in the AP configuration pages. For convenience, Network Updater automatically sets this value in the AP to the IP address of the Network Updater server when it performs any of the update commands

August 2021

([Update→Update Entire Network Root](#), [Update→Update Selected Network Elements](#), or [Update→Update Selected Network Branches](#)). These operations can use either an IP address specified by the user or a detected IP address that the AP derives from its communications with Network Updater. As long as the user performs an update operation before enabling the SM Autoupdate capabilities on the AP (by using the operation [Update→Enable/Disable APs for SM Autoupdate](#)), there will be no communication issue between Network Updater and the AP. For the case where the user wishes to set the IP address in the AP separate from the automatic setting, Network Updater provides an auxiliary script that allows the user to do this. For details on this script, see [Set Autoupdate Address on APs](#).<sup>2</sup>

The user should be aware that since Network Updater uses the UDP command method for enabling and disabling of SM Autoupdate on APs, the user may not get an accurate status response from the AP if they are using the Telnet interface on an AP to inquire on the status of Autoupdate on the AP. This is because the Telnet interface will only report on the status of Autoupdate based on previous Telnet commands – without taking into account if the AP received a separate UDP command for Autoupdate.

Starting with the device Release 8.1, software images were delivered in two platform formats (big Endian and little Endian formats) to support two different CPUs running on the radios. The capacity of the file system on an AP handles the software images for only one platform at a time. This means that SM Autoupdate, when finished with the AP as the image distribution site, can handle only one type of SM at a time. To address the issue where a single AP is communicating with SMs of both CPU formats, Network Updater automatically monitors the progress of SM Autoupdate in each sector of the network, and switches the images and instructions given to the AP from one set of images to the other after all SMs of the initial format have been updated. Network Updater starts the Autoupdate process on a given sector using the image format associated with the *majority* of the SMs within the sector. After Autoupdate activity within the sector ceases for a period of time, Network Updater detects whether SMs of the other platform type exist in the sector and, if they do, switches the AP to administer SM Autoupdate images for the other platform type. This image swapping on the AP can continue until either all active SMs are updated or SM Autoupdate is turned off in Network Updater.

Later packages support the Network Updater capability to

1. Scan the SMs that are registered to the selected AP and thus retrieve their hardware platform versions.
2. Run Autoupdate to those SMs that have the most common hardware platform version in the sector, and then run it to those that have the next-most common, and so forth.

---







<sup>2</sup> For more information on Network Updater script capabilities, see [Script Engine](#).

August 2021







## 2.4 Network

The Network referred to by the Network Updater is the set of AP, SM, BH radios as well as CMM platforms that have upgradeable software (such as CMM Micro). It is assumed that the network operator has deployed these components within a single network layout, such that a computer in the back office or at the POP can communicate with these modules for management purposes. Although Network Updater refers to *Network Elements* in a generic sense, the user can assume that each network element represents a device in their network.

The release notes will always provide the full list of network element types that the current Network Updater release supports. Network Updater uses the following set of icons to represent various elements within your network:

Icon	Device Type
	PTP 300/400/500/600/650/700/800 HSBH
	PTP 110 BH2/BH4 PTP 120 BH PTP130/200 BH20 PTP 230 BHUL PTP 230 BH10 PTP 450 BH PTP700 PTP650 PTP 670 PTP 450i PTP 450b
	PMP 320 Series AP
	PMP 100/450/500 AP PMP 450i AP PMP 450m PMP 450b AP PMP 100 APAS PMP 100 APL ePMP AP
	PMP 400/430 AP
	PMP 100/450/500 SM PMP 450i SM PMP 450b SM PMP 450b SM ePMP STA

August 2021

Icon	Device Type
	PMP 320 Series SM
	PMP 400/430 SM
	CMMmicro
	CMM4
	CMM4-ES14 (14-port switch) CMM4-ES8 (8-port switch)
	Group (non-element)

## 2.5 Network Element Addressing – IP Addresses and Hostnames

Network elements are directly referenced by the Network Updater through the use of IP Addresses supplied by the user. The Network Updater also supports the use of standard Hostnames, which are basically alias names for IP addresses. Hostnames are automatically translated by the Network OS layer into IP addresses through the use of either DNS servers or a local `/etc/hosts` file on Linux or the `C:\WINDOWS\system32\drivers\etc\hosts` file on Windows platforms.

## 2.6 Image Package Files

“Cambium networks” uses a variety of image package files for controlling modules. For a given device, these may be a software file (referred to by its software release name), a software boot file (referred to by its boot file name), and a firmware file (referred to by its firmware file name). The firmware file sometimes referred to as an FPGA release. For CMMs with upgradeable software, there is one CMM software file (referred to by its CMM software name). Network Updater hides most of this complexity from the users by packaging all variations of the upgrade files into a single installation package file (see [Installation Package](#)).

## 2.7 Element Groups (Folders)

For user convenience, network elements can be combined into user defined element groups (folders). These groups or folders can help organize the display of the various network elements, such as by AP cluster or regional distribution. By selecting a group level item, the user can simultaneously perform operations on all elements within the group. Group level defaults can be set for the device login ID and password as well as the SNMP community string values to be used for all elements within the group.



August 2021

**note** ..... Any element within the group can override the group level default with a specific value for only that element if required. The user need not create any groups if they don't wish to, but there is always one group created at the top level by the Network Updater tool, which is referred to as Network Root.

## 2.8 Installation Package

An installation package for Network Updater is a pre-packaged set of software, boot, and hardware files for all versions of radios and CMM platforms. The administrator does not need to open or individually manipulate these files when using Network Updater. Network Updater can intelligently extract the correct files from the package for the specific modules in question, including distinguishing the need for AES or DES encryption loads. A manifest file that is embedded in each package, which can be viewed through the **Manage Packages** operation, provides details of the contents of each package (see [Update→Manage Packages](#)).

There are three versions of the Network Updater Installation Package format:

Network Updater Version	Radio System Release	Package
1.00	4.1 through 7.3	Uses package format . pkg
1.10	4.1 through 7.3	
2.00	7.x <sup>1</sup> and later	Uses package format . pkg <sup>2</sup>
2.20	7.3.6 <sup>2</sup> and later	
3.10, 3.20, 4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10 and later	8.4 and later	Uses package format . pkg <sup>3</sup>
<b>NOTES:</b> 1. Not all historical release may be available in the new package format. Consult the Cambium Networks website for package availability. 2. Earlier packages if needed may be available through Technical Support.		

## 2.9 Network Layers and Orders of Updating Equipment

A network can contain multiple layers of equipment; with a layer meaning that one piece of equipment is behind (receiving its network connectivity through) another piece of equipment. For example, an AP may be behind a BH, or SMs are behind an AP. It is important to properly portray

August 2021

these layers of the network within Network Updater, so that Network Updater can perform module and AP cluster upgrades in an appropriate order. Proper layer information ensures that Network Updater does not command an AP that is behind another AP/SM pair (such as a remote AP installation) to do an upgrade at the same time as the SM that is feeding the AP. If this was done then the remote AP would lose its network connection in the middle of an upgrade when the SM it was attached to complete its upgrade and rebooted. The section [Adding Network Elements](#) contains additional details about laying out your network hierarchy within Network Updater, specifically for APs, SMs, PTP 100 Series Ethernet bridges, and CMM type devices. When upgrading HSBHs some additional care is needed in defining the element hierarchy, this is documented under [Upgrading High-speed Backhauls](#).

## 2.10 Upgrading High-speed Backhauls

HSBHs have the unique requirement that the far side of a link must be upgraded prior to the near side. By far side it is meant the side of the link for which communications from the Network Updater computer are required to traverse the wireless link between the two ends of the backhaul pair. During the upgrade process of the HSBHs the two ends of the link will lose communications after one unit has been updated, and will not regain communication until the second side is updated to the same software release as the first unit. Therefore, if the far side is not upgraded first, the loss of communication will prevent access to the far side and prevent a successful upgrade of the backhaul link.

To support this requirement, Network Updater will automatically place PTP links in a hierarchal mode when refreshing the network elements. During a Firmware upgrade, Network Updater will update both ends of the links simultaneously. This will prevent any issues with units losing connectivity.

While the above process is automatic, it may be necessary to manually perform updates on units.

The following is the manual way that HSBHs should be updated using the Network Updater tool:

1. When defining the hierarchy of the HSBH link, the parent device should be the far side of the link and the child should be the near side of the link.
2. Upgrades should always operate on both sides of the link in the same operation.
3. The Continue Updating Child Elements if Parent Element Fails to Update option must be set before initiating the upgrade of the HSBH pair (see [Update→Configure](#)).
4. After the parent unit (far side) is updated, the Network Updater will attempt to verify the upgrade. This verification will fail due to the loss of the link during the upgrade process. Ignore this failure error.
5. After the child unit (near side) is updated, Network Updater will perform a verification of the child's upgrade, which complete with a successful state message.
6. After the upgrade operation has completed, perform a **Refresh/Discover Selected Network Elements** operation on the parent units (see [View→Refresh/Discover Selected Network Elements](#)). This will gather current information on the far side of the link which should now be communicating with the near side again and clear out the failure message seen in Step 4 above.

Because of this slightly different process and paradigm involved in upgrading HSBHs in the network, the Network Updater user may find it easier to create a separate Network Archive file just for performing upgrades on their HSBH elements of their network.

August 2021

## 2.11 Time Duration Estimates to Complete a Network Upgrade

The amount of time it will take to upgrade any network will vary based on multiple factors, such as (generally in order of biggest impact to smallest):

- The total upgrade time will also be affected by the speed and performance of the computer that is running the Network Updater tool and the number of simultaneous update sessions they specify in the Update Configuration window (see [Update→Configure](#)).
- If SM Autoupdate is being used to upgrade the SMs in the network.
- The total number of network elements being updated,
- The configuration (hierarchy) of the network elements,
- The type of elements being updated

It takes approximately 4.5 minutes to update a network element. This time includes file transfer time to push the new software and FPGA to the element, programming time to burn in the new files to the module, and time to reboot the element using the newly upgraded software and FPGA. This time is reduced if only the software or only the FGPA of the element is being upgraded.

A network upgrade typically requires the following amounts of time:

- 30 seconds to transfer the software and FPGA files to an element
- 80 seconds to burn in the FPGA load into an element
- 130 seconds to burn in the software load into an element
- 30 seconds to reboot an element

The AP in SM Autoupdate mode has the following capacity:

- AP Supports up to 4 simultaneous updates of software/FPGA files to SMs when SM Autoupdate is enabled and the AP is used as the file server.
- AP Supports up to 20 simultaneous updates of software/FPGA files to SMs when SM Autoupdate is enabled and a local HTTP or TFTP server is used.

The following tables shows some network upgrade times. These assume a release with new software and FPGA for each element, that SM distribution is even across all APs, and that all SMs are on the network and available for update. The layer number refers to how many hops away the furthest network element is from the Network Updater computer.

**Estimated example network upgrade durations**

Layer 1	Layer 2	Layer 3	Layer 4	Layer 5	Layer 6	Elements	Notes	Estimate
1 BH	1 BH	6 APs	200 SM	N/A	N/A	208	1,3,5	59 mins
1 BH	1 BH	6 APs	200 SM	N/A	N/A	208	2,4,5	23 mins
3 BH	3 BHs	36 AP	2,000 SM	N/A	N/A	2,148	1,3,5	122 mins

August 2021

Layer 1	Layer 2	Layer 3	Layer 4	Layer 5	Layer 6	Elements	Notes	Estimate
+ 6 AP	+ 100 SM							
3 BH + 6 AP	3 BHs + 100 SM	36 AP	2,000 SM	N/A	N/A	2,148	2,4,5	41 mins
3 BH + 12 AP	3 BHs + 1,000 SM	2 BH + 36 AP	2 BH + 3,000 SM	24 AP	2,000 SM	6,082	1,3,5	189 mins
3 BH + 12 AP	3 BH + 1,000 SM	2 BHs + 36 AP	2 BH + 3,000 SM	24 AP	2,000 SM	6,082	2,4,5	68 mins
<b>NOTES:</b> <ol style="list-style-type: none"> <li>1. Uses the AP as the file transfer server for SM Autoupdate.</li> <li>2. Uses an external TFTP server for SM Autoupdate – assumes TFTP server can handle all connection requests and network bandwidth is not a limiting factor between TFTP server and SMs.</li> <li>3. Uses default value of 4 simultaneous updates from Network Updater.</li> <li>4. Increases simultaneous updates from Network Updater to 20.</li> <li>5. Time estimates do not consider time for switching SM Autoupdate image types on an AP. Estimates assume only one image type of SMs is on the same AP.</li> </ol>								

Overall these examples are meant to emphasize that the processing power of the Network Updater computer (to support higher simultaneous updates) and the depth of the network tree are the most significant factors to determine how long a network upgrade will take. The breadth of the tree, though it represents most of the elements in the network, does not greatly affect the upgrade time when the SM Autoupdate capabilities are fully used.

Since the SM Autoupdate feature is not available in PMP 320 sectors, the breadth of the tree can be a significant factor in the time required to complete a complete sector upgrade.

## 2.12 Script Engine

The Script Engine is the capability within the Network Updater to run any user defined script against any network component or group of components. This can be very useful for management scripts or any other script that is run repetitively across your Network. By having this capability within the Network Updater, it ensures you are running your script across all of your components (because of the Network Updater's Auto Discovery capability), and allows you to maintain one master list of all equipment you need to run scripts against. The Network Updater refers to these user-defined scripts as External Tools. See [Building Custom External Tools](#) for additional information on this topic.

August 2021

## 2.13 Subscriber Modules Accessibility: Routable IPs versus AP LUIDs

There are two ways SMs in a network can be accessed. The more direct way is if a routable IP address is assigned to the SM such that a user on a management server on the network can directly access the SM (such as through the Network Updater tool). By default, an SM has a non-routable IP address assigned, so unless the network operator changes this for the SM, direct access to the SM is not possible. In that instance, the SM can be accessed by first communicating with the AP that the SM is attached to, and then referencing the SM by the LUID assigned by the AP to the SM. The LUID is a value assigned by the AP when the SM registers with it. The Network Updater will only be able to directly update SMs that have routable IP addresses assigned to them.

All other SMs must be updated using the SM Autoupdate feature (see [SM Autoupdate Feature](#)), which can be controlled and managed through the Network Updater. In general, most SMs should be updated by the SM Autoupdate capability as it allows greater concurrent updates to occur throughout the network thus minimizing the overall time a network upgrade requires. However, SM Autoupdate is not available in PMP 320 series sectors. In these sectors, SMs are updated in parallel directly by Network Updater, and the AP plays no role in the update.

Individual upgrades to address one-off issues can be done directly to an SM in instances where most of the network does not need to be upgraded, or a special software load is being put on one or more SMs for testing or other purposes.

## 3 Installation

### 3.1 Uninstalling Network Updater

The Network Updater Tool comes with an uninstall program that can be run by the user. Generally, when upgrading from one version of Network Updater to another, there is no need to uninstall the previous version unless it is not just the immediate previous release. If you wish to downgrade from a higher version to a lower, you may not be able to do this without uninstalling the higher release version first. If this is not done, then installation errors, such as not being able to properly select the installation directory for the downgrade may occur.

**Important** ..... When downgrading Network Updater from a new version to an older version, it may be necessary to uninstall the newer version before installing the older version.

August 2021

## 3.2 Installing Network Updater on Red Hat Linux

### 3.2.1 Assumptions

1. You have a Linux machine with a supported version already installed and are able to open a command line terminal.
2. You have `root` access to the Linux machine in which you will be installing this software.
3. There is a functioning web browser available on the machine for use by the Network Updater help system, under one of the following commands:

```
mozilla
firefox
htmlview
```

If this is not true, then the user may need to edit the `CNUTLauncher.sh` script within the Network Updater installation directory to indicate the name and/or location of their web browser before being able to access on-line help for the tool.

### 3.2.2 Instructions

1. Download the Network Updater setup package at the following web address using the Mozilla web browser that comes included with Red Hat Linux:  
<http://www.cambiumnetworks.com/products/software-tools/cambium-network-updater-tool/>
2. Save the file in `/tmp`.
3. Skip to Step 4 if you're already logged in as root. Otherwise, enter the following shell command:  

```
su -
```
4. Enter the root password when prompted and press the **Enter** key.
5. Enter one of the following sets of commands:
  - To perform a GUI based installation, enter  

```
cd /tmp
chmod 755 CNUTInstaller-4.12.8-linux-installer.run
./ CNUTInstaller-4.12.8-linux-installer.run
```

where `CNUTInstaller` is the name of the Linux installer downloaded from the software delivery web site.
  - To perform a console-based installation, enter  

```
cd /tmp
chmod 755 CNUTInstaller-4.12.8-linux-installer.run
./ CNUTInstaller-4.12.8-linux-installer.run -console
```

where `CNUTInstaller` is the name of the Linux installer downloaded from the software delivery web site.

August 2021

6. Follow the on-screen instructions for reviewing and accepting the software license agreement and completing the installation.

### 3.2.3 Program Usage

1. Type the following command at a Linux terminal:  
`CNUTLauncher.sh`
2. If you receive an error about the networkupdater command not being found, it probably means that your PATH environment variable is not set up. You can either update your PATH environment variable with the following command:

```
export PATH=$PATH: /usr/local/cambium/networkupdater
```

Alternatively, you can simply run the program by specifying the full location to the networkupdater program:

```
/usr/local/cambium/networkupdater/CNUTLauncher.sh
```

You will see the Network Updater menu bar appear on screen.

### 3.2.4 Caveats

If you choose to perform a custom installation and did not install Java then, when you start the Network Updater, you may be prompted to locate java on your system. This information will be stored on the system for future use, and you will not be prompted again. Because of this, please make sure that all users of this program have access to the same Java installation (for example, avoid installing Java in a home directory when running as a regular user, as this may prevent other users from using your Java installation).

The installer writes out a log file of installation if you should encounter any installation difficulty. This file is located at `/usr/local/cambium/networkupdater/log.txt`.

## 3.3 Installing Network Updater on Windows

### 3.3.1 Assumptions

- You have a Windows machine with a supported Windows operating system.
- You have administrator access to the Windows machine in which you will be installing this software.

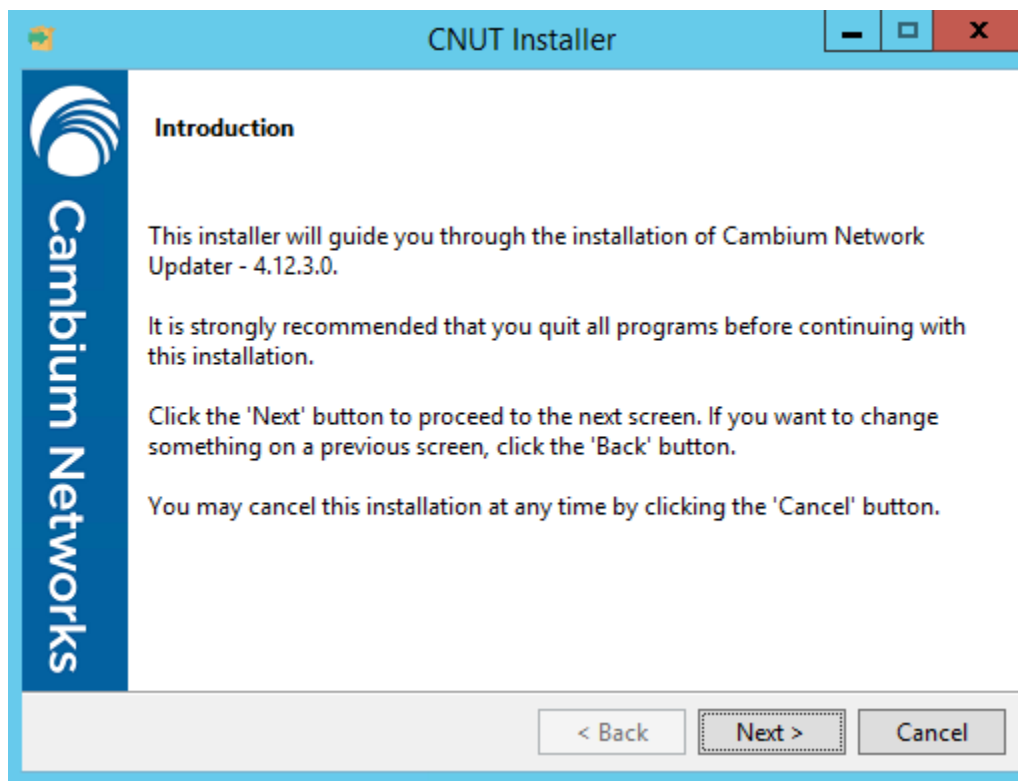
**note** ..... Network Updater installs its own instance of Java.

August 2021

## 3.3.2 Instructions

1. Download the release notes at <http://www.cambiumnetworks.com/products/software-tools/cambium-network-updater-tool/>
2. Read the release notes.
3. Download **Network Updater Tool v4.x.x (Windows)** at <http://www.cambiumnetworks.com/products/software-tools/cambium-network-updater-tool/>
4. Log in as Administrator for the system on which you will install or upgrade Network Updater.
5. Unzip the downloaded software package.
6. Double-click the **CNUTInstaller-4.12.8-windows-installer.exe** icon to begin installation downloaded from the software delivery web site. The installation program prompts for information.

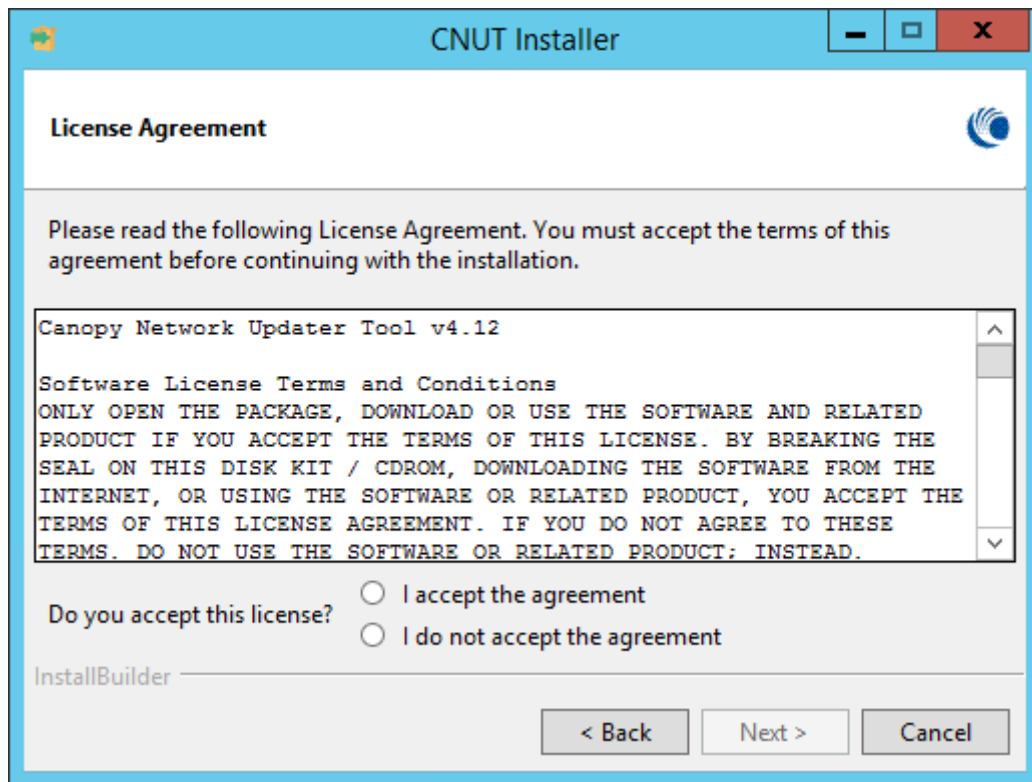
The CNUT Installer Install Builder wizard opens to its Introduction panel.



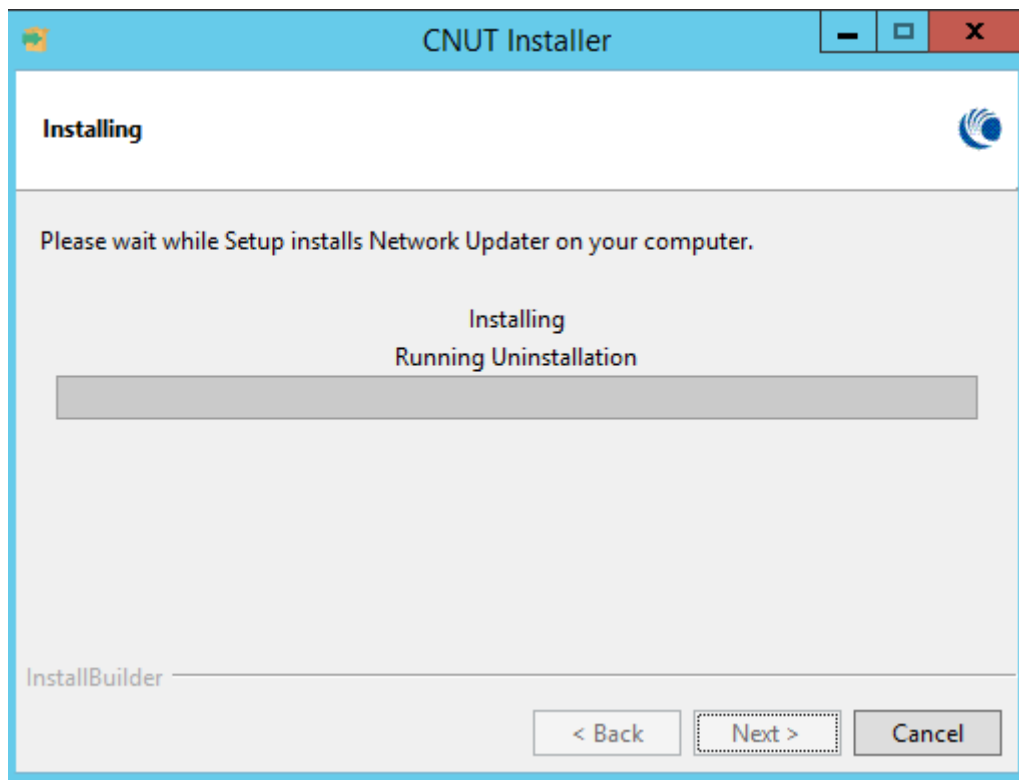
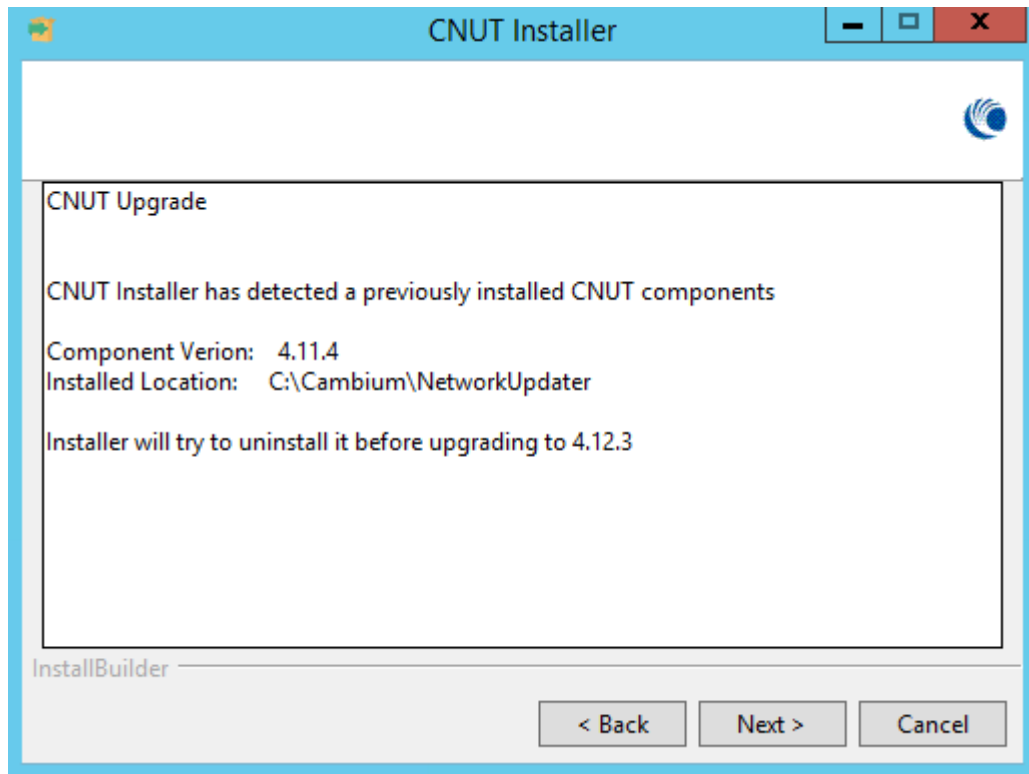
1. Click the **Next** button.  
The License Agreement panel opens.



August 2021

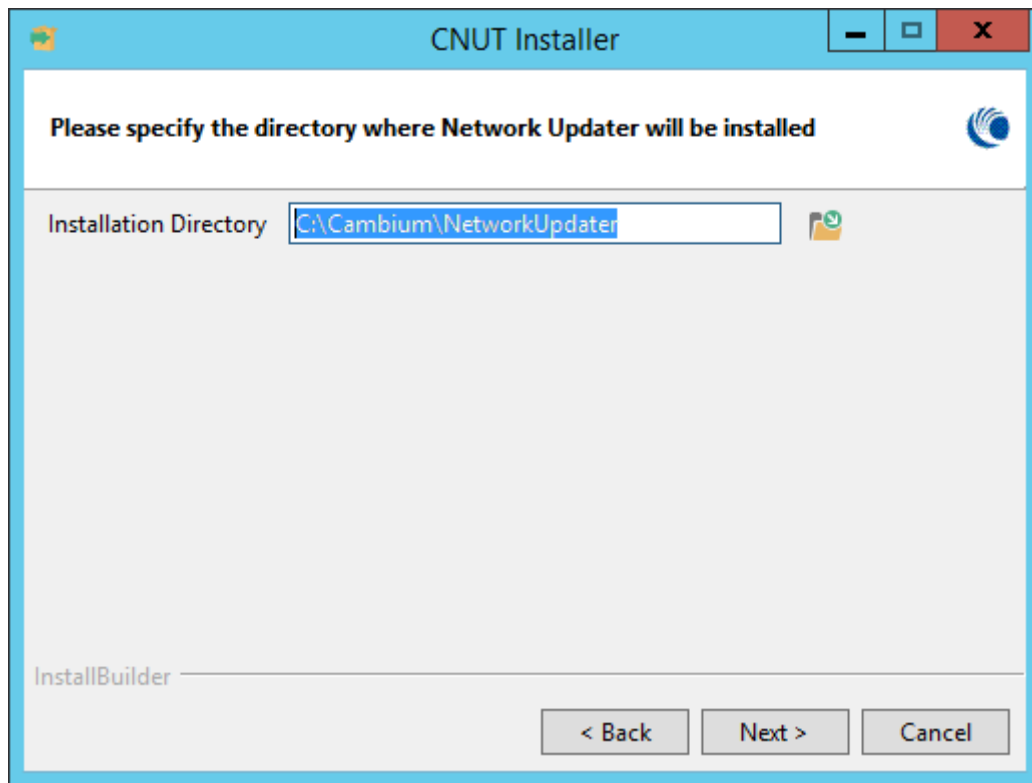


2. Scroll to read the full text of the License Agreement.
3. If you agree, select the I accept the terms of the License Agreement radio button.
4. Click the **Next** button.
5. If a previous release of CNUT is present on your local device, and the wizard opens the CNUT Upgrade panel, click the **Next** button.



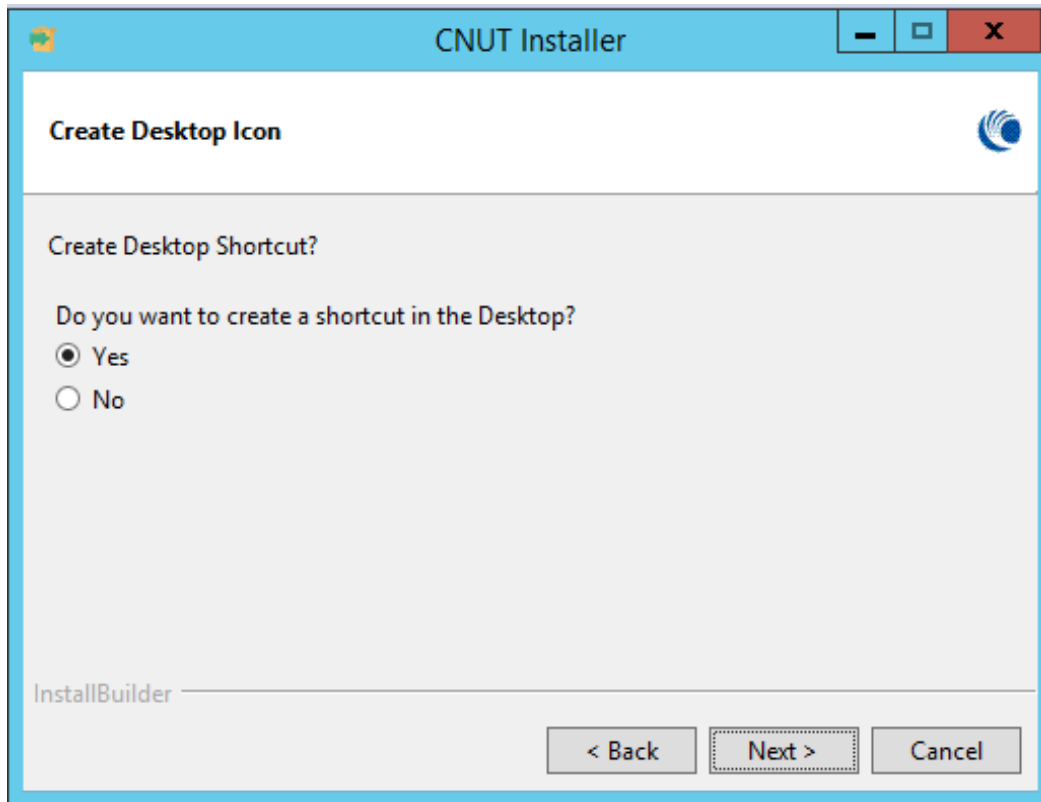
August 2021

6. When the Choose Install Folder panel opens (only in case of fresh install, in case of migration the install directory remains the installed location of previous Network Updater) either
  - Click the **folder icon** to browse to a path where you want to install CNUT and then click the **Next** button.
  - Click the **Next** button to accept the displayed default path  
C:\Cambium\NetworkUpdater



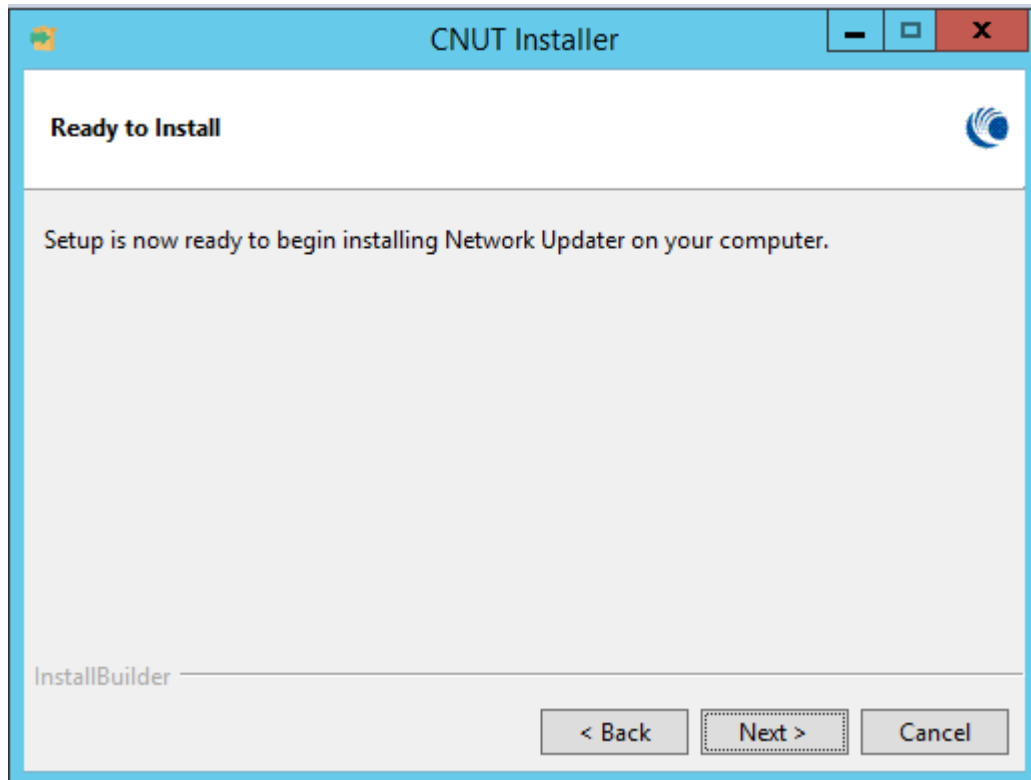
Desktop Icon's choice panel opens

August 2021

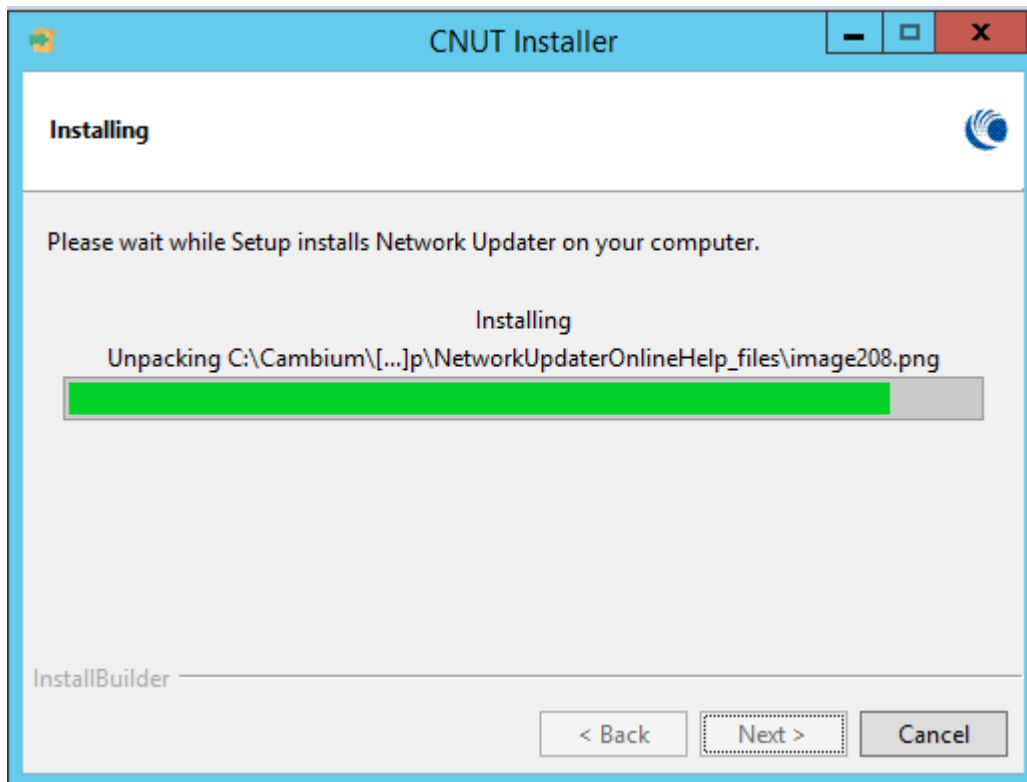


Ready to Install Panel opens

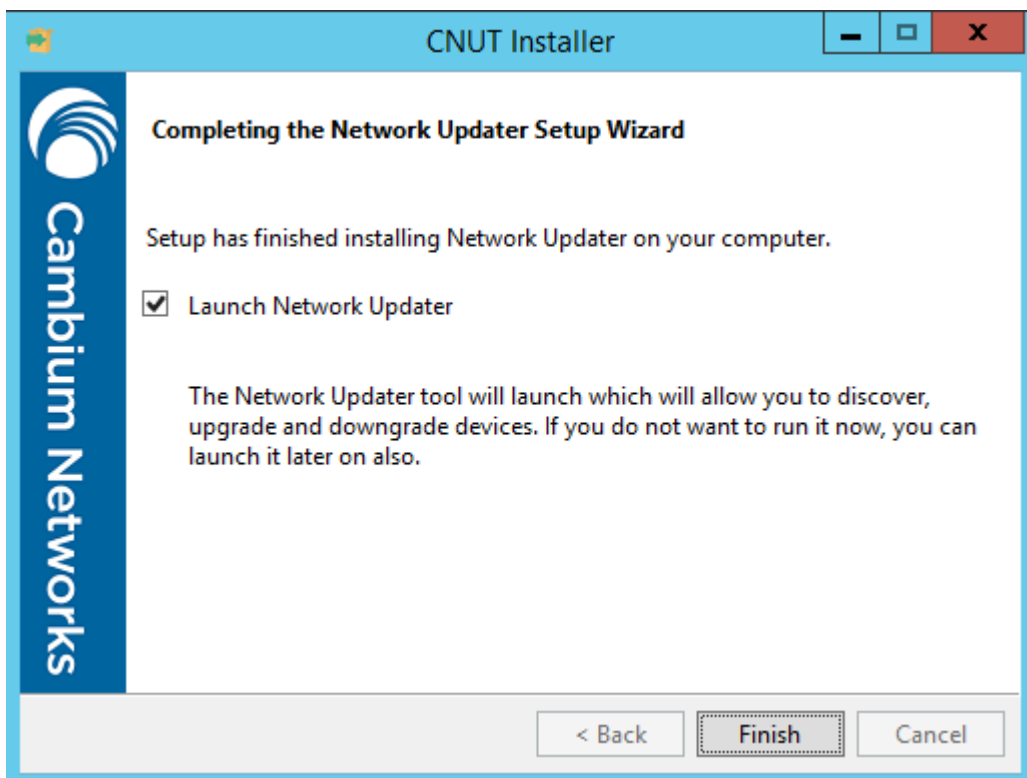
August 2021



1. Ensure that the required amount of disk space is reported in this panel as available.
2. Click the **Next** button.  
The Installing Network Updater panel opens to indicate progress.



When the process has concluded, the Install Complete panel opens and indicates success.




August 2021

- Click the **Finish** button.

The installation tool places the Network Updater shortcut onto the desktop.



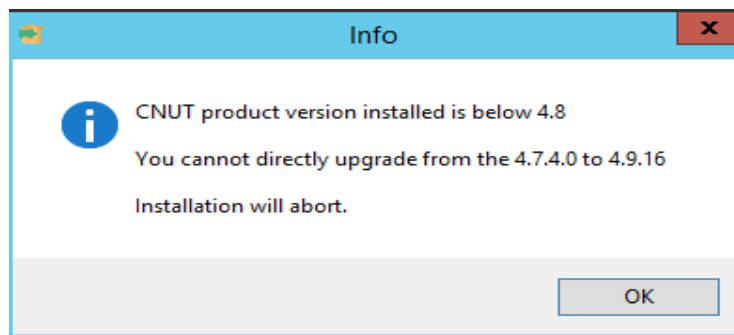
### 3.3.3 Program Launch

Double-click the  icon or, from the **Start** menu, select **Programs→Canopy→Network Updater x.x→Network Updater**. This launches the application.

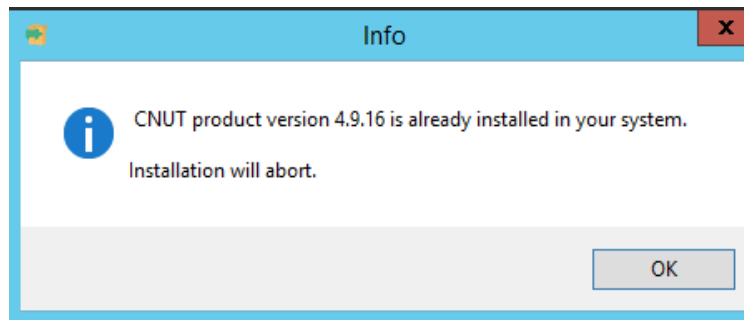
Canopy Network Updater - (New Network)*										
File Edit View Update Tools Help										
Element	Type	ESN	Software Ver.	HW/FPGA Ver.	Boot Ver.	Last Access	State	Progress	Auto Update	
Network Root										
10.120.143.50 PTP700	PTP700	00045658007D	45700-00-05	B0P04.02-C		09/14/15 04:34:04	Refreshed	100%		
10.120.143 PTP700	PTP700	000456580077	45700-00-05	B0P04.02-C-FPS		09/14/15 04:34:05	Refreshed	100%		
10.120.143.45 PTP650	PTP650	000456500018	50650-01-98	B0P01.01-C		09/14/15 04:52:43	Refreshed	100%		
10.120.143 PTP650	PTP650	000456500014	50650-01-98	B0P01.01-C		09/14/15 04:52:43	Refreshed	100%		
10.120.140 IPMP450AP - DES	DES	0A003EA00438	CANOPY 14.1 (Build 2) ... 082815		CANOPYBOOT 1.0	09/14/15 07:06:29	Autoupdate Enabled	100%	Enabled	

## 3.4 Installation Restriction

CNUT 4.9 and above can only be installed either as a fresh installation or migration from the CNUT previous release. This restriction is imposed due to many changes in the canopy-preferences file from much previous CNUT releases. In case, if you are having CNUT 4.7 or previous installed on your system, kindly uninstall it and then fresh install CNUT 4.9.



Previously, CNUT could migrate to the same version that was already installed on the system. That seemed unnecessary, so we restricted this by giving the below info message to user and abort the installation. CNUT 4.9 and later does not allow same version migration.



## 4 Configuration and Settings

### 4.1 Security of Tool and Data

The Network Updater Tool does not provide any security to restrict access to the tool itself or the data stored within its Preference settings or Network Archive Files. It is assumed that the Network Updater Tool is installed on an inherently secure workstation or server and only authorized personnel have access to the tool and its related files. It is not recommended that the tool be installed on a computer open to the outside world without proper external security measures being implemented.

### 4.2 Configuration Files and Directories

Network Updater makes use of several directories within its installation area, and several configuration files.

#### 4.2.1 Archived Log Files

Archived Log files are created when the current log file reaches its maximum size. Archived log files have a name of `nwupdater` with the ending date and time of the file appended to the end of the filename. Archived log files are stored within the `logs` subdirectory. Users may use these archived log files as needed, including parsing them for relevant information using scripts or other mechanisms.

#### 4.2.2 Network Archive Files

Network archive files are used to store all information entered by the user or automatically discovered about a network. This includes element data, element groupings, and package files to be used for upgrading the network. Network Archive files are stored in XML format and should end with



August 2021

.net extensions. The last used Network Archived File is remembered by Network Updater to allow the user to automatically open that file upon startup.

### 4.2.3 Preference File

Session preference information and information on the screen layout settings, last opened Network Archive File, and other session related information are stored in the **cambium\_nwupdater\_pref.txt** file in the **pref** subdirectory. Session information is saved on **Exit** from the Network Updater. The user should not edit or modify this file.

## 4.3 Network Communications

Network Updater runs on a computer in the back-office environment, but needs to communicate with the various network elements in the network, including APs, SMs, BHs, and CMMs. To ensure proper function, the user must ensure that required ports for communications between the computer running Network Updater and network elements are open.

The following are the communications protocols and ports through which Network updater communicates with the network elements. Depending on your network configuration, enabling these may involve your router, firewall, and any hardware or software protocol filters you have running.

Service	Port Used	Protocol
FTP (Active)	20 21	tcp
FTP (Passive)	21	tcp
Telnet	23	tcp
HTTP	80	tcp
HTTPS	443	tcp
TFTP	69	udp
SNMP	161	udp
SM Autoupdate Enable/Disable	2501	udp

TFTP is an UDP service and thus connectionless. Since communications is required in both directions for this service, ensure that two-way communication on the listed port is enabled (from the Network Updater server to the network and from the network to the Network Updater server).

August 2021

## 4.4 Tool Dependencies

Network Updater is dependent on some third-party software components to be properly installed prior to running Network Updater. The Network Updater installation scripts should help identify these dependencies for the user and perform some basic checks to ensure they are configured appropriately for Network Updater's use.

### 4.4.1 Operating Systems Supported

Network Updater has been tested on Windows 2000, Windows Server 2008 R2, Windows XP, Windows 2012, and Red Hat Enterprise Linux v4, Linux 6.6. Other operating systems may also work, but have not been tested and cannot be officially supported by the support organization.

### 4.4.2 Java

Since the external tools in this release require that JRE is running on the host machine, the installation tool for this release loads a proper version of JRE for the exclusive use of the Network Updater Tool.

### 4.4.3 Release Supported

Network Updater supports upgrading or downgrading network from or to all releases starting with system release 4.1. If an operator has a network that is not yet running release 4.1, they should first upgrade their network manually to release 4.1 prior to running Network Updater.

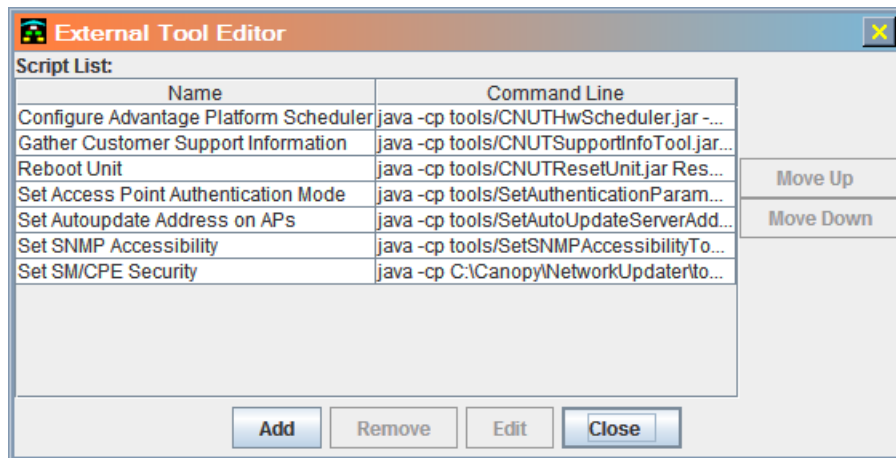
Starting with R8.0 of the system software, installation packages for the Network Updater tool will only work with Network Updater v2.0 or greater releases. The operator should also be aware that radios that are shipped from the factory with R8.0 or higher system releases cannot be downgraded below R8.0. See [Troubleshooting](#) for more details on this topic.

## 4.5 External Tools Included

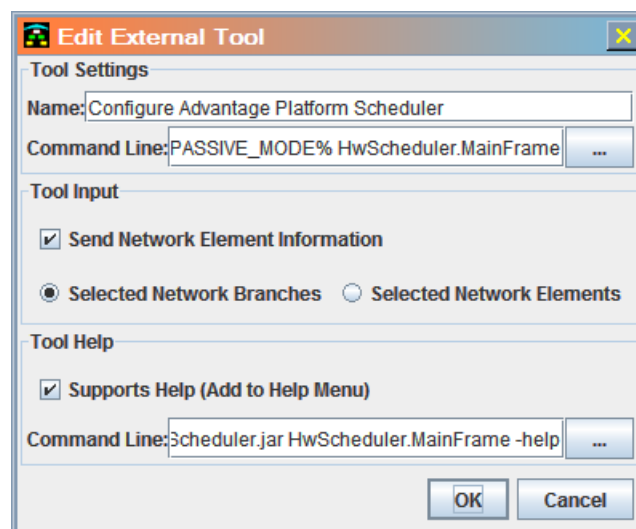
The following External Tools are automatically supplied with the Network Updater. Each of these is either a Java jar file or a Perl script. These specific external tools come preloaded within Network Updater, and each one includes online help for the tool itself (see [Help→Tools→ToolName](#) for more information on external tool help).

The external tools are intended for optional use and customized execution. For this reason, the Network Updater GUI provides the capability to edit an included tool or even to remove it from, and optionally replace it in, the selection list (edit the tool list).

August 2021



If you highlight one of the tools in the External Tool Editor window (accessed via the **Tools→Edit External Tool Menu** command option), click to highlight a specific tool, and then click the **Edit** button, you can modify the properties of that tool.



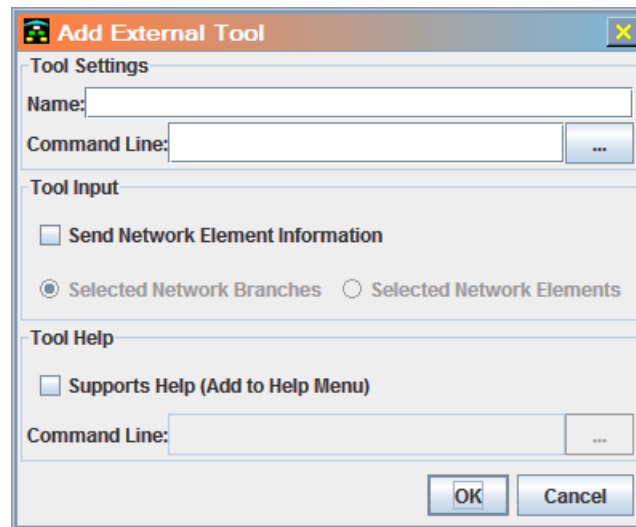
For example, you can rewrite the script for Network Updater to call or even the script that provides help text for the tool when you select the **Help→Tools→ToolName** command option.

If you uncheck the option **Supports Help (Add to Help Menu)** and save your changes, that tool can later be added back into the set of tools for you to access.

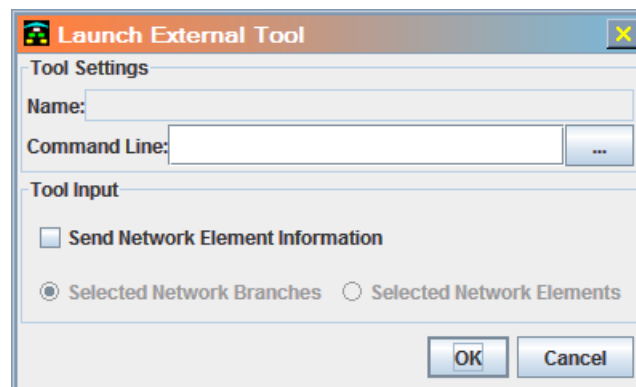
## 4.5.1 Custom Local Tools

You can also add a tool of your own creation to the list, using the **Tools→Add External Tool to Menu** command option.

August 2021



Similarly, you can launch a local script that you have kept out of the menu of external tools. To do so, select the **Tools→Launch External Tool** command option.



## 4.5.2 Configure Advantage Platform Scheduler

The purpose of this external tool is to provide operators with a convenient and controlled/safe manner for enabling/disabling the Hardware Scheduling feature on the Advantage product line. This tool only works on pre-R8.0 release of System software, since all R8.0 and higher releases use only Hardware Scheduling.

Device Release 6.1 implemented a Hardware Scheduler that improves the communications pipe between Canopy Radios. An option exists to toggle between Hardware Scheduling and Software Scheduling.

In order for this new feature to function, it is necessary for both sides of the communications pipe to utilize the same scheduler:

August 2021

- Subscriber Modules (SMs) with hardware scheduling enabled will only be able to communicate/register with Access Points (APs) with hardware scheduling enabled.
- Subscriber Modules (SMs) with software scheduling enabled will only be able to communicate/register with Access Points (APs) with software scheduling enabled.

For newer Subscriber Modules, Hardware Scheduling can be enabled by selecting a Configuration option on the Subscriber Module Web Page. For older Subscriber Modules, Hardware Scheduling can only be enabled in a separate Hardware Scheduler FPGA.

## Features

The Network Updater External Tool for performing batch configuring of the Scheduler Option will support the following options:

- Ensure that only Advantage Access Points (APs) with Release of 6.1 up to but not including 8.0 can be configured.
- Allow Configuring of Subscriber Modules (SMs) with Release of 6.1 up to but not including 8.0 or above.
- Allow Toggling between Hardware and Software Scheduling.
- Allow the configuration option to be automatically propagated to Subscriber Modules currently registered with the AP.
- Provide a GUI to the user to allow selection of the above options.

## Specific Operations

1. User has installed Release 6.1 to AP and SM, and wishes to enable Hardware Scheduling:
  - a. Identify the APs to configure by selecting them on the tree view display.
  - b. Launch the Network Updater External Tool.
  - c. Select the Hardware Scheduler Option. By default, the Option to propagate to SMs is checked.
  - d. Initiate the Configuration changes
  - e. For each AP in the list, the Tool will:
    - i. Check to ensure that the AP is capable of supporting Hardware Scheduling.
      1. If any AP is not capable of HW scheduling, skip it, and notify the user.
    - ii. Check to ensure that the SMs attached to the AP are at a minimum release of 6.1.
    - iii. If any SM is not capable of Hardware Scheduling, skip the AP, and notify the user. (This is to ensure there are no stranded SMs)
    - iv. Set the Scheduler Option for all SMs and reboot them.
      1. If the SM is a newer SM, then just set the HW Scheduling Flag
      2. Else, Flash the SM with the HW Scheduling FPGA
    - v. Set the Scheduler Option for the AP and reboot it.

August 2021

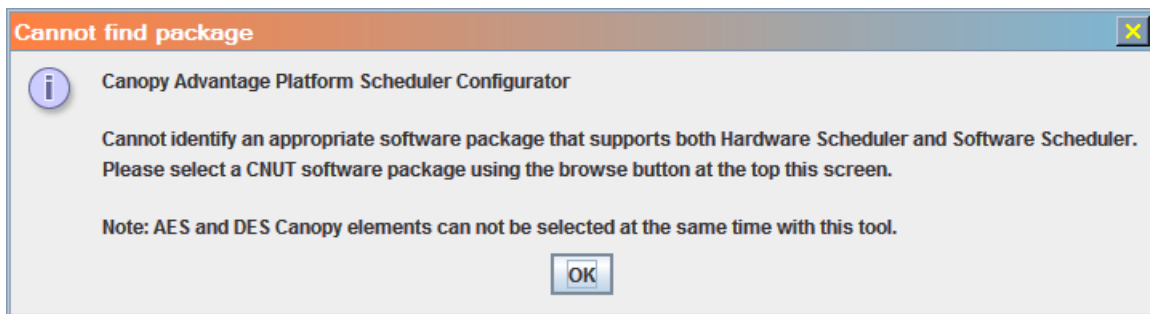
2. User has turned on HW Scheduling, but needs to recover any stranded SMs that are still in SW Scheduling mode.
  - a. Identify the APs to configure by selecting them on the tree view display.
  - b. Launch the Network Updater External Tool.
  - c. Select the Recover Misconfigured Modules Option. By default, the Option to propagate to SMs is disabled.
  - d. Initiate the Configuration changes
  - e. For each AP in the list, the Tool will:
    - i. Set the AP to the opposite of the Targeted Configuration.
    - ii. Reboot the AP.
    - iii. Allow sufficient time for any mis-configured SMs to register to the AP.
    - iv. Apply the Target Configuration to any SMs and reboot it.
      1. If Hardware Scheduler is selected and the SM is not capable of HW Scheduling, flag an error and skip the AP.
        - a. The AP will be left at the current configuration so that the user can reapply Network Update to update the SMs to R6.1.
        - b. On completion of Network Update, the User can re-launch this external tool to reconfigure to Hardware Scheduler
      2. Reset the AP to the target Configuration and reboot it.
      3. Wait for All SMs to register to the AP.
      4. Verify that the Total SMs is as expected (Original Count + Recovered Count).
3. User has installed Release 6.1 to AP and SM, and wishes to enable Software Scheduling:
  - a. Identify the APs to configure by selecting them on the tree view display.
  - b. Launch the Network Updater External Tool.
  - c. Select the Software Scheduler Option. By default, the Option to propagate to SMs is checked.
  - d. Initiate the Configuration changes
  - e. For each AP in the list, the Tool will:
    - i. Set the Scheduler Option for all SMs and reboot them.
      1. If the SM is a newer SM, just select the SW Scheduling Option
      2. Else for older SMs Flash the SM with the SW Scheduling FPGA
    - ii. Set the Scheduler Option for the AP and reboot it.
4. User wishes to directly convert an older SM to Hardware Scheduling:
  - a. Add the SM to Network Updater, and ensure that Network Updater can communicate to it (Direct connect the SM to the PC running Network Updater)
  - b. Identify the SMs to configure by checking them on the tree view display.
  - c. Launch the Network Updater External Tool.
  - d. Select the Hardware Scheduler Option.
  - e. Initiate the Configuration changes
  - f. The Tool will:
    - i. Check to ensure that the SM is at a minimum release of 6.1 and is below Release 8.0.
    - ii. Set the Scheduler Option for the SM and reboot it.
      1. If the SM is a newer SM, then just set the HW Scheduling flag.
      2. Else, for older SMs, Flash the SM with the HW Scheduling FPGA.

August 2021

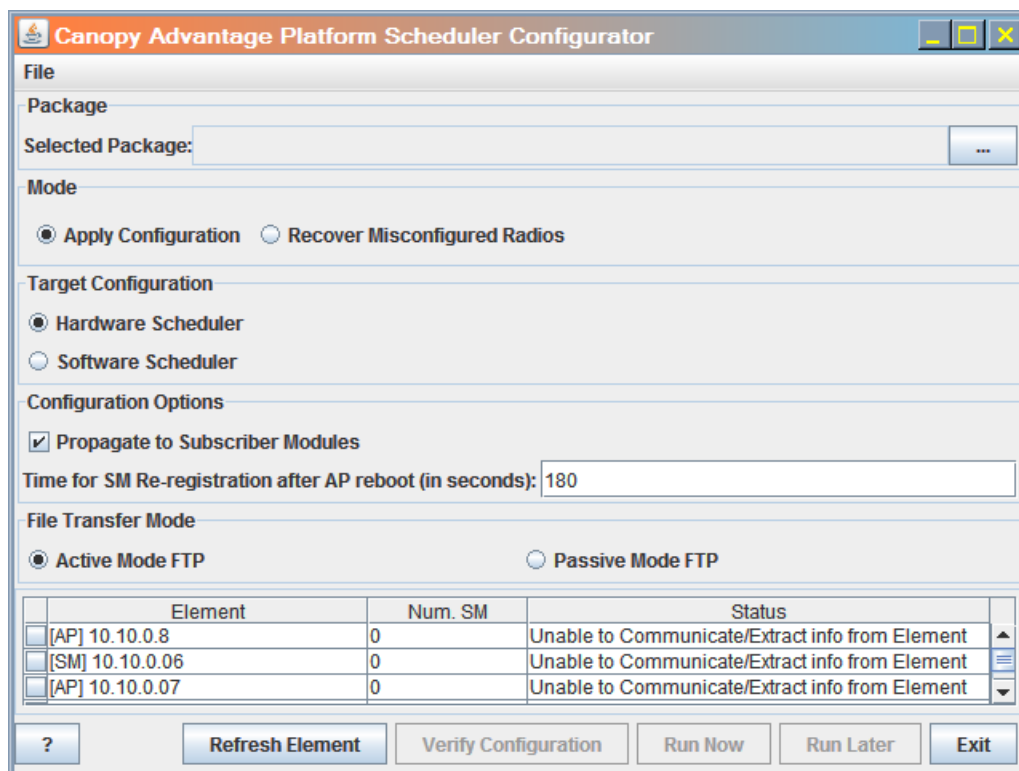
## GUI

If the tool is unable to identify a package that contains FPGAs for Hardware Scheduler and Software Scheduler, the tool pops up a dialog box to select a particular package that contains the FPGAs for both kinds of scheduler.

**note** ..... The tool does not get an up-to-date list of currently selected packages from the Network Updater tool, so you may see this message and be required to specify an appropriate package even if you have such a package active within the Network Updater Manage Packages dialogue.



Otherwise, the main window of the tool will directly appear.



Options:

August 2021

- **Refresh Element:** Connect to the Element, Query its state and that of its Subscriber Modules (If Applicable).
- **Verify Configuration:** Check All Elements against the desired Target Configuration (Hardware or Software Scheduler).
- **Run Now:** Execute the Current Configuration against the Selected Elements.
- **Run Later:** Execute the Current Configuration at a Later Time (See Screen Shots Below).

**note** ..... The scheduled time will be based on your Network Updater computer clock, not any time set on the elements being manipulated.

- **Exit:** Exit the Program.

## Running Parallel Instances of Tool

To optimize the amount of time it takes to change many APs and SMs over to Advantage Scheduler, it is possible to run multiple instances of the Configure Advantage Scheduler Platform tool in parallel, each operating on a different set of APs.

To initiate such parallel instances, the following process can be followed:

1. Select the AP(s) the first instance of the Configure Advantage Scheduler Platform tool should operate on.
2. Launch the tool from the **Tools** menu.
3. Configure and initiate the Configure Advantage Scheduler Platform tool.
4. While the tool is running, return to the Network Updater main window.
5. Select the AP(s) for the second instance of the Configure Advantage Scheduler Platform tool.

**note** ..... Remember to unselect the previous set of APs

6. Launch the tool from the **Tools** menu.
7. Configure and initiate the Configure Advantage Scheduler Platform tool.
8. Repeat as needed, up to the performance capabilities of the computer that is being used.

The user can also make use of the scheduling capability of the Configure Advantage Scheduler Platform tool for each instance of the tool started. In this way they may be able to initiate some instances of the Configure Advantage Scheduler Platform immediately, and schedule others to start in the future at a point where they estimate the initial set of instances of the Configure Advantage Scheduler Platform tool have already completed their operation.

**note** ..... It is highly recommended that all of the APs on a single cluster of APs be upgraded together by the same instance of the Configure Advantage Scheduler Platform. This is due to the fact that as SMs on the cluster are upgraded it is possible (depending on color code and frequency settings on the cluster) for an SM to move from one AP to another during the upgrade process (especially if the SM falls on the barrier line between two AP sectors). The Configure Advantage Scheduler Platform tool has accounted for this possibility, and during the verification step will ensure all SMs have been upgraded across the entire pool of APs it was working on. Therefore, if an SM was properly upgrade, but moved to another AP, this will not be flagged as an issue and will allow the Configure Advantage Scheduler Platform tool to still complete normally.



August 2021

## 4.5.3 Gather Customer Support Information

The purpose of this external tool is to provide operators with a convenient yet effective method to collect pertinent information from the Network Updater Tool and Network Elements for the purposes of submitting to the Customer Support Team. When executed, the Tool will generate a Zip file that contains

- current Network Updater Settings and Logs.
- Status, Event Log and Configuration Web Pages for any network elements that are selected.

The zip file can then be emailed to the Customer Support team, who can use the information contained in the zip file to aid in resolving field issues.

### Features

The External Tool for collecting customer support information supports the following options:

- Attach the current CNUT Preferences File.
- Attach the current CNUT Network Archive File.

The archive file provides contextual information on the Hierarchy of the Network Elements.

The Tool maintains the security of the customer network by removing all Password information from the Network Archive file.

- Attach the current CNUT Event Log File.
- Attach the Status/Event Log and Configuration Web Pages of Selected Network Elements

The Tool extracts web pages for all elements, either directly (through IP Address), or via the AP LUID proxy (for Subscriber Modules that are not directly addressable).

### Specific Operations

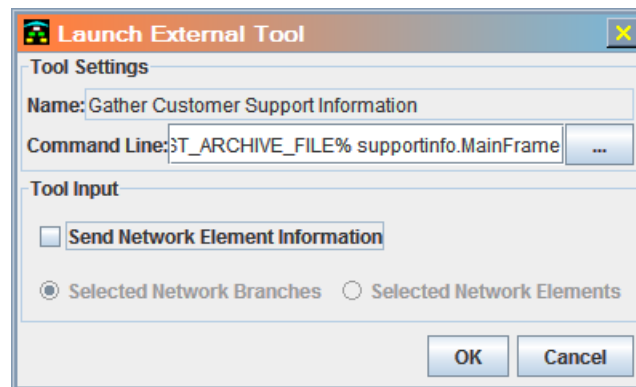
#### ***Generating a Report File involving several Elements in a Network Updater Archive***

4. Select the network elements from within Network Updater.

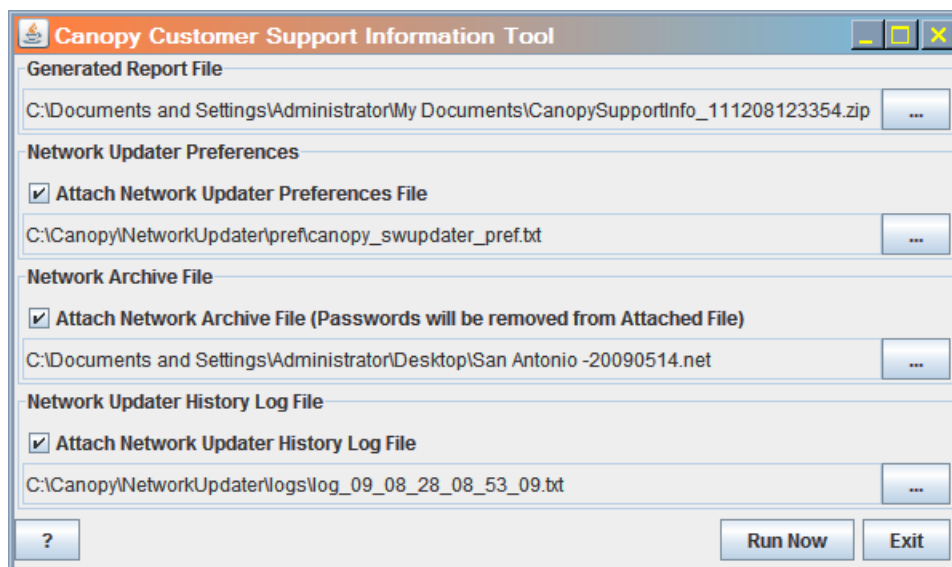
**note** ..... The larger the number of Network Elements that are selected, the longer the Tool will have to execute. This will also result in a larger zip file.

5. Launch **Tools★Gather Customer Support Information**.

August 2021



6. Check the check box for **Send Network Element Information**.
7. Select the radio button of one of the options (**Selected Network Branches** or **Selected Network Elements**).
8. Click **OK**.



9. If desired, change the default file attachment options.
10. Click the **Run Now** button.

The Customer Support Information Tool generates a zip file by the following process:

11. It attaches the current CNUT Preference File to the Zip File.
12. It loads the current CNUT Network Archive File.
13. It removes all password information from the Network Archive File, then attaches this file.
14. It attaches the current CNUT Event Log File to the Zip File.
15. It iterates through all the selected Network Element's and process their Web Pages.

August 2021

16. If the Element is directly accessible via IP Address, it collects the web pages via the Web interface (e.g., `http://ipaddress/status.html`), and attaches them to the Zip File.
17. If the Element is a Subscriber Module without a directly accessible IP Address (e.g., `AP:[169.254.253.10].LUID:[002]`), it sets the current LUID in the Access Point, access the Subscriber Modules web pages via the Proxy address (e.g., `http://ipaddress:1080/status.html`), and attaches them to the Zip File.
18. When finished, it displays a Message Box indicating that it has completed generating the Report File.

## ***Extracting and Viewing the Contents of a Report File***

The report file is just a simple zip file.

19. Extract it to a folder in your file system.
20. For a formatted view of the report, open the file (`index.html`) in a Web Browser. A frames page with three frames will be displayed.
  - The top left frame indicates the items that are contained in the report. This includes the attached configuration/log files as well as the list of elements that were selected.
  - When an element is selected, the bottom left frame contains a list of web pages that can be viewed for the element.
  - The right frame (the main one) provides a view of the file that is selected by the left frames.

The attached Network Archive File (`*.net`) can be opened using the Network Updater Tool.

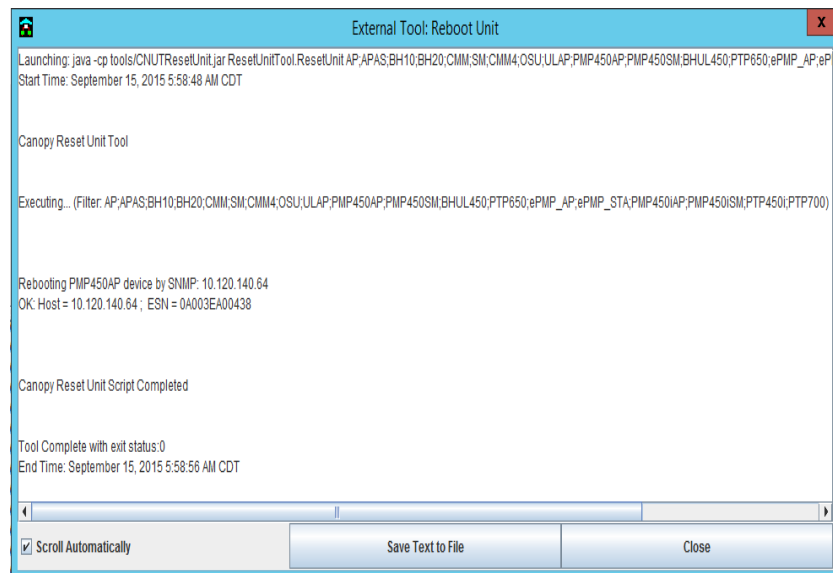
## **4.5.4 Reboot Unit**

This tool is used to cause selected radios to reboot as soon as you select **Tools★Reboot Unit**, so you should ensure that the devices selected are only those intended for a reboot before you make this option selection.

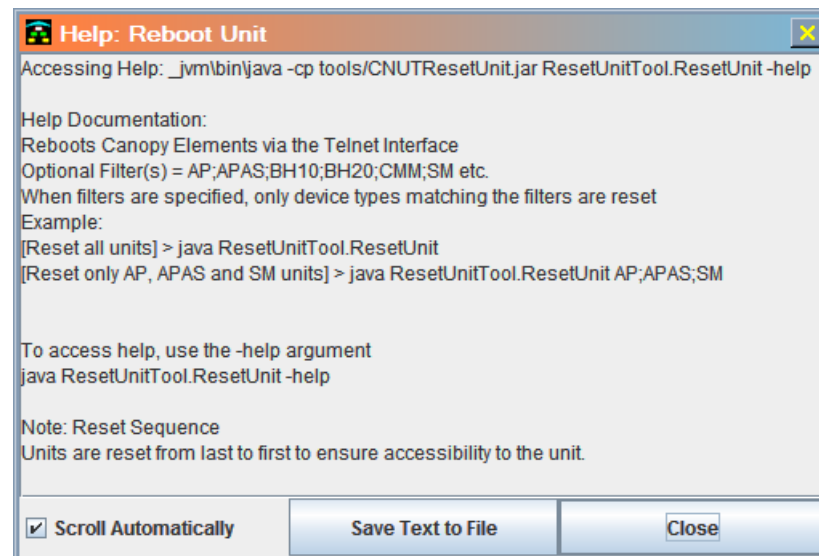
## Network Updater On-Line Help

### Issue 1

August 2021



Help for this tool is available at **Help★Tools★Reboot Unit**.



However, if this Help: Reboot Unit window continues to state that the telnet interface is used, be aware that, for any element that has a valid IP address in Network Updater, this application uses SNMP, not telnet, to force the reboot.

August 2021

## 4.5.5 Set Access Point Authentication Mode

This tool allows you to quickly and easily change the authentication parameters of access points managed by BAM server or RADIUS server, using the Network Updater tool rather than having to access each APs web interface. This tool eases migration by providing the capability to temporarily disable authentication during the upgrade so that your customers are not affected. This tool also allows you to easily resume authentication required when the upgrade is complete. In addition, it allows you to configure the authentication server IP addresses into each of your access points.

To use the tool, identify the APs to manage by checking them on the tree view display and then launch **Tools★Set Access Point Authentication Mode**.

**AP Authentication Mode**

Authentication Mode: **Authentication Disabled**

Authentication Servers

Authentication Server	IP Address	Authentication Mode
Authentication Server 1:	0.0.0.0	BAM Server
Authentication Server 2:	0.0.0.0	AP Pre-Shared Key
Authentication Server 3:	0.0.0.0	Radius AAA Server
Authentication Server 4:	0.0.0.0	(BAM Only)
Authentication Server 5:	0.0.0.0	(BAM Only)

Authentication Key

☒ Use Default Key

☐ Set User Key (32 0xFF's Key)

Secret:

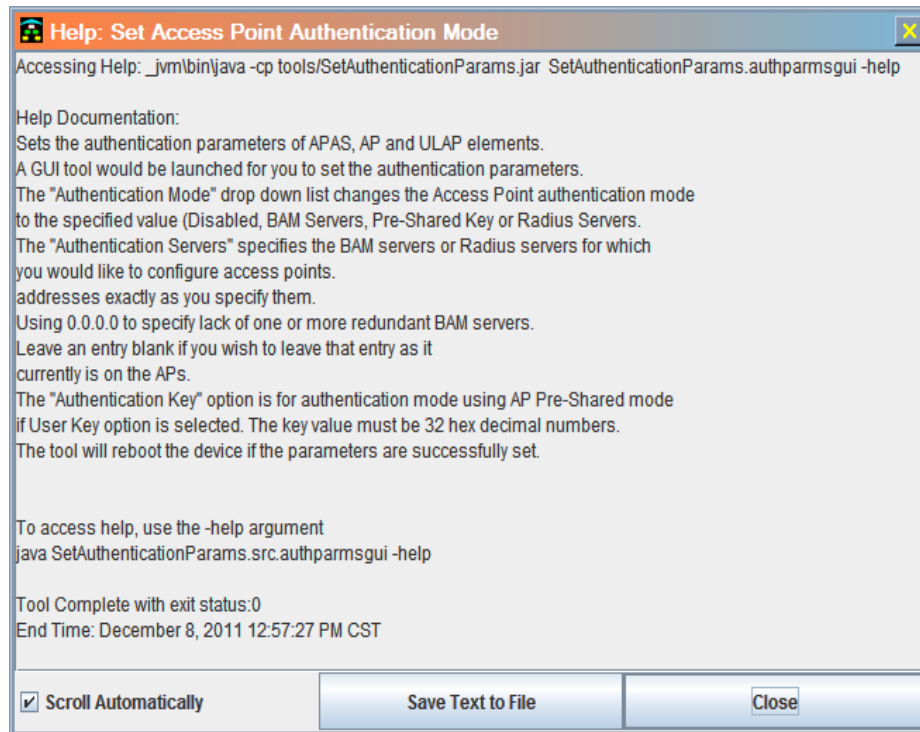
Secret:

Shared Secret:

OK Cancel

August 2021

The **Help★Tools★Set Access Point Authentication Mode** option displays the following overview of this Network Updater utility:



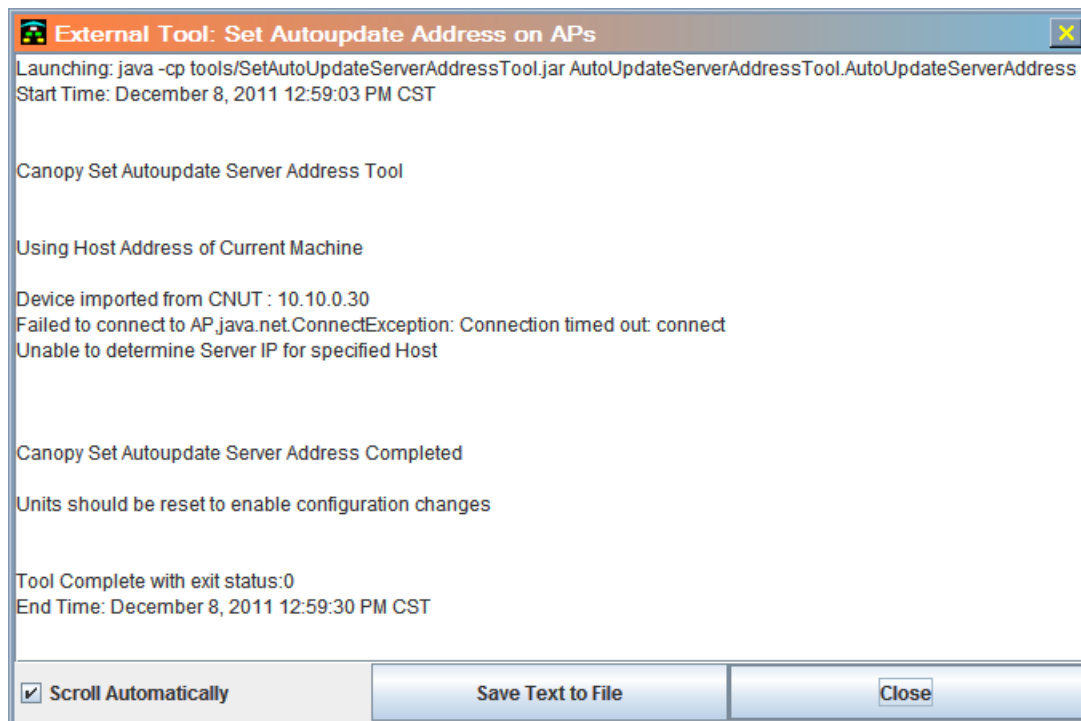
The IP address section of the dialog box will allow you to leave an entry blank. When this is done, you are indicating that for each AP, you wish to leave the currently configured value as is for that IP entry.

A reboot operation to make the configured values effective is automatic.

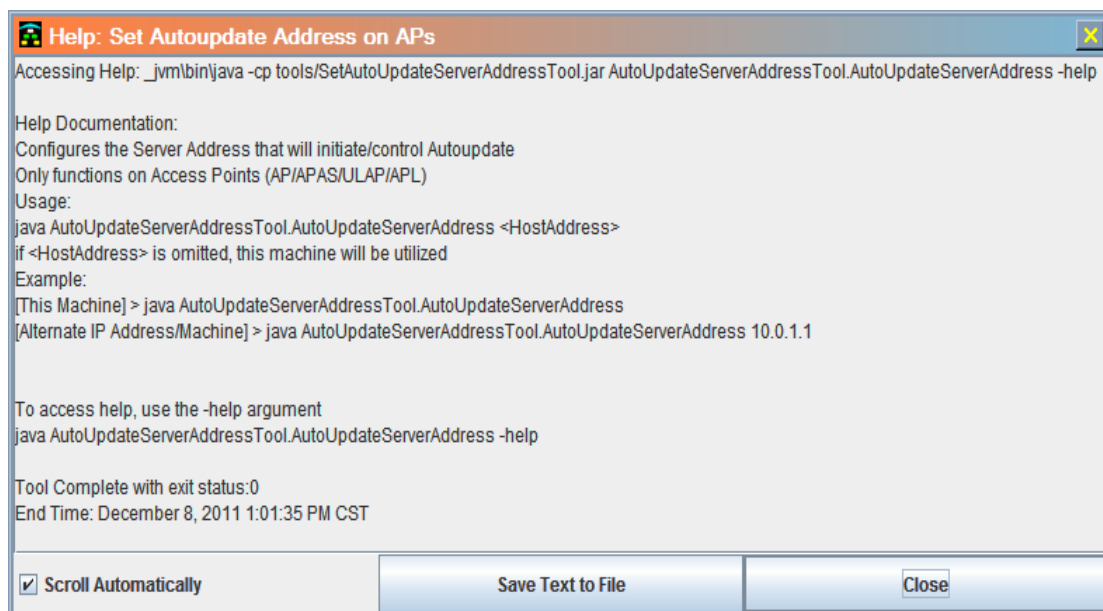
## 4.5.6 Set Autoupdate Address on APs

This external tool is used to set the valid address from which APs will accept Autoupdate commands. This tool is not supported for use on PMP 320 APs. To use the tool, identify the APs to manage by checking them on the tree view display and then launch **Tools★Set Autoupdate Address on APs**.

August 2021



The **Help★Tools★Set Autoupdate Address on APs** option displays the following overview of this Network Updater utility:

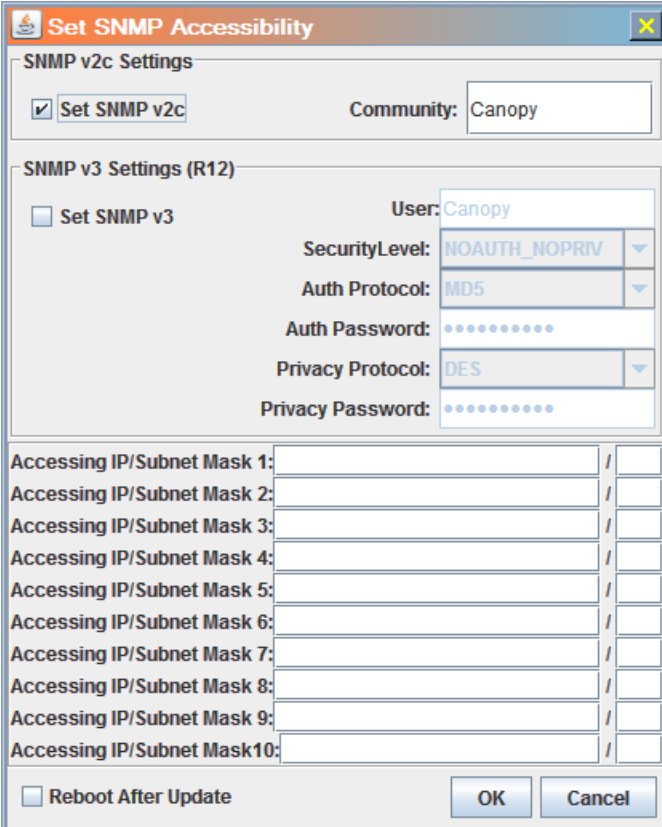


**note** ..... If you use the Update commands on the network, this address will automatically be set without the need for this external tool. See [SM Autoupdate Feature](#) for more information on this subject.

August 2021

## 4.5.7 Set SNMP Accessibility

This external tool is used to set the valid network mask for indicating from which machines the modules will accept SNMP requests.



The dialog box titled "Set SNMP Accessibility" contains the following elements:

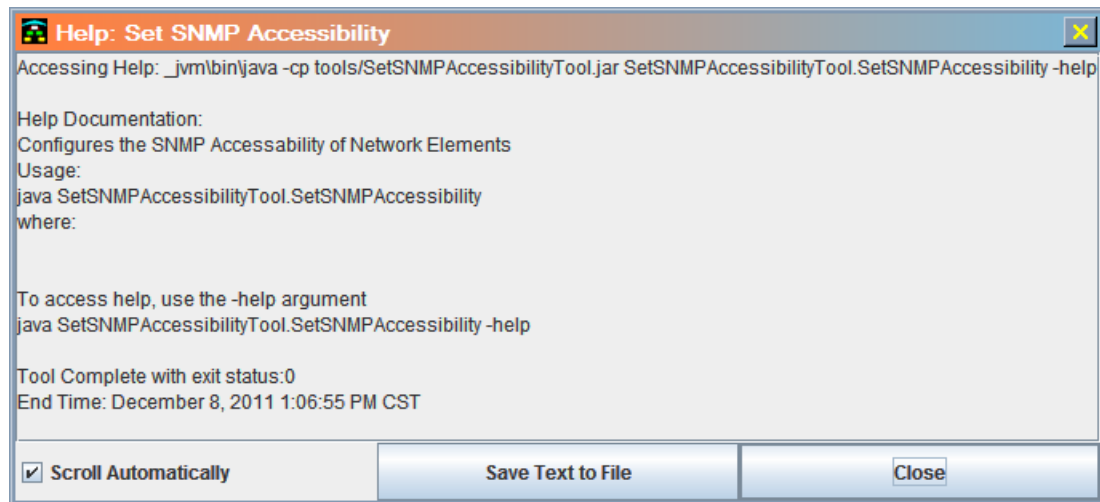
- SNMP v2c Settings:**
  - ☒ Set SNMP v2c
  - Community: Canopy
- SNMP v3 Settings (R12):**
  - ☐ Set SNMP v3
  - User: Canopy
  - SecurityLevel: NOAUTH\_NOPRIV
  - Auth Protocol: MD5
  - Auth Password: .....
  - Privacy Protocol: DES
  - Privacy Password: .....
- Accessing IP/Subnet Mask:** A list of 10 rows, each with a text input field and a checkbox.

Accessing IP/Subnet Mask 1:	
	<input type="checkbox"/>
Accessing IP/Subnet Mask 2:	<input type="checkbox"/>
Accessing IP/Subnet Mask 3:	<input type="checkbox"/>
Accessing IP/Subnet Mask 4:	<input type="checkbox"/>
Accessing IP/Subnet Mask 5:	<input type="checkbox"/>
Accessing IP/Subnet Mask 6:	<input type="checkbox"/>
Accessing IP/Subnet Mask 7:	<input type="checkbox"/>
Accessing IP/Subnet Mask 8:	<input type="checkbox"/>
Accessing IP/Subnet Mask 9:	<input type="checkbox"/>
Accessing IP/Subnet Mask 10:	<input type="checkbox"/>
- ☐ Reboot After Update
- OK and Cancel buttons.

The **Help★Tools★Set SNMP Accessibility** option displays the following overview of this Network Updater utility:



August 2021

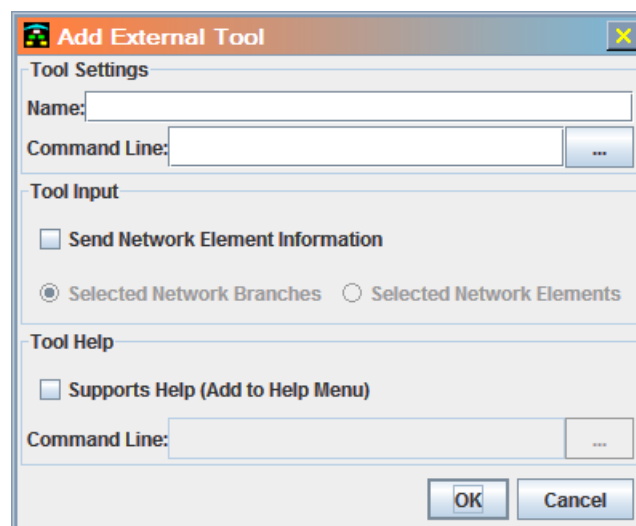


This tool may be required if the current SNMP mask value on the modules is too restrictive in that it will not allow the Network Updater server to communicate with the modules through SNMP.

## 4.5.8 Set SM/CPE Security

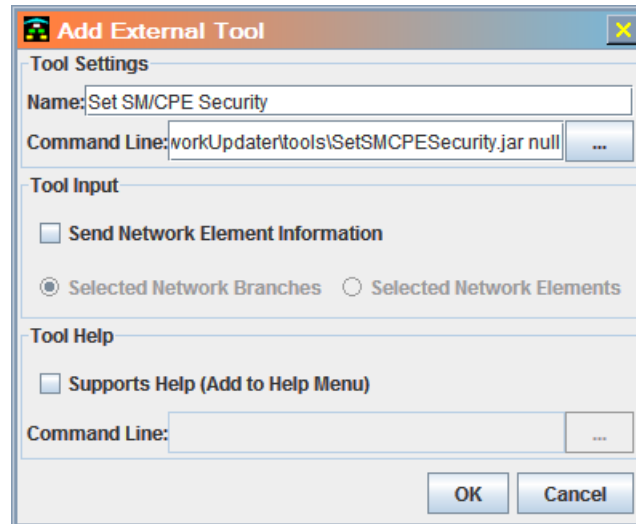
The installation tool for Network Updater deposits all the pre-scripted tools into the folder `C:\Cambium\NetworkUpdater\tools` or its Linux counterpart path. This set of tools includes not only those that the application user can invoke from the main menu by selecting **Tools★ToolName**, but also the Set SM/CPE Security tool for configuring RADIUS authentication options in PMP SMs and PMP 320 CPE devices.

To put access to this tool into the application menu, select **Tools★Add external Tool to Menu**. In the resulting Add External Tool dialog, click the browse button (labeled with an ellipsis).



August 2021

Browse to the path stated above and select the file **SetSMCPESecurity.jar**. In the **Name** field above Command Line where the new tool is shown as the argument to a java command, type in a name by which you will distinguish this tool when you wish to execute it; **Set SM/CPE Security**, for example.



August 2021

Adjust the other settings in this dialog, then click **OK**. From this point forward, whenever you select **Tools★Set SM/CPE Security**, the interface specific to this utility will open. The interface for this utility consists of two tabs:

- one for target PMP SMs...

The screenshot shows the 'Set SM/CPE Security' dialog box with the 'Set SM Security' tab selected. The dialog has two tabs: 'Set SM Security' and 'Set CPE Security'. The 'Set SM Security' tab contains the following settings:

- ☒ Lock AAA: ☒ Disable ☐ Enable
- ☒ Phase 1: EAPTTLS (dropdown)
- ☒ Phase 2: PAP (dropdown)
- ☒ Use Realm: ☒ Disable ☐ Enable
- ☐ Realm: (text field)
- ☐ EAP User Name: (text field)
- ☐ EAP Password: (text field)
- ☐ Identity: (text field)

Below these settings is a section titled 'Manual SNMP Community and IP Address Scan' with the following options:

- ☒ Enable
- Current Community String: (text field)
- IP Adresse(s)/IP Address Range: (text area)

The text area for 'IP Adresse(s)/IP Address Range' contains the following text:

```
<Sample ip address>  
<169.254.1.1>  
<etc.>  
<sample ip range>  
169.254.1.1-169.254.1.100  
<etc.>
```

To the right of the text area is a 'Description' box with the following text:

Enter one/more host name(s)/IP addresse(s) or one/more IP address range(s). Enter ONE LINE per IP/IP range.

Note\*: The type of devices with the IP/IP range will be assumed matching the current selected tab.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

August 2021

- the other for target PMP 320 CPE devices...

**Set SM/CPE Security**

**Set SM Security** | **Set CPE Security**

☒ Phase 1

☒ Phase 2

☒ Use Realm

☐ Realm

☐ EAP User Name

☐ EAP Password

☒ Identity Type

☐ Identity

☒ Use Device Certificate

☐ Validate Date Certificate

☐ Validate Server Certificate

EAP-TTLS

PAP

☒ Disable ☐ Enable

Manual Identity

☒ Disable ☐ Enable

☒ Disable ☐ Enable

☒ Disable ☐ Enable

**Manual SNMP Community and IP Address Scan**

☒ Enable

Current Community String:

IP Adresse(s)/IP Address Range:

<Sample ip address>  
<169.254.1.1>  
<etc.>  
<sample ip range>  
169.254.1.1-169.254.1.100  
<etc.>

**Description**

Enter one/more host name(s)/IP  
addresse(s) or one/more IP address  
range(s). Enter ONE LINE per IP/IP  
range.

Note\*: The type of devices with the  
IP/IP range will be assumed matching  
the current selected tab.

OK Cancel

For information about AAA authentication, the two certificate positions, and the effect of applying certificates, see the user guide and release notes that support the target device(s). See also

- [Error! Reference source not found.](#)
- [Update→Upload Certificate to Selected Branches.](#)

## 4.5.9 Bandwidth Updater

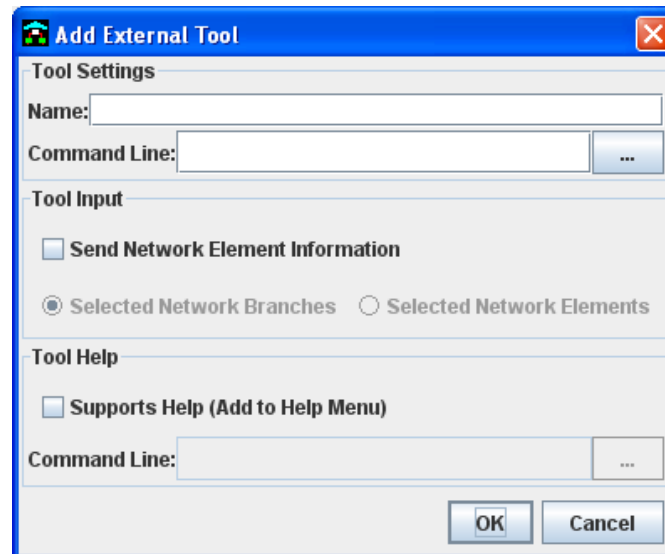
The installation tool for Network Updater deposits all of the pre-scripted tools into the folder C:\Cambium\NetworkUpdater\tools or its Linux counterpart path. This set includes the Bandwidth Updater tool.

This tool provides an advantage over the use of the HPAP Channel Bandwidth tab, in that this tool configures the bandwidth of the target elements without pushing a new firmware image package to them. For comparison, see [HPAP Channel Bandwidth Tab](#).

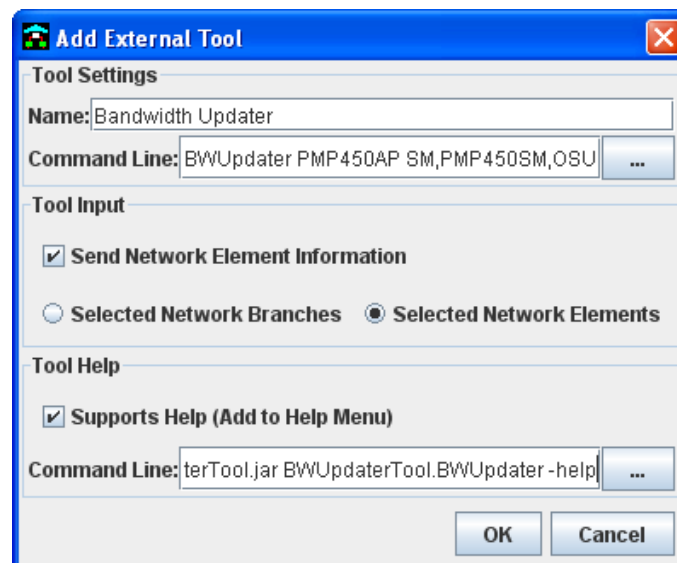
August 2021

## Adding the Bandwidth Updater Tool

To put access to this tool into the application menu, select **Tools\*Add external Tool to Menu**. In the resulting Add External Tool dialog, click the browse button (labeled with an ellipsis).



Browse to `C:\Cambium\NetworkUpdater\tools` or its Linux counterpart path and select the file `BWUpdaterTool.jar`. In the **Name** field, type a name for the tool to distinguish it; for example, **Bandwidth Updater**.



**important** ..... In its command line argument, this tool accepts only the *short name* of supported device types.

August 2021

## Command Line

```
Java -cp NetworkUpdater_path/tools/BWUpdaterTool.jar BWUpdaterTool.BWUpdater
Supported_AP Supported_SM,Supported_SM,Supported_SM
```

## Example

To set this command line to configure PMP 450 AP, PMP 450 SM, and PMP 430 SM bandwidth, edit it to the following syntax:

```
java -cp tools/BWUpdaterTool.jar BWUpdaterTool.BWUpdater
PMP450AP,APL,PMP450iAP,PMP450m,PMP450bAP SM,PMP450SM,OSU,PMP450iSM,PMP450bSM
BHUL450,PTP450i,PTP450b
```

**note** ..... In this example, the short name SM is added to the comma-separated SM list to have the tool configure the bandwidth of auto-discovered PMP 450 SMs and PMP 430 SMs, which are known to Network Updater as only SMs (in contrast to manually discovered SMs, which are known by their device types).

The short names of supported device types are as follows.

Supported Device Type	Short Name
PMP 450 Access Point (AP)	PMP450AP
PMP 450 Subscriber Module (SM)	PMP450SM
PMP 430 Subscriber Module (SM)	OSU
PMP 100 Access Point CAP 110 (APL)	APL
PMP 450i Access Point (AP)	PMP450iAP
PMP 450i Subscriber Module (SM)	PMP450iSM
PMP 450m Access Point (AP)	PMP450m
PMP 450b Access Point (AP)	PMP450bAP
PMP 450b Subscriber Module (SM)	PMP450bSM
PMP 100 Subscriber Module (SM)	SM
PTP 450	BHUL450
PTP 450i	PTP450i
PTP 450b	PTP450b

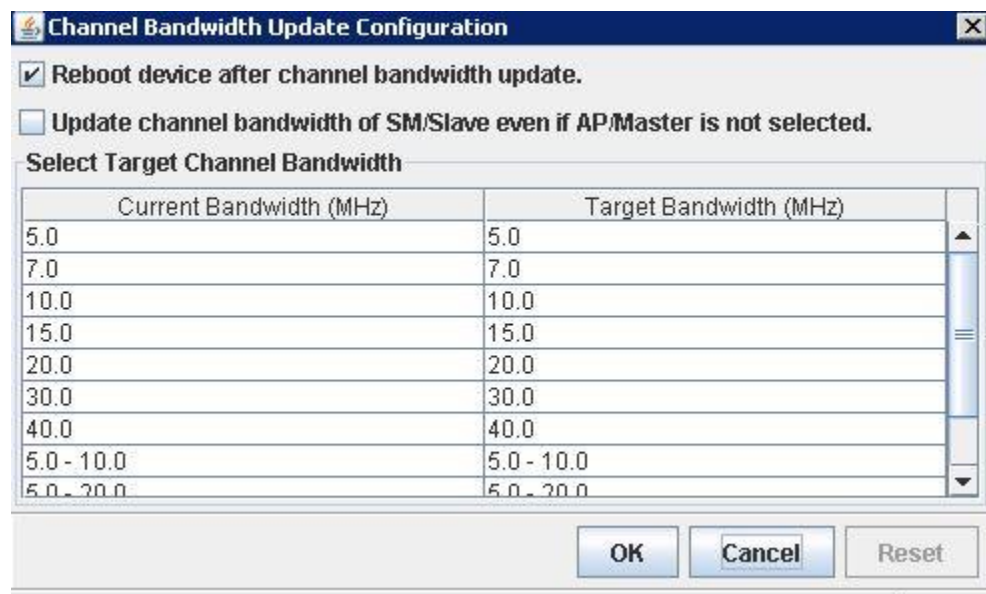
Although this tool, as is, has the capability to configure the bandwidth of any device that supports bandwidth configuration, the following devices do not.

August 2021

Unsupported Device Type	Short Name
PMP 430 Access Point (AP) <sup>1</sup>	ULAP
PMP 100 Access Point (AP)	AP
PMP 100 Access Point Authentication Server (APAS)	APAS
<b>IMPORTANT:</b>	
6. Do not attempt to execute this tool on PMP 430 APs.	

## 4.5.10 Using the Bandwidth Updater Tool

The interface of the Bandwidth Updater tool is configurable as follows.



This section uses an example case to configure an entire sector of PMP 450 elements and PMP 430 SMs in Release 12.0 to operate at 10.0 MHz of bandwidth. This case assumes that

- the PMP 450 AP is already operating at 10.0 MHz.
- its connected PMP 450 SMs are operating at 5.0 to 10.0 MHz.
- its connected PMP 430 SMs are operating at 10.0 to 20.0 MHz.

To set the entire sector to 10.0 MHz, perform the following steps.

21. Plan the execution to occur at a date and time when historical data suggests that the all of the target SMs are connected and operating.

August 2021

22. Identify the current bandwidth of all devices in sector (in the example case, the 10-MHz, 5-10 MHz and 10-20 MHz devices).
23. In the Network Updater interface, select the AP and all its SMs.
24. From the main menu, select **Tools**★**Bandwidth Updater**.
25. In the Launch External Tool dialog, select the radio button for **Selected Network Elements**.
26. Click **OK**.
27. In the **Select Target Channel Bandwidth** block of the Channel Bandwidth Update Configuration dialog, click to highlight
  - **5.0 – 10.0**, **10.0**, and **10.0 – 20.0** in the Current Bandwidth (MHz) column.
  - **10.0** in the Target Bandwidth (MHz) column.
28. Ensure that the selections in Current Bandwidth comprise those identified in Step 2. Click **OK**.

**RESULT:** The channel bandwidth of all the devices (the PMP 450 AP and its connected PMP 450 SMs and PMP 430 SMs are all updated to operate at 10 MHz

## 5 Network Updater Operations

### 5.1 Quick Start Examples

This section provides examples of how the Network Updater Tool may be used to solve specific problems or use cases for a user. In addressing these scenarios not all the Network Updater Tool capabilities and components may be used or needed. Refer to [Detailed Procedural Operations](#) for more coverage on all the aspects of using the Network Updater Tool presented in a more robust example/walk-thru.

#### 5.1.1 Upgrading a Single Radio before Deployment

In some instances, it may be necessary to upgrade the software or FPGA on a new radio prior to deploying it in your network. The Network Updater tool can be used to perform this operation quickly and efficiently. The following steps could be used to perform an upgrade of a new radio that is in its default factory configuration:

#### Assumptions

- Network Updater is installed and operational on your computer.



August 2021

- The radio is connected to the same LAN as the Network Updater Computer. The simplest way to do this is to directly plug the Ethernet output of the radio power adaptor into the Network Updater computer Ethernet port.
- **important** If a switch or hub is used to connect the radio and Network Updater computer, then only one radio should be on the LAN at a time, since in default mode they all have the same IP address.
- The Network Updater computer has an IP address that can directly access the default IP on the radio, which is 169.254.1.1 this can be done in the case of a Windows computer by adding simply an additional IP address to the computer network interface with an IP address of 169.254.1.2 and a subnet mask of 255.255.255.0.
- The Installation Package needed to upgrade the radio has been downloaded from the website and added to the Network Updater through the **Manage Packages** operation (see [Update→Manage Packages](#)).

## Steps to Perform a Single Radio Local Upgrade

29. Start Network Updater.
30. If you don't start up with a blank new network file, then open a new network file with the **New Network Archive** operation (see [File→New Network Archive](#)).
31. Enter a new network element to the empty network tree using the **Add Elements to Network Root** operation (see [Edit→Add Elements to Network Root](#)).
32. On the Add Elements dialogue, select a type of **Subscriber Module** and enter the IP address of 169.254.1.1 within the Element Host Names area of the dialogue.
33. Make sure the proper Installation Package is active with the Package Manager dialogue (see [Update→Manage Packages](#)).
34. To verify connectivity with the radio, perform a **Refresh/Discover Entire Network** operation (see [View→Refresh/Discover Entire Network](#)). You should see the details columns for the new element filled in with ESN and software version information.
35. Initiate the upgrade of radio using the **Update Entire Network Root** operation (see [Update→Update Entire Network Root](#)). When this operation finishes, the radio is done being upgraded.

### 5.1.2 Upgrading a Single AP and its Associated SMs

The following steps can be used to update a single AP and all of its SMs in a rapid fashion, except in PMP 320 sectors. This can be useful if a single sector is being updated for testing purposes. Also, these operations are a logical building block for performing larger updates across your entire network.

August 2021

## Assumptions

- Network Updater is installed and operational on your computer.
- The AP has a routable IP address that the Network Updater computer can communicate.
- All the SMs associated with the AP are powered up and currently registered to the AP.
- The Installation Package needed to upgrade the radio has been downloaded from the website and added to the Network Updater through the **Manage Packages** operation (see [Update→Manage Packages](#)).

## Steps to Perform a Single AP Sector Upgrade

36. Start Network Updater.
37. If you don't start up with a blank new network file, then open a new network file with the New Network Archive operation (see [File→New Network Archive](#)).
38. Enter a new network element to the empty network tree using the Add Elements to Network Root operation (see [Edit→Add Elements to Network Root](#)).
39. On the Add Elements dialogue, select a type of Access Point and enter the IP address of the AP within the Element Host Names area of the dialogue.
40. Make sure the proper Installation Package is active with the Package Manager dialogue (see [Update→Manage Packages](#)).
41. To verify connectivity with the radio and to automatically gather the list of SMs attached to the AP, perform a Discover Entire Network operation (see [View→Refresh/Discover Entire Network](#)). You should see the details columns for the AP be filled in with ESN and software version information and you should see a list of SMs appear within the Subscriber Modules (Auto-Detected) branch of the tree.
42. Configure the system to use Autoupdate to upgrade the SMs associated with the AP automatically after the AP has been upgraded. This is done by opening the Update Configuration ([Update→Configure](#)) dialogue and checking the Enable SM Autoupdate when an Access Point is Updated option (see [Update→Configure](#)).
43. Initiate the upgrade of the AP and its SMs using the Update Entire Network Root operation (see [Update→Update Entire Network Root](#)). When the direct update of the AP is completed a dialogue will open indicating SM Autoupdate has been started.
44. Leave the SM Autoupdate started dialogue open and monitor the progress of the SMs being updated.
45. When all SMs show updated software and FPGA version, the AP sector upgrade is complete. You should now disable the SM Autoupdate mode on the AP by selecting the AP element and using the **Enable/Disable APs for SM Autoupdate** operation (see [Update→Enable/Disable APs for SM Autoupdate](#)).

August 2021

## 5.1.3 Minimum Actions to Perform Future Network Upgrades

Once the user has defined a network layout and performed an upgrade at least once on their network, subsequent network upgrades are practically one-touch operations. The following minimum steps could be used to initiate future network upgrades:

46. Download the new installation package from the website at <http://www.cambiumnetworks.com/support/pmp/software/index.php> for PMP devices and/or <http://www.cambiumnetworks.com/support/ptp/software/index.php> for PTP devices.
47. Open your current network archive within Network Updater.
48. Link the new Installation Package to Network Updater, using the **Manage Packages** operation (see [Update→Manage Packages](#)).
49. Ensure SM Autoupdate is enabled on the network, if you are using that option, by either having it automatically set within the Update Configuration window (see [Update→Configure](#)), or by using the **Enable/Disable APs for SM Autoupdate** operation (see [Update→Enable/Disable APs for SM Autoupdate](#)) after the next Update operation (next step) is complete.
50. Initiate the network upgrade by using the **Update Entire Network Root** operation (see [Update→Update Entire Network Root](#)).
51. Allow the update operation to complete, and check the status of the network with a **Discover Entire Network** operation (see [View→Refresh/Discover Entire Network](#)) as appropriate.

## 5.2 Detailed Procedural Operations

This section is meant to walk the user through the major operations involved in performing network upgrades using the Network Updater tool. The material here is presented in the logical order a user would need to perform each operation the first time they use Network Updater.

### 5.2.1 Creating a New Network Archive File

The Network Updater uses a local data file for keeping track of information entered by the user or automatically discovered about the network in question. This file is referred to as a Network Archive File. The user can create a new archive file at any time by using the **New Network Archive** operation (see [File→New Network Archive](#)). This operation will clear the current network (if any) from Network Updater and provide a clean slate to the user for entering new network information. The creation of a Network Archive file is not actually completed until the user does a **Save Network Archive** operation (see [File→Save Network Archive](#)), at which time they will be prompted for a path and filename to identify the actual archive file.

August 2021

If a network archive file already exists, then the user can just load it with the **Load Network Archive** operation (see [File→Load Network Archive](#)). Network updater will also remember the last loaded network archive file and automatically re-load it upon startup.

## 5.2.2 Adding Network Elements

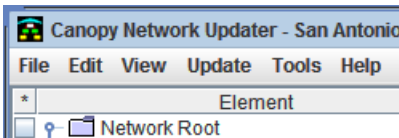
**important** ..... Because of how Network Updater processes passwords, HTML entity symbols (special characters such as, but not limited to ~, !, and @, °, ª, á, é, í, ó, and ú) as characters in configured passwords typically prevent the associated user from logging into Network Updater. Although a particular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

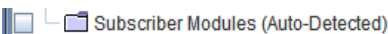
The first operation that a user must do for a new network is to enter information about APs, BHs, and CMMs for the network. All the various types of devices are referred to as Network Elements in this document and within the GUI of the Network Updater. The basic information that is required for each of these types of network elements added is an IP address. It is also important for the user to enter an appropriate hierarchy of devices (see [Network Layers and Orders of Updating Equipment](#)). This is needed to ensure that modules are updated in an appropriate order on the network to avoid causing modules to be stranded during an upgrade process do to their parent being upgraded concurrently.

Initially, the user sees two top-level branches in the Network Updater network tree window:

Network Root and Subscriber Modules (Auto-Detected):



...



All elements added by the user should be added below the Network Root branch. The user will not be allowed to enter elements directly to the Subscriber Modules (Auto-Detected) branch, as that is reserved for information that the Network Updater finds on the network itself.

August 2021

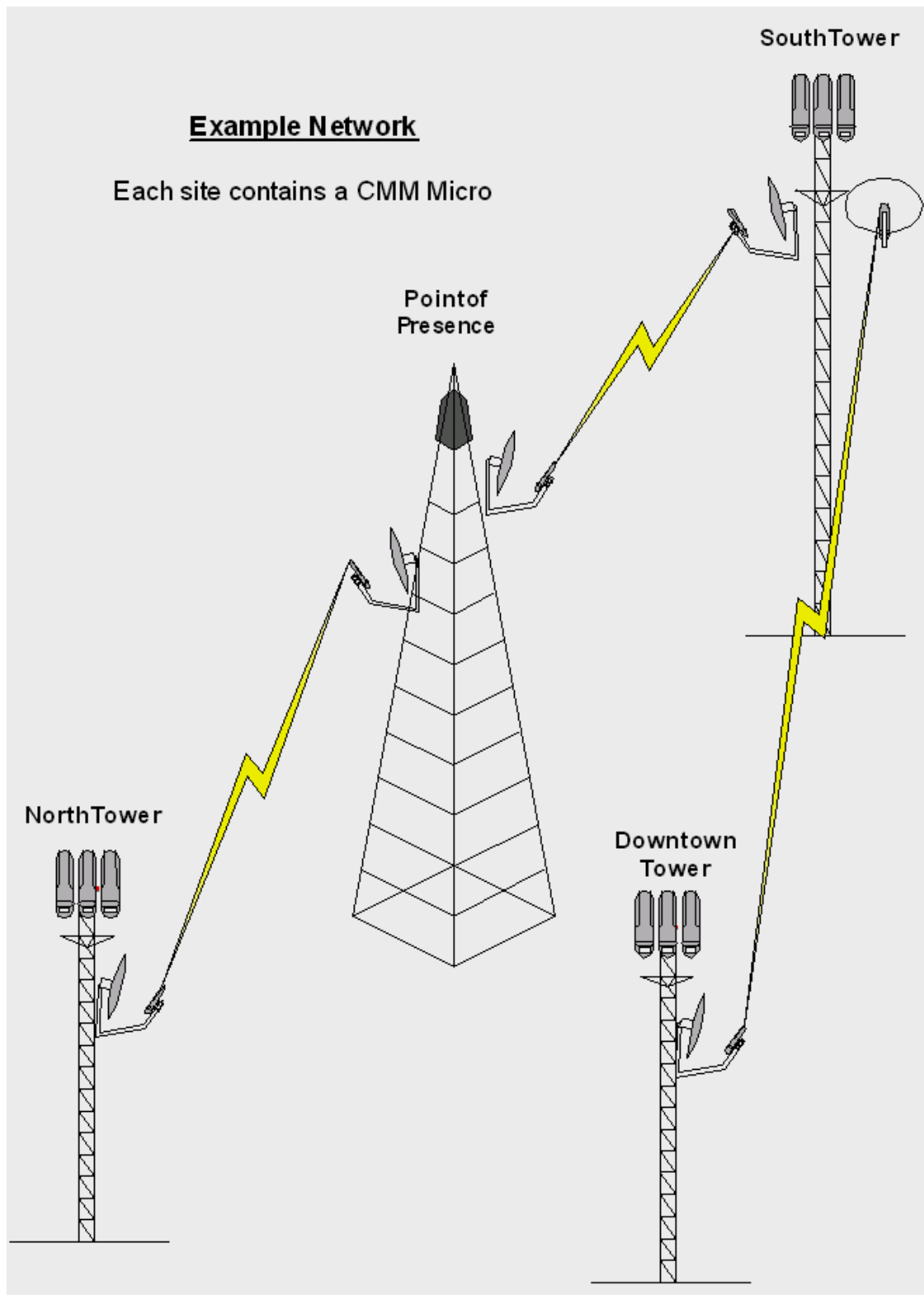
The user can initiate an add element in three ways:

- [Edit→Add Elements to Highlighted Element](#), which requires an element to be selected on the network tree window, such as the Network Root
- [Edit→Add Elements to Network Root](#)
- Select an element (such as Network Root) and right click to access the Add Network Element operation.

All three of these operations will perform the same operation, allowing the user to add a new network element. For grouping and management purposes, it may help to create element groups (folders) to contain different sets of elements within your network tree, such as creating an element group to contain all the APs and BHs related to single cluster. You can enter multiple elements at the same time by entering multiple host names, IP addresses, or IP address ranges in the Add Network Element window.

The following example is a network of three main clusters, each with 4 sectors, with backhaul connections to a single POP location. One of the clusters in the example (DowntownTower) is daisy chained to the POP through the backhaul of another cluster (South Tower). Each cluster location and the main POP have a CMM for synchronization purposes. For readability, the example is using host names that would be resolved by the `/etc/hosts` file on the local machine. It is also possible to enter the direct IP addresses in the Add Element window if host names weren't defined or the user didn't want to use them. The Network Updater tool will make use of a combination of SNMP and HTTP access to the elements to obtain additional information about the element related to its current configuration.

The following diagram is a representation of this example network:



The following Network Updater network tree represents this network in an appropriate hierarchical manner that ensures radios and CMMs will be updated in a non-conflicting manner:

Element	Type	ESN	Software Ver.	HWIF...	Boot Ver.	Last Ac...	State	Progress	Auto Up...
Network Root									
10.120.143.21	NE						Disabled		
10.120.143.22	NE						Disabled		
10.120.143.31	NE						Disabled		
10.120.143.32	NE						Disabled		
10.120.143.33	NE						Disabled		
10.120.143.34	NE						Disabled		
10.120.143.41	NE						Disabled		
10.120.143.42	NE						Disabled		
10.120.143.45	NE						Disabled		
10.120.143.46	NE						Disabled		
10.120.143.64	NE						Disabled		
10.120.143.65	NE						Disabled		
10.120.143.74	NE						Disabled		
10.120.143.75	NE						Disabled		
10.120.143.84	NE						Disabled		
10.120.143.85	NE						Disabled		
10.120.143.95	NE						Disabled		
10.120.143.96	NE						Disabled		
10.120.143.100	NE						Disabled		
10.120.143.101	NE						Disabled		
10.120.143.50	NE						Disabled		
10.120.143.51	NE						Disabled		
Subscriber Modules (Aut)									

**note** ..... The use of the Element Groupings **South Tower**, **Downtown Tower**, and **North Tower** were purely a matter of choice. They could have been left out if the user desired, though they do provide an easy way to select all the radios associated with a particular CMM.

A toggle-type command option in the main menu enables horizontal scroll bar. The option

[View→Debug on](#)

If the Debug On option is selected, then Network Updater will show the debug logs.

[View→Horizontal Scroll Deep Tree](#) allows the user to see subfolders beyond the 55<sup>th</sup> record to any desired depth of elements.

## 5.2.3 Detecting SMs in Network

It is not necessary for a user to enter the SMs that exist within their network as long as they have entered all of the APs to which their SMs communicate. The user may optionally add SMs to their Network Root. This may be useful for situations where the network operator has remote AP configurations (an AP hard linked to a SM, where the SM is providing the backhaul to the AP). The

August 2021

user should be aware that if the same SM is auto-detected by Network Updater, it might also appear in the Subscriber Modules (Auto-Detected) section as well. There are no negative side effects of having the SM appear in both places.

Network Updater has the ability to communicate with the APs and detect all of the SMs that are connected to the APs. This information is used to auto populate the Subscriber Module (Auto-Detected) network branch.

Once your APs have been entered you can do an automatic discovery of all the SMs on your network, as well as current information on the other elements of the network that you just entered, by using the option [View→Refresh/Discover Entire Network](#). This operation will talk with each element in the network, detecting SMs and discovering current software, boot, and FPGA version information for each device. The user may watch the progress of the network discovery both through the Event Window at the bottom of the Network Updater window and in a progress bar that appears in the center of the screen.

If the user cancels this operation before it finishes then some SMs may not be auto-detected and some AP, BH, and CMM information may not be gathered.

**note** ..... Only information on currently registered SMs can be auto-detected. Therefore, it may be necessary to periodically re-run the refresh network operation to gather information on new SMs.

Once an SM has been auto-detected it will remain within the Network Updater tree until the user manually removes it, even if the SM is not registered to an AP the next time a refresh operation is done.

## 5.2.4 Viewing Current Versions

At this point a full picture of your network including entered and auto-detected elements is available in the Network Updater window. The user can view the version information for all software, boot, and FPGA versions to determine where, if anywhere, there are inconsistencies. They can also see MAC address information for each element in the network. The last accessed column provides information on the last time the displayed Network Updater information was refreshed for any particular network element.



The screenshot shows the 'Canopy Network Updater - (New Network\*)' application window. It features a menu bar (File, Edit, View, Update, Tools, Help) and a table of network elements. The table has columns for Element, Type, ESN, Software Ver., HW/FPGA Ver., Boot Ver., Last Access, State, Progress, and Auto Update. The elements are listed in a tree view on the left, with checkboxes for selection. The table shows various elements like NE, HSBH, PTP, and BHUL, each with its own set of details and a progress bar indicating the state of the update process.

Element	Type	ESN	Software Ver.	HW/FPGA Ver.	Boot Ver.	Last Access	State	Progress	Auto Update
Network Root									
10.120.143.33	NE					09/15/15 08:41:25	Not responding	100%	Disabled
10.120.143.34	NE					09/15/15 08:41:43	Not responding	100%	Disabled
10.120.143.41	NE					09/15/15 08:42:02	Not responding	100%	Disabled
10.120.143.65	NE					09/15/15 08:45:05	No SNMP response	100%	Disabled
10.120.143.74	NE					09/15/15 08:42:28	Not responding	100%	Disabled
10.120.143.75	NE					09/15/15 08:42:46	Not responding	100%	Disabled
10.120.143.84	NE					09/15/15 08:43:04	Not responding	100%	Disabled
10.120.143.85	NE					09/15/15 08:43:22	Not responding	100%	Disabled
10.120.143.21	HSBH 150/300	000456803942	25600-10-07	D05-R01-C-FPS		09/15/15 08:41:07	Refreshed	100%	
10.120.143.22	HSBH 150/300	0004568032A8	25600-10-07	D05-R01-C-FPS		09/15/15 08:41:07	Refreshed	100%	
10.120.143.31	HSBH 800	0004563013E4	800-06-01	06.06-FIPS		09/15/15 08:41:07	Refreshed	100%	
10.120.143.32	HSBH 800	00045630138C	800-06-03	06.06-FIPS		09/15/15 08:41:07	Refreshed	100%	
10.120.143.42	Generic					09/15/15 08:42:02	Refreshed	100%	
10.120.143.45	PTP650	000456500018	50650-01-98	BOP01.01-C		09/15/15 08:42:02	Refreshed	100%	
10.120.143.46	PTP650	000456500014	50650-01-98	BOP01.01-C		09/15/15 08:42:02	Refreshed	100%	
10.120.143.64	BH20 - DES	0A003E70001B	CANOPY 13.3 (Build 9)	BH20-D... 030210	CANOPYBOOT 1.0	09/15/15 08:42:02	Refreshed	100%	
10.120.143.95	BH20 - DES	0A003E519BF3	CANOPY 13.4 (Build 11)	BH20-... 111010	CANOPYBOOT 1.0	09/15/15 08:43:23	Refreshed	100%	
10.120.143.96	BH20 - DES	0A003E519930	CANOPY 13.4 (Build 11)	BH20-... 111010	CANOPYBOOT 1.0	09/15/15 08:43:24	Refreshed	100%	
10.120.143.100	BHUL450 - AES	0A003EA09472	CANOPY 13.4 BHUL450-AES	040715	CANOPYBOOT 1.0	09/15/15 08:43:24	Refreshed	100%	
10.120.143.101	BHUL450 - AES	0A003EA093C8	CANOPY 13.4 BHUL450-AES	040715	CANOPYBOOT 1.0	09/15/15 08:43:24	Refreshed	100%	
10.120.143.50	PTP700	00045658007D				09/15/15 08:44:38	Refreshed	100%	
10.120.143.51	PTP700	000456580077				09/15/15 08:44:39	Refreshed	100%	
Subscriber Modules (Auto-Detect)									

Network Updater will validate the element type value when it communicates with the element on the network. If the user entered the wrong type of element originally when they added the network element to the network tree, Network Updater will update the element type value to reflect the real element type as discovered in the network.

## 5.2.5 Current State Information on Network Elements

Network Updater captures current state information on each element as it interacts with the element. This information is showed in the **State** column. Many Network Updater operations can update this state field indicating successful operation or error conditions. This state can also be used to monitor the progress of a **Refresh** or **Update** operation on the network. State information will correlate to action information logged to the event window.

## 5.2.6 Identifying Installation Package for Performing Upgrades

The next logical operation the user needs to do is to identify the Installation Packages for Network Updater to use when updating the network. This is done through the **Manage Packages** operation

August 2021

(see [Update→Manage Packages](#)). Installation packages can be downloaded off the website, from the Network Updater download page.

**important** ..... Normal image package files for devices can also be downloaded from the website, but *do not work with Network Updater*, so be sure to download Network Updater installation packages for the software you need.

The user may have one or more packages active in the system at the same time. In the case of multiple packages, then the packages at the top of the Manage Package window will take precedence. Network Updater will search the packages from the top down until it finds package files for any element type it is required to update. Because of this fact, if a single package contains all the upgrades required for this network upgrade activity, then the user may want to be sure that only that single package is selected (by checking the box next to the package name).

To allow the SM Auto update process to finish as quickly as it can, load only those packages onto the AP that are appropriate for the SMs in the sector. For example, do not load any P7 through P9 packages onto an OFDM AP or a 5.4-GHz AP, since these packages are not supported by the SMs in the sector of these types of AP. Using separate package load and update operations for mixed networks, while it takes a little bit more operator time, takes considerably less update time overall.

## 5.2.7 Ensuring the Network is configured for Using SM Autoupdate

Network Updater will directly update all specified APs, BHs, and CMMs in your network. For sectors other than PMP 320 series, there are two ways to upgrade the SMs, either directly by selecting them and instructing Network Updater to perform an upgrade on them, or by using the SM Autoupdate feature. See [SM Autoupdate Feature](#) for more information on that mechanism for performing SM upgrades.

**note** ..... This feature is not available in PMP 320 sectors.

Configuring the SM Autoupdate Feature settings are done through the **Configure** operation (see [Update→Configure](#)). See that section for additional information on why you may want to use the SM Autoupdate feature in favor of direct SM updates through Network Updater. In general, your overall network upgrade will proceed much quicker by fully leveraging the power of the SM Autoupdate capabilities of the network.

The SM Autoupdate capability is controlled on an AP by AP basis by setting the SM Autoupdate option on the AP. The Network Updater can enable or disable SM Autoupdate on all or any portion of the APs in your network. This is done using the **Enable/Disable APs for SM Autoupdate** operation (see [Update→Enable/Disable APs for SM Autoupdate](#)). When this operation is chosen, a progress window will appear while the Network Updater is communicating with the appropriate APs.

**important** ..... SM Autoupdate is supported for SMs whose **Network Accessibility** parameter (in the IP tab of the SM's Configuration management web page) is set to **Local**, not **Public**. Even where Network Updater can discover SMs as children of their APs, if their **Network Accessibility** is set to **Public**, then Network Updater *must* discover them directly.

**note** ..... Canceling this operation before its completion may result in the desired SM Autoupdate configuration change not being set on all the specified APs.

## 5.2.8 Determining Where SMs Will Obtain Package Files

When using the SM Autoupdate capability, it is necessary to specify from where SMs should directly obtain package files. SM Autoupdate supports the capability to put the SM package files on the APs, a local TFTP server, or a CNUT HTTP server. Network Updater places the SM package files in the appropriate location for the SMs to obtain them. All you need to do is

- specify the file server type in the Update Configuration dialog (see [Update→Configure](#)).
- where a local TFTP server is specified and the Network Updater device has multiple network interface cards (more than one IP address), specify its IP address.
- where CNUT HTTP server is specified, specify its IP address.

## 5.2.9 Initiating or Discontinuing a Network Upgrade


After entering the core network element information, the operator

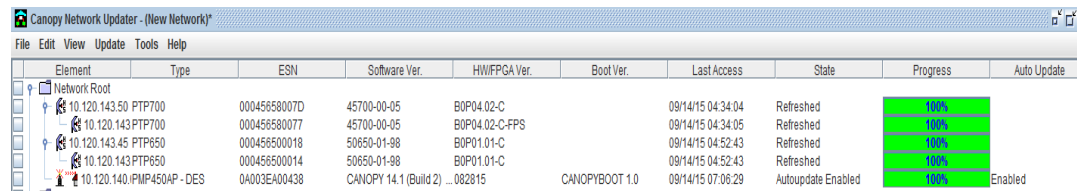
52. specifies installation packages with the image files.
53. decides whether to use the SM Autoupdate feature.
54. configures SM Autoupdate, if that feature is used.
55. initiates an upgrade on all or any part of their network, through one of the following operations:
  - [Update→Update Entire Network Root](#)
  - [Update→Update Selected Network Elements](#)
  - [Update→Update Selected Network Branches](#)

The upgrade operation walks the network according to the specified hierarchy and the version of the update operation selected, and then performs direct upgrades of all APs, BHs, CMMs, and any specifically selected SMs. At the end of each device upgrade, the device is remotely rebooted. Network Updater does not proceed to lower tiers of elements in the hierarchy until upper-tier devices have completed their upgrade cycle. Network Updater proceeds to other branches of the network while devices in another are being rebooted.

If the current configuration includes automatically enabling SM Autoupdate when the direct element upgrades are completed (see [Update→Configure](#)), and at least one network element that was updated was an AP, then Message window opens, stating `Auto Update process in progress`. This indirectly advises the user that the Network Updater portion of the upgrade is completed, and that Autoupdate of the SMs is occurring.

August 2021

If the SM Autoupdate option was not automatically set within the current configuration, the user can initiate the SM Autoupdate activities directly by using the **Enable/Disable APs for SM Autoupdate** operation (see [Update→Enable/Disable APs for SM Autoupdate](#)). This dialogue can be closed and other Network Updater activities can be performed while SM Autoupdate is enabled for the APs. The user can see progress of the overall system by examining the list of auto-discovered SMs, specifically their current version information and the status fields, to track progress on SM Autoupdate activity. The symbol  appears next to the device type icon to indicate the AP is actively in the SM Autoupdate mode. The following screen shows how this symbol is used, as well as how the **State** column of the APs indicates Autoupdate has been enabled, and the Auto Update column indicates Autoupdate is **Enabled**:



Element	Type	ESN	Software Ver.	HW/FPGA Ver.	Boot Ver.	Last Access	State	Progress	Auto Update
Network Root									
10.120.143.50 PTP700		00045658007D	45700-00-05	BOP04.02-C		09/14/15 04:34:04	Refreshed	100%	
10.120.143 PTP700		000456580077	45700-00-05	BOP04.02-C-FPS		09/14/15 04:34:05	Refreshed	100%	
10.120.143.45 PTP650		000456500018	50650-01-98	BOP01.01-C		09/14/15 04:52:43	Refreshed	100%	
10.120.143 PTP650		000456500014	50650-01-98	BOP01.01-C		09/14/15 04:52:43	Refreshed	100%	
10.120.140 PMP450AP-DES		0A003EA00438	CANOPY 14.1 (Build 2)	..082815	CANOPYBOOT 1.0	09/14/15 07:06:29	Autoupdate Enabled	100%	Enabled

Network Updater continues to update the status of the auto-discovered SMs in SM Autoupdate activities.

**important** ..... Closing the Network Updater application will not turn off SM Autoupdate on the APs in your network, but if your network contains a mixture of older and newer CPU formats, then closing the application ends Network Updater's ability to automatically switch the APs on your network between different image types. This can have the effect of preventing some SMs on the network from being upgraded, even though SM Autoupdate is still running on the APs.

SM Autoupdate continues to run on the AP until one of the following scenarios exists:

- SM Autoupdate is disabled on the AP within Network Updater.
- a reboot of the AP, If only one type of image is being used on the sector.
- shutting off Network Updater and rebooting the AP, if two types of images are being used on the sector.

Network Updater transitions the AP between the various software images upon the following conditions:

56. No Autoupdate activity has been detected for 20 minutes on the network.
57. Network Updater information regarding the AP in question indicates that there are still SMs of the alternate image type that require upgrading to the specified package.

**caution** ..... Ensure that the Network Updater computer can receive all the associated SM Autoupdate UPD packets communicated on your network so that image transitions do not occur prematurely.

August 2021

## 5.2.10 Scheduling an Upgrade for a Future Time

It may be desired to schedule an upgrade for a specific future time, such as off-peak usage time in the middle of the night. Network Updater provides this capability through the **Schedule Network Update** operation (see [Update→Schedule Network Update](#)).

## 5.2.11 Examining the Network for Straggler Elements to be upgraded

After the network upgrade process is completed, and the user has performed a **Refresh/Discover Entire Network** operation (see [View→Refresh/Discover Entire Network](#)), any previously identified or discovered network elements that were not successfully upgraded are obvious is a scan of the list of elements, in that Network Updater not show the new software, boot, and FPGA version for them. For these cases, the user must identify the reason(s). Possible reasons might be:

- The element was a part of a branch that was specifically omitted from the update activity (by the user not selecting the element/branch and choosing the operation [Update→Update Selected Network Elements](#) or [Update→Update Selected Network Branches](#), instead of the **Update→Update Entire Network Root** operation.
- The network element is not currently on the network (for example, an SM is powered down).
- No image files were found among the currently active packages to support that element type.
- There was a problem upgrading the element. Manually validate the health and operations of the element.

## 5.2.12 Disabling Autoupdate after all SMs have been upgraded

After all SMs on an AP or group of APs have been updated to the desired software and FPGA versions, it is recommended that SM Autoupdate be turned off for those APs. Disabling of SM Autoupdate is done through the operation [Update→Enable/Disable APs for SM Autoupdate](#). Performing this operation will help ensure that

- the AP does not inadvertently downgrade new SMs that may be added to the sector.
- unnecessary traffic is not generated, as
  - Network Updater constantly switches images on the AP in anticipation of new SMs upgrading.
  - every SM distinguishes during registration whether it should be upgraded.

Additionally, no reliable means exists to detect the enabled or disabled Autoupdate mode of an AP.

August 2021

## 5.2.13 Saving Status Information in the Network Archive File

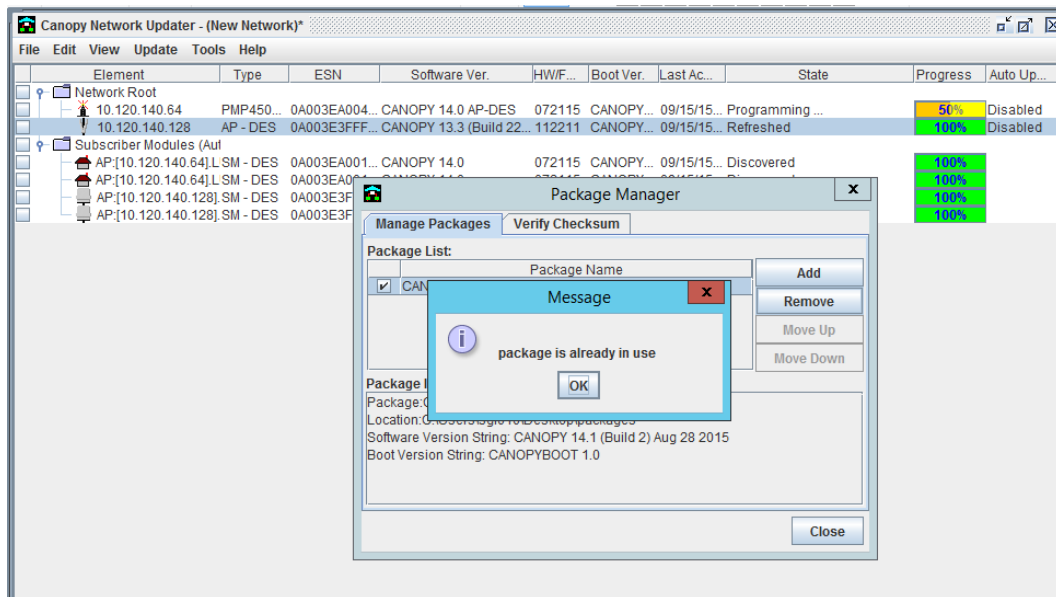
The user must initiate saves of the current network to the network archive file to ensure that the information entered, detected, and discovered on the network is maintained for the next session of Network Updater. The user can use the save operation [File→Save Network Archive](#) (or [File→Save Network Archive As](#), if this is a new file). Upon **Exit** (see [File→Exit](#)), or upon a request to load an alternate network archive file (using [File→Load Network Archive](#)), Network Updater prompts the user to save the current file first, if any changes have been made.

## 5.2.14 Refreshing the Status Information upon Start-Up

When the user starts Network Updater, the previously loaded network archive is automatically loaded as the current network. Since it is possible that the network could have changed since the user last entered Network Updater (for example, when new SMs joined network or further progress of an ongoing SM Autoupdate operation has occurred), the user may want the network archive data refreshed based on the current network. For this reason, Network Updater automatically asks the user whether to perform a **Refresh/Discover Entire Network** operation upon startup (see [View→Refresh/Discover Entire Network](#)).

This is for the convenience of the user, who can be cancel it if the user does not want a refresh, knows nothing has changed, or is not currently linked to the network, in which case the operation would fail.

## 5.2.15 Package cannot be removed while devices are in upgrade state



Warning message will be shown if user tries to remove package which is being used in current upgrade process. However, after upgrade, package can be removed.

## 5.2.16 Using Network Updater to Run Auxiliary Scripts against your Network

In upgrading and managing the network, performing element upgrades may be only one among other activities that the network operator wants or needs to perform. Network Updater has a built-in script running engine that allows user-defined scripts to be run against all or any part of their defined network. Scripts can be run once for the entire network, or once for any selected elements in the network. Network Updater passes a standard list of parameters to the script, giving the script all the information it may need to communicate with and manipulate network elements and their information.

It is anticipated that network operators will find many uses for scripts run within their Network Updater environment, including but not limited to configuration, manipulation of generic elements that may be associated with or attached to Cambium elements, and reporting element information.

Network Updater is distributed with a set of scripts to help the user perform operations that are anticipated to be common among operators. Given the standard interface for initiating scripts, and parameters passed along with them, operators may wish to share scripts among each other.

See [Tools→Add External Tool to Menu](#) for more information on creating and running your own scripts.

August 2021

## 5.2.17 Improved Update Tracking

Update progress monitor is improved in CNUT 4.9. Instead of popping of the update progress window and blocking all the key functions on CNUT UI, progress is embedded as a column on CNUT UI and other key operations are enabled for the devices which are not in progress. Various colors have been defined to show various states in device upgrade, like yellow in queued state, pink in transferring state, dark yellow in programming, reboot and verify state, green for operation success state and red for operation failure state.

## 5.2.18 Improved Auto-Update Tracking

This feature is introduced to improve the monitor of the auto-discovered SMs on CNUT reloaded. If the user started the update on some devices and closes CNUT in between the update process, then the user can monitor the update status of auto-discovered SMs, once he reloads the CNUT. But there are some limitations to this implementation. If the SMs are not discovered with public IP, sometimes the SMs might fail to update the software version string on CNUT UI, even after a successful update. In such case, the user should perform a manual refresh to update the software version string.

# 5.3 GUI Menu Operations

## 5.3.1 File Menu

New Network Archive
Load Network Archive
Save Network Archive
Save Network Archive As
C:\...\San Antonio -20090514.net
Exit

### File→New Network Archive

It clears the current network information from the active interface in preparation for the entering and discovery of a new set of network information. The user should save their work prior to starting a new network, as unsaved work will be lost.



August 2021

Changes to the active network are not saved until the operation [File→Save Network Archive](#) or [File→Save Network Archive As](#) is performed. Until the active network has been assigned a name, the **Save Network Archive** operation will not work, but will instead launch the **Save Network Archive As** operation.

## **File→Load Network Archive**

The user is prompted for the network archive file to be loaded as the active network. Network archive files will end with `.net` extensions. The user should save work before starting a new network, because unsaved work is lost when a new network starts. When a network archive is opened, the user has the choice of automatically initiating a **Refresh/Discover Entire Network** operation of the network to bring their information on the network up to date (see [View→Refresh/Discover Entire Network](#)). This is most useful if an active upgrade of the network was ongoing (through the SM Autoupdate feature) while Network Updater was not actively running (see [SM Autoupdate Feature](#)).

## **File→Save Network Archive**

The operation causes the currently active network information to be saved to the network archive file previously identified through either a **Load Network Archive** or **Save Network Archive As** operation (see [File→Load Network Archive](#) and [File→Save Network Archive As](#)). Until the active network has been assigned a name, the **Save Network Archive** operations will not work, but will instead trigger the **Save Network Archive As** operation. Network archive files should end with `.net` extensions.

## **File→Save Network Archive As**

This operation prompts the user for a filename and location to create a new network archive file with the network information from the currently active network. Network archive files should end with `.net` extensions. If the user does not supply an extension on their network archive filename, then `.net` will automatically be appended. Once the **Save Network Archive As** operation has been performed, the user may use the **Save Network Archive** operation to update the network archive file in the future without re-specifying the network archive file name (see [File→Save Network Archive](#)).

## **File→ *any of five most recent files***

This operation presents a list of the five most recently used network archive files for quick loading without browsing.

August 2021

## File→Exit

This operation causes the Network Updater tool to terminate. If the active network has had changes performed to it since last being saved, the user will be prompted to save their changes prior to the **Exit** operation being performed. If the user chooses not to save their changes and exits anyway, all changes to the active network will be lost. The user may also **Cancel** the **Exit** operation, in which case they will be returned to normal Network Updater operations.

## 5.3.2 Edit Menu

Preferences
Show/Hide Extended Element Information
Manage Subscriber Module Password List
Add Elements to Highlighted Element
Add Elements to Network Root
Remove Selected Elements
Modify Selected Network Element Access
Change Selected Network Elements Type
Move Selected Network Elements
Open Highlighted Network Element Web Page
Undo Network Changes
Find
Cancel Current Task

## Edit→Preferences

The following screen is used to capture user preferences for use by Network Updater. These preferences are maintained through multiple sessions of Network Updater.

August 2021

**Preferences/Default Settings**

**History Log File Settings**

Max History Log File Size (M): 10

**SM Auto-Discovery Settings**

☐ Gather SM Passwords and Extract IP Address and SNMP Settings

**Default Network Settings**

Default Network Settings are used for communicating with all Network Elements unless otherwise specified in the individual Element Configurations.

**User Account**

Device Login ID: root

Device Password:

Retype Password:

**HTTP Settings**

HTTP ☒ Port: 80

HTTPS ☐ Port: 443

☒ Try another protocol if Selected fails.

**SNMP Settings**

SNMP Community: Canopy

SNMP Version: v2c

SecurityLevel: NOAUTH\_NOPRIV

Auth Protocol: MD5

Auth Password: .....

Privacy Protocol: DES

Privacy Password: .....

Context Name:

SNMP Port: 161

**Auto Update Server Address**

Leave it empty for Auto detection:

Ok Cancel

The **Max History Log File Size** setting for the history log is used to control how large Network Updater will allow the Event Log file to grow. When the current Event Log file, `nwupdater.log` located in the `logs` directory below the Network Updater directory, reaches the specified maximum size, it is archived into the same directory and a fresh Network Updater log file is created. Archived log files have their filenames appended with the date and time of the last entry in the file.

The **Gather SM Passwords and Extract IP Address and SNMP Settings** option is used to specify whether the Network Updater should automatically attempt to discover SM IP addresses and SNMP community string information for SNMP v1 and v2c SMs. If this is enabled, then whenever a new SM is auto-discovered, Network Updater attempts to extract its IP address and community string from its web configuration pages. To complete this activity and to support direct software updates to the SMs after the IP address is determined, Network Updater needs the write-access password for each SM.

**note** ..... This write-access password should be the **Full Access** password for releases prior to 8.0, and should be the *password/login ID* for the account with admin privileges for Releases 8.0 and later.

August 2021

The **Default Network Settings** are used to specify password and SNMP community string values that apply to all or a large part of the network. These values are the default values that Network Updater will attempt to use to obtain information and interact with elements. In **User Account**, set the **Device Login ID** to the admin-level account. If these values are not correct for a specific element, then Network Updater may prompt the user for element-specific values (where the **Device Password** is incorrect) or show incomplete information for an element, such as only site location and site contact (where the **SNMP Community** is incorrect). Having the correct **SNMP Community** specified may also improve the performance of Network Updater during the initial discovery activity for infrastructure elements (elements added to Network Updater by specifying an IP address).

**note** ..... This password should be the **Full Access** password for releases prior to 8.0, and should be the password for the *specified login ID* for Releases 8.0 and later.

The fields of the Default Network Settings block are context sensitive as follows:

Field	Settable in SNMP Version	Not Settable in SNMP Version
Security Level	v3	v1, v2c
Auth Protocol	v3 <sup>1</sup>	
Auth Password	v3 <sup>1</sup>	
Privacy Protocol	v3 <sup>2</sup>	
Privacy Password	v3 <sup>2</sup>	
<b>NOTES:</b>  7. Only if Security Level is set to either AUTH_NOPRIV or AUTH_PRIV.  8. Only if Security Level is set to AUTH_PRIV.		

For **SNMP Version**, select the version number from the drop-down list. If you select v3, select a **Security Level** from the drop-down list. This list provides the alternatives for checksum algorithm (authentication) and encryption (privacy):

- **NOAUTH\_NOPRIV** for no authentication and no privacy
- **AUTH\_NOPRIV** for authentication without privacy
- **AUTH\_PRIV** for authentication and privacy

If **Security Level** is set to either **AUTH\_NOPRIV** or **AUTH\_PRIV**, then

- for **Auth Protocol**, select either **MD5** or **SHA**.
- for **Auth Password**, type a string that operators who use this SNMP account will need to remember.

If **Security Level** is set to **AUTH\_PRIV**, then

- for **Privacy Protocol**, select either **DES** or **AES**.
- for **Privacy Password**, type a string that operators who use this SNMP account will need to remember.

August 2021

Network Updater attempts to use a known list of SM passwords first and, if none of these gain access to the radio, it will then prompt the user for the write-level password for the specific SM. See [Edit→Manage Subscriber Module Password List](#) for more details on SM Password usage.

The **HTTP Settings** block allows you to select **HTTP** or **HTTPS**. Devices that operate in their secure mode can be updated by only the HTTPS server, regardless of whether the SM Autoupdate feature is active. These devices in their insecure mode, as well as devices that operate an earlier device software release, can be updated by only the HTTP server if the SM Autoupdate feature is active. Those on an earlier release will be updated by the local HTTP or TFTP server, but the **HTTP** selection here in the preferences will not inhibit that process. The associated port numbers for these selections *are not* reconfigurable and must be unimpeded by the local firewall.

The option **Try another protocol if Selected fails** works as follows:

- When this option selected, the first access attempt for a new operation will always be via the protocol that the operator specified when initially adding the device. If that fails, an attempt will automatically be made using the other protocol.
- When this option is not selected, only one attempt will be made, via the protocol that the operator specified when initially adding the device.

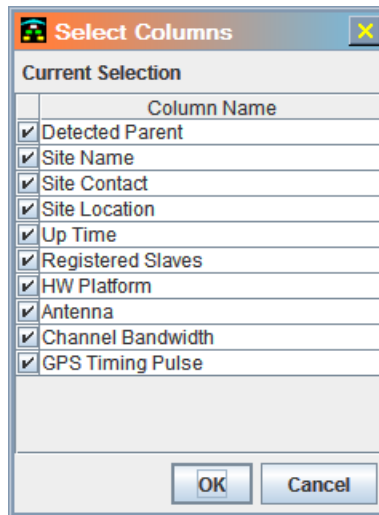
The **Autoupdate Server Address** field is used to specify the default IP address that should be given to APs for their Autoupdate authorization value, which is the IP address that is allowed to initiate Autoupdate commands with the AP. This should be the IP address of the computer running the Network Updater Tool, as seen by the AP. For a description of how the value of this field was set, see [SM Autoupdate Feature](#).

If this value is left blank, then the IP address to be used will be auto-detected based on actual communications between the Network Updater Tool and the AP – in other words the network updater tool will ask the AP “by what IP address do you see my communications?” and use that IP address to load into the AP. In most situations, this value should be left blank. If you have an unusual network configuration, such as the Network Updater Tool behind a NAT box, then you may need to specify this value directly in order for the APs to accept the Autoupdate commands from Network Updater.

## **Edit→Show/Hide Extended Element Information**

Additional attributes about network elements may be available through the extended element information list. These attributes include **Site Name**, **Site Location**, **Site Contact**, **Up Time**, and **Detected Parent**.

August 2021



These attributes are filled in only if information is available for them on the network elements. The following is an example of a network archive file that is displaying the extended attribute columns.

Canopy Network Updater - (New Network)\*

File Edit View Update Tools Help

	Element	Type	ESN	Software Ver.	HW/FPGA Ver.	Boot Ver.	Last Access	State	Progress	Auto Update	Detected Par...	Site Name	Site Contact	Site Location	Up Time
	Network R														
	10.12CPTP700		00045658007D	45700-00-05	B0P04.02-C		09/14/15 04:34...	Refreshed	100%					test_llloc	000:00:01:21
	10.12CPTP700		000456580077	45700-00-05	B0P04.02-C-F...		09/14/15 04:34...	Refreshed	100%				700_Contact	700_Location	000:00:01:20
	10.12CPTP650		000456500018	50650-01-98	B0P01.01-C		09/14/15 04:52...	Refreshed	100%		a	Testing	New Test Loca...		000:00:00:49
	10.12CPTP650		000456500014	50650-01-98	B0P01.01-C		09/14/15 04:52...	Refreshed	100%		test	test	test	test	000:00:00:49

**Detected Parent** is available for only SMs that appear within the Auto-Detected SM list. This information shown has the format

AP: [ *Host\_Name\_or\_IP* ] .LUID: [ # ]

where *Host\_Name\_or\_IP* is the host name or IP address as specified by the user when they entered the AP information into Network Updater, and # is the LUID number assigned to the SM by the AP. For SMs that do not have a direct IP associated with them and shown within the **Element** column for the SM, the **Detected Parent** value may be a duplicate of the information shown in the **Element** column for the SM.

**Up Time** represents the amount of time since the last reboot of the network element.

**note** ..... This value has a maximum limit of ~497days, at which time the “counter” that is reported automatically wraps back around to zero. Therefore, this value may not be entirely accurate if the element has been continuously running for more than 497 days.

Channel Bandwidth applies to only PMP 400/430/500 Series High-performance AP (HPAP) in Release 10.2 or later and the registered SMs in its sector.

**GPS Timing Pulse** applies to only the CMM and indicates its synch mode. Possible values are **Master** and **Slave**.

August 2021

## Edit→Manage Subscriber Module Password List

The Network Updater automatically gathers a list of passwords used for SM write access. This list is gathered by prompting the user when a new SM is discovered and the existing password list does not already contain the write-access password for that SM.

**note** ..... This write-access password should be the **Full Access** password for releases prior to R8.0, and should be the password for the **root** account for releases 8.0 and later.

The existing password list consists of the password for the AP that the SM is registered to, the default system password, and any previously entered SM passwords by the user. The purpose of gathering this list of passwords is to let the Network Updater automatically determine IP addresses and SNMP community string information of SMs. With this information the Network Updater can automatically set up Auto Discovered SMs for direct software updates, as well as display the full list of extended attributes for the SMs (Site Location, Site Contact, and Up Time). See [Edit→Show/Hide Extended Element Information](#) for more details on these attributes.

This edit capability allows users to manage the list of SM passwords automatically gathered by the Network Updater, including removing passwords that are no longer in use by any elements in the system. This menu option is only available if the **Gather SM Passwords and Extract IP Address and SNMP Settings** in the Preferences/Default Settings window is checked (see [Edit→Preferences](#)).

## Edit→Add Elements to Highlighted Element

The element added by this operation will appear under the element currently selected in the network tree. The meaning of the tiers or levels for the items involves the order of updating by the Network Updater tool. Higher-level elements will be updated first. All elements at the same level may be updated simultaneously. Refer to [Network Layers and Orders of Updating Equipment](#) and the maximum number of concurrent updates set within the Update Configuration screen for more information on how Network Updater performs concurrent updates (see [Update→Configure](#)).

August 2021

When adding an element, the user must select either **Network Element** or **Network Element Group (Folder)** from the pull-down menu. By default, it is assumed the element will use the default network password to access it, and it uses the default SNMP community string. If this is not the case then the default box should be unchecked, and the specific password and community string should be entered. For security, the entered password appears as all asterisks in the interface.

**note** ..... This password should be the **Full Access** password for releases prior to R8.0, and should be the password for the **specified login id** for releases 8.0 and later.

Where **Use Default/Inherit Settings from Parent Element** is unchecked, the definitions and guidance provided under [Edit→Preferences](#) for the **User Account**, **HTTP Settings**, and **SNMP Settings** apply. Where it is checked, the fields of these blocks are inherited from the parent and not reconfigurable.

The host names, IP addresses, or ranges of IP addresses for all elements to be added should be put in the **Element Host Name(s)/IP Address(s)** box. This window allows cutting and pasting. Note that each entry should be put on a separate line. Non-IP address text strings are assumed to be host names and are compared against the host file on the workstation that is running Network Updater at the time when communication with the element is required.

After adding elements, you must use one of the following Refresh/Discover options:

- [View→Refresh/Discover Entire Network](#)
- [View→Refresh/Discover Selected Network Elements](#)



August 2021

- [View→Refresh/Discover Selected Network Branches](#)
- [View→Continuous Refresh](#)

## **Edit→Add Elements to Network Root**

This operation behaves like [Edit→Add Elements to Highlighted Element](#), except that the elements added will be added to the root level regardless of what branch is currently selected. All other actions are the same.

August 2021

After adding elements, you must use one of the Refresh/Discover options:

- [View→Refresh/Discover Entire Network](#)
- [View→Refresh/Discover Selected Network Elements](#)
- [View→Refresh/Discover Selected Network Branches](#)
- [View→Continuous Refresh](#)

## Edit→Remove Selected Elements

The user can remove one or more network elements using this operation. All currently selected elements will be removed from the active network. Elements are selected by checking the box to the left of the element in the tree window. If a higher-level element group is selected then all items below it area automatically selected. The user will be prompted to confirm the delete command.

## Edit→Modify Selected Network Element Access

The user can change the network settings for any element or the group name for any element group by selecting this operation. The following dialog opens if *a single element* was selected.

August 2021

**Modify Network Element Access**

Host Name / IP Address: 10.10.0.8

Element Type: PMP 320 FED Access Point (PMPF)

**Network Settings**

☒ Use Default/Inherit Settings from Parent Element

**User Account**

Device Login ID: root

Device Password:

Retype Password:

**HTTP Settings**

HTTP ☒ Port: 80

HTTPS ☐ Port: 443

**SNMP Settings**

SNMP Community: Canopy

SNMP Version: v2c

SecurityLevel: NOAUTH\_NOPRIV

Auth Protocol: MD5

Auth Password: .....

Privacy Protocol: DES

Privacy Password: .....

Context Name:

SNMP Port: 161

**Auto Update Server IP Address**

Leave it empty for auto detection:

OK Cancel

The following dialog opens if *multiple elements* were selected.

August 2021

Additionally, the use of the default password and default SNMP community string for any specific element or element group can be controlled on this screen.

**note** ..... This password should be the **Full Access** password for releases prior to R8.0, and should be the password for the **specified login id** for releases 8.0 and later.

Where **Use Default/Inherit Settings from Parent Element** is unchecked, the definitions and guidance provided under [Edit→Preferences](#) for the **User Account**, **HTTP Settings**, and **SNMP Settings** apply. Where it is checked, the fields of these blocks are inherited from the parent and not reconfigurable.

For PMP 320 APs, the operator must enter the user name and password, separated by underscore, of the admin account (*not* the read-only access string associated with the guest or the installer account) in the **SNMP Community** string field. Where the username and password are unchanged from the factory, the operator must enter the default **admin\_admin**. Where either has been changed, the operator must specify the string composed from and formatted as **username\_password**. Network Updater will not discover the SNMP Community or send a default string where the operator omits populating this field.

The **SNMP Version** field should be set to the version of the agent in the selected element or of the agents that are hierarchically associated with the selected folder. Possible values for the agent(s) are **v1**, **v2c**, and **v3**.

The **Auto Update Server Address** field is used to specify the default IP address that should be given to APs for their Autoupdate authorization value, which is the IP address that is allowed to initiate Autoupdate commands with the AP. This should be the IP address of the computer running the Network Updater Tool, as seen by the AP. If this value is left blank, then the IP address to be used will be auto-detected based on actual communications between the Network Updater Tool and the AP –

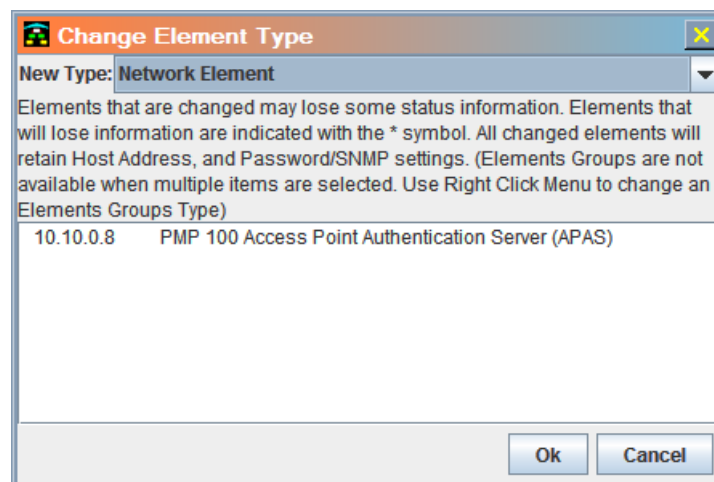
August 2021

in other words the network updater tool will ask the AP “by what IP address do you see my communications”, and use that IP address to load into the AP. In most situations, this value should be left blank. If you have an unusual network configuration, such as the Network Updater Tool behind a NAT box, then you may need to specify this value directly in order for the APs to accept the Autoupdate commands from the Network updater. This field *does not* apply to the PMP 320 AP, which does not support the SM Autoupdate feature.

## Edit→Change Network Element Type

**note** ..... Some network elements may lose information when they are changed to a different element type. The user will be notified which elements are about to lose information, and will be prompted to confirm the operation before continuing.

This operation allows the user to change the type of network element for all currently selected items in the tree.



Element Group may be changed as well as normal network elements, but they may only be changed through the right click convenience function access to the Modify Element Type operation due to how the normal modify operation affects sub items in the tree structure.

August 2021

## Edit→Move Selected Network Elements

This operation allows the user to move the location of a specific element within the Network Updater tree structure. This is very useful if you decide after entering your base network to create element groups, or to fix hierarchical ordering issues with your network tree. This operation will affect the currently selected network elements. A second network tree window will appear allowing the user to select where they would like the selected element moved to. It is possible to move an auto-detected SM from the Subscriber Module (Auto-Detected) tree to the user managed Network Root tree, but it is not possible to move network elements the other way, into the Subscriber Module (Auto-Detected) tree.

## Edit→Open Highlighted Network Element Web Page

This operation opens the web browser to the management interface of the element that is currently highlighted. This operation is similarly available through a right-click on the element followed by selection of the Open Network Element Web Page from the resulting drop-down list of options.

## Edit→Undo Network Changes

This operation rolls back all changes that have been made since the last execution of the **Save Network Archive** command option occurred (see [File→Save Network Archive](#)). This may be useful, for example, in the case where elements that have been deleted should be restored.

## Edit→Find

The find operation is used to search either the network elements tree or the history log for a phrase or word. The user can control the direction of the sort (up or down) and walk through all the

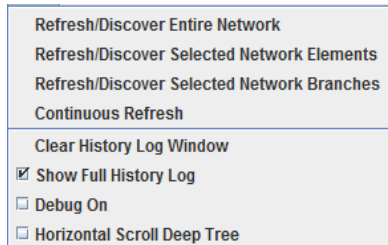
matching instances with the **Find Next** button. When searching within the network element tree all fields related to the elements will be searched for the specified phrase.

## Edit→Cancel Current tasks

This operation allows the user to cancel all the in-progress upgrade processes.

August 2021

### 5.3.3 View Menu



#### View→Refresh/Discover Entire Network

This operation will instruct Network Updater to communicate (through a combination of SNMP and telnet capabilities) with each network element to gather their relevant information (software versions, hardware versions, etc.) as well as inquire as to the latest updated list of SMs that are seen below the indicated APs. Network Updater will validate the element type value for each network element, and if incorrect (based on actual element type information detected from the network), this field will also be updated as a part of the refresh/discover operation. For each element that information is gathered on, Network Updater will update the **Last Access** column indicated as of when the information is valid. The **State** column will indicate if the element was successfully refreshed, or if an SM was newly discovered, or if there was any errors in communicating with the element.

#### View→Refresh/Discover Selected Network Elements

This operation will act like [View→Refresh/Discover Entire Network](#), except it will only operate on the network elements currently selected by checking the box to the left of each network element in the tree. Elements below the selected elements will not be operated upon unless they are also individually selected.

#### View→Refresh/Discover Selected Network Branches

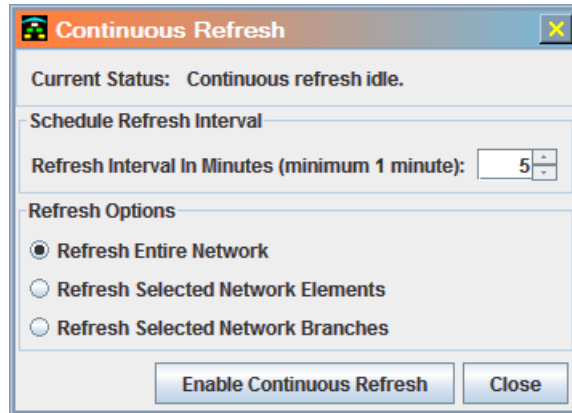
This operation is like [View→Refresh/Discover Entire Network](#), except it will only operate on the network elements and branches that are currently selected by checking the box to the left of each network element in the tree. The elements physically selected, as well as all elements below those selected elements within the tree structure (even if they are not selected) will be refreshed.

#### View→Continuous Refresh

This operation can be used to have the Network Updater continuously poll the network elements for their software version information. The user can do a continuous refresh on the entire network, the selected branches, or the selected elements. This can be useful when the user wishes to monitor the

August 2021

progress of automated updates occurring on the network. The continuous refreshes will repeat based on the interval specified on the dialogue presented to the user.



To initiate continuous refreshes the user must press the **Enable Continuous Refresh** button on the dialogue. When Continuous Refreshes are enabled, the user will see a Continuous Refresh (Enabled) pop-up window that includes the message `Current Status: Refresh in progress ..` as well as buttons to disable this feature or close the progress window.

Continuous refreshes will continue until the user selects either the **Close** button or the **Disable Continuous Refresh** button. If the user wishes to change the interval at which refreshes are occurring, they can press **Disable Continuous Refresh**, change the interval value, and press **Enable Continuous Refresh** again.

## View→Clear History Log Window

This operation clears the History Log Window of all event history. This operation has no effect on the History Log History File, as all events are automatically saved to the History File. This operation is meant to aid the user in tracking current events without the clutter of historical events being on the display window.

## View→Show Full History Log

If the Show Full History Log option is selected, then Network Updater will load the entire history log into the event viewer window upon startup or upon the selection of this option. Otherwise, only the new events generated since Network Updater was started will be shown in the window.

**tip** ..... It is more efficient if only the latest events are shown in the window, so the user may want this option off until a time where they need to view historical events. The user should be aware that if this option is turned on, and they select the Clear History Log Window option, the full history log will no longer be displayed in the Event Window (see [View→Clear History Log Window](#)). To redisplay the full history log the user would either need to restart the Network Updater, or unselect and reselect the **Show Full History Log** option.



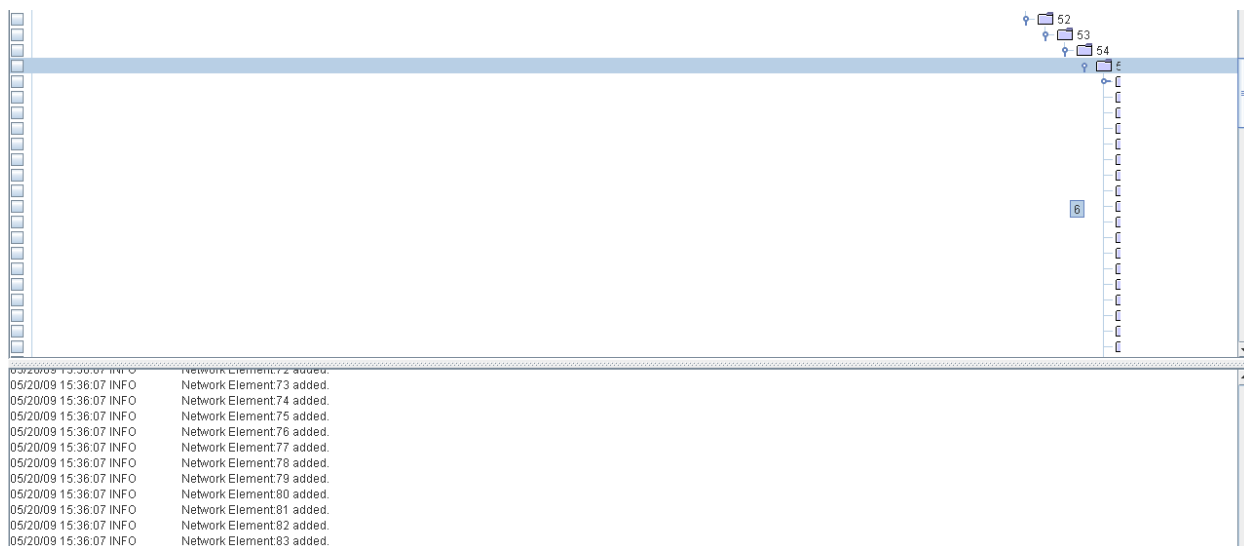
August 2021

## View→Debug on

If the Debug On option is selected, then Network Updater will show the debug logs.

## View→Horizontal Scroll Deep Tree

A toggle-type command option in the main menu enables horizontal scroll bar. The **View→Horizontal Scroll Deep Tree** selection allows the user to see subfolders beyond the 55<sup>th</sup> record to any desired depth of elements.



## 5.3.4 Update Menu

Configure
Http Server Configure
Manage Packages
Update Entire Network Root
Update Selected Network Elements
Update Selected Network Branches
Enable/Disable APs for SM Autoupdate
Schedule Network Update
Upload Certificate To Selected Elements
Upload Certificate To Selected Branches

August 2021

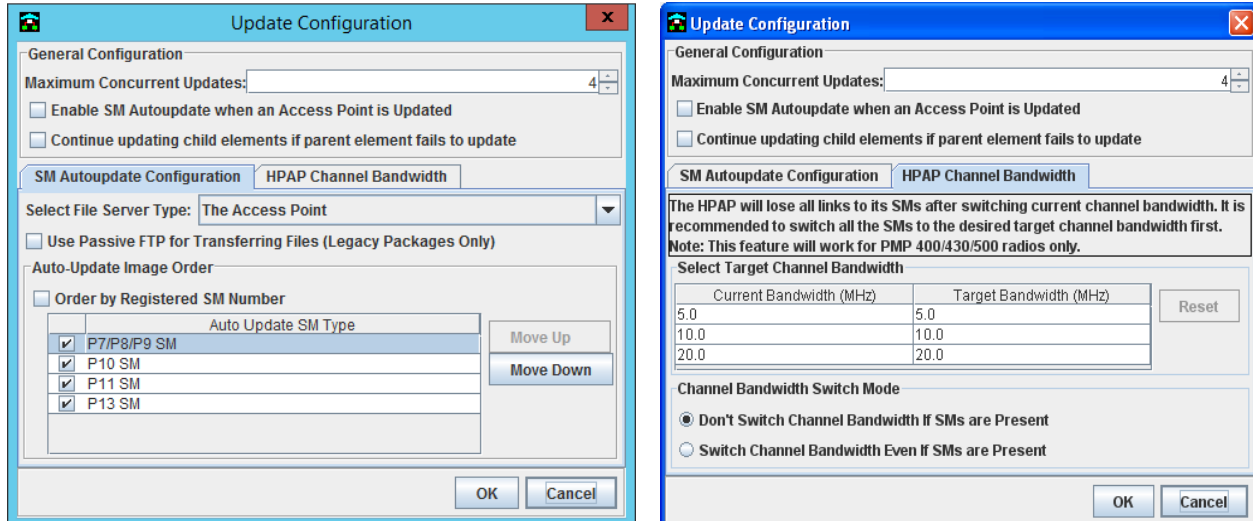
## Update→Configure

This operation allows the user to configure settings related to the Update operations. The user can control:

- how many concurrent updates will be run.
- whether the AP<sup>3</sup> should be used as a file manager, or a local HTTP or TFTP server should be used by the SMs to access software, boot, and FPGA image files.
- the IP address of the local TFTP server access, if this server type is to be used.
- whether Network Updater and associated External Tools should use Active or Passive FTP when communicating to the network elements.
- the order in which to load software images onto the AP, depending on selected firmware type(s).
- in the case of the high-performance PMP 400/430/500 AP
  - a specific channel bandwidth to instruct the HPAP to switch its operation to, based on its current channel bandwidth.
  - whether to proceed with or abandon the channel bandwidth switching operation in the case where the HPAP has at least one currently registered SM.

The specific configurable settings are as follows.

- Where **The Access Point** is selected as the file server type:



<sup>3</sup> Only where the AP supports SM Autoupdate.

August 2021

- Where **CNUT HTTP Server** is selected as the file server type:

The screenshot shows the 'Update Configuration' dialog box. The 'General Configuration' tab is active. Under 'Select File Server Type', 'CNUT HTTP Server' is selected. The 'Auto-Update Image Order' section shows a list of SM types: P7/P8/P9 SM, P10 SM, and P11 SM, all of which are checked. The 'Max Concurrent Updates (Per AP)' is set to 20. The 'HPAP Channel Bandwidth' tab is also visible.

The screenshot shows the 'Update Configuration' dialog box with the 'HPAP Channel Bandwidth' tab selected. A warning message states: 'The HPAP will lose all links to its SMs after switching current channel bandwidth. It is recommended to switch all the SMs to the desired target channel bandwidth first. Note: This feature will work for PMP 400/430/500 radios only.' Below this, there is a table for 'Select Target Channel Bandwidth' with columns for 'Current Bandwidth (MHz)' and 'Target Bandwidth (MHz)'. The table shows values for 5.0, 10.0, and 20.0 MHz. The 'Channel Bandwidth Switch Mode' section has two radio buttons: 'Don't Switch Channel Bandwidth If SMs are Present' (selected) and 'Switch Channel Bandwidth Even If SMs are Present'.

- Where **Local TFTP Server** is selected as the file server type:

The screenshot shows the 'Update Configuration' dialog box with the 'Local TFTP Server' selected as the file server type. The 'Local TFTP Server IP Address' is set to 192.168.0.199. The 'Max Concurrent Updates (Per AP)' is set to 20. The 'TFTP Root Folder' field is empty, and there is a 'Test TFTP Server' button. The 'HPAP Channel Bandwidth' tab is also visible.

The screenshot shows the 'Update Configuration' dialog box with the 'HPAP Channel Bandwidth' tab selected. A warning message states: 'The HPAP will lose all links to its SMs after switching current channel bandwidth. It is recommended to switch all the SMs to the desired target channel bandwidth first. Note: This feature will work for PMP 400/430/500 radios only.' Below this, there is a table for 'Select Target Channel Bandwidth' with columns for 'Current Bandwidth (MHz)' and 'Target Bandwidth (MHz)'. The table shows values for 5.0, 10.0, and 20.0 MHz. The 'Channel Bandwidth Switch Mode' section has two radio buttons: 'Don't Switch Channel Bandwidth If SMs are Present' (selected) and 'Switch Channel Bandwidth Even If SMs are Present'.

The **Maximum Concurrent Updates** should be an attribute of the processing power and available RAM on the computer running Network Updater. This number of updates applies to the number of APs, BHs, and CMMs, that will be updated directly by Network Updater. SMs are not directly updated by the Network Updater unless they have a routable IP address defined for them and are directly selected for updating, but instead SMs are commanded to update themselves by their parent AP, typically after the AP has itself been updated (see [SM Autoupdate Feature](#)). A general rule is that one update per 20 MB of available RAM can be supported. So, if the computer has 256 MB of RAM, then a value of approximately 13 concurrent updates could be supported. Actual performance will vary so the user may need to determine the appropriate value for their network according to their situation and configuration.

August 2021

The user must also consider how concurrent updates both by Network Updater and through the SM Autoupdate feature, will affect network bandwidth (due to usage of available bandwidth in order to deliver the image files to the various network elements). The user may wish to not maximize the parallelism of the upgrade process, or choose to run the network upgrade during off hours when the bandwidth utilization will not impact active customer usage.

If the **Enable SM Autoupdate When an Access Point is Updated** option is checked, then the Network Updater will automatically enable SM Autoupdate on all selected APs after the direct element updates are completed. Using this option saves the user from having to separately turn on SM Autoupdate using [Update→Enable/Disable APs for SM Autoupdate](#). By waiting until all selected network elements (including SMs if they are selected by the user) are directly updated before enabling SM Autoupdate, Network Updater helps to avoid problems that could occur when concurrently using SM Autoupdate at multiple levels in the network tree hierarchy.

**caution..... The Continue updating child elements if parent fails to update option has the inherent risk of putting the child elements out of ability to communicate with the parent. So, extreme caution is advised when this option is considered for selection.**

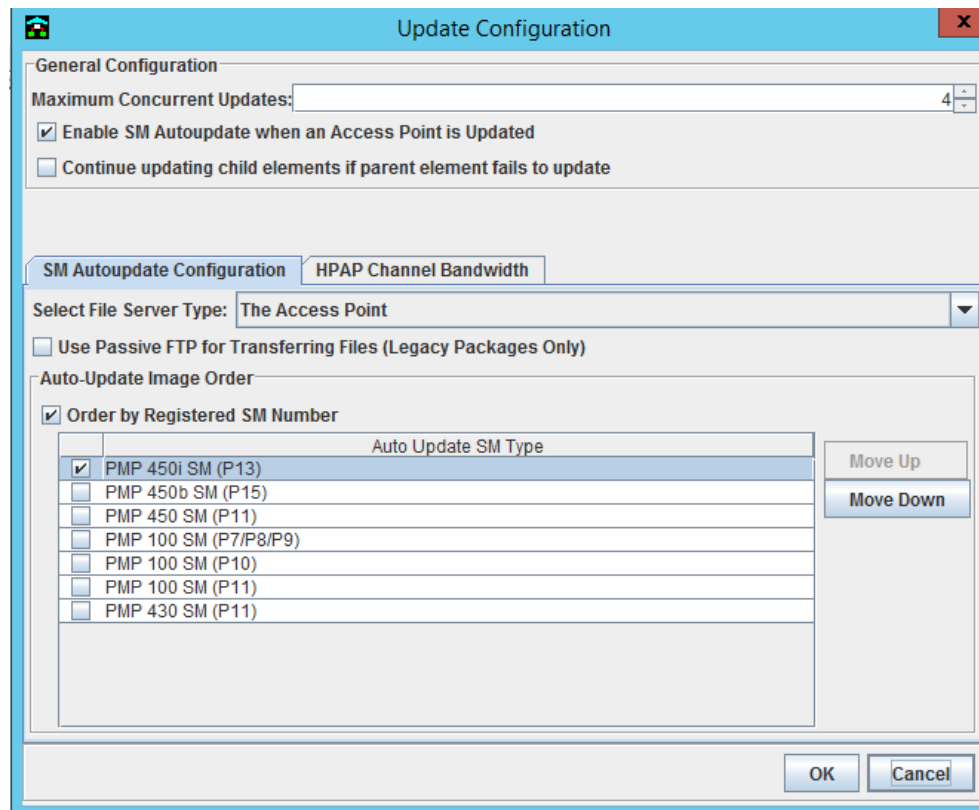
## ***SM Autoupdate Configuration Tab***

To help optimize the upgrade performance on a sector, the selections **The Access Point** and the **CNUT HTTP Server** include the **Auto Update SM Type** block options to **Move Up** or **Move Down** an SM Type and thereby reorder the updates by SM type. Different software images are needed, depending on whether the platform revision is **P7/P8/P9, P10, P11, P13 or P15**, and an AP can hold only one set of the images at a time. Because of this, it is necessary to switch the image on the AP from one to the other to ensure all SMs on the sector can be upgraded. The upgrade package itself will attempt to determine which image is best to load on the AP first during the Autoupdate sequence, but if it cannot determine a good first choice it will make use of the value set here to control which image type to load first. Therefore, if you are running a network of only one image type, and you see a delay in Autoupdate commencing on your network, you can switch this option setting to try to expedite it.

However, a check box is available for **Order by Registered SM Number**. If you check this check box, WM counts the number of registered SMs of each **Autoupdate SM Type** (how many P7/P8/P9, how many P10, and how many P11), and first updates the all the type with the most, then all of the type with the second-most, and then all of the type with the least, ignoring the vertical order specified in the **Auto Update SM Type** block. If you leave this box unchecked, it uses the order in the block.

**Note:** Due to memory limitation on AP devices, it is recommended to select only one SM type at a time when using The Access Point as File Server option to Autoupdate the SMs.

August 2021



If **Continue Updating Child Element if Parent Element Fail to Update** option is set then Network Updater will continue to perform update operations on network elements that appear in the network tree below an element that failed to update. If this option is not checked, then no network elements under a failed element will be updated if a higher-level element failed to update. This option allows the user to ensure consistent releases between parents and children in the network, if that is a concern. On the other hand, if this is not a concern to the user, then by having this option checked they could ensure that Network Updater will update the largest possible portion of the network automatically.

Some non-fatal causes for the tree failing to update an element are as follows:

- The address for the element is non-routable or incorrectly specified, or there is no host value in the host file.
- The current Installation Packages do not contain any upgrade files for the type of network element encountered.
- The network element is not on the network at the time the update is performed.

In several of these instances, it may be possible and safe to continue upgrading elements in the network tree below the element in question.

The SM Autoupdate Configuration section allows the user to specify what among the following means should be used for the file server from which SMs obtain their upgrade files:

- to allow Network Updater to act as an HTTP/HTTPS server. This option configures Network Updater to allow devices to pull their image files from the HTTP/HTTPS server and to

August 2021

monitor upgrade status via SNMP messages. When **CNUT HTTP Server** is selected as the file server type, set the toggle for either

- **Update With All Images** (The update process uses the order specified in the **Auto-Update Image Order** block or automatically chooses the order if that capability is supported in the firmware.)
- **Update Following Image Order Settings** (the update process uses the order specified in the **Auto-Update Image Order** block for all devices that are flagged for updating)
- to use the local TFTP server. With this option, if the firmware supports a *secure* mode, then the device must be set to its *insecure* mode.

This **Local TFTP Server** option requires a configured IP address for the TFTP server and the root directory where Network Updater store the files for the SMs to pull. On a multi-homed computer (one with multiple network interface cards and IP addresses), the address to select from the drop-down list is the one on which the network resides.

The operator is responsible for configuring the TFTP server appropriately, ensuring it is on the network for all SMs to access, and for setting up the root directory. If the TFTP server is configured correctly, the **Test TFTP Server** operation should return a success message. Update progress is monitored by FTP messaging.

When a network TFTP server is used, as many as 20 SMs per AP can perform concurrent upgrades. You can configure Network Updater to allow fewer if you are concerned about overloading the capability of the TFTP server.

- to have the APs serve the upgrade files (**The Access Point**). This typically is the least favorable option, since the other options offload processing from the APs and support a greater number of simultaneous SM updates in the network. When an AP is used as a file server, only 4 SMs associated with a AP can perform concurrent upgrades. The update process uses the order specified in the **Auto-Update Image Order** block for all devices that are flagged for updating. Update progress is monitored by FTP messaging.

**note** ..... An external TFTP server can be used only if the SMs on the network can communicate with the IP address that is specified. In most networks, where the SMs have been configured with an IP address with local Network Accessibility, this will not be the case. The Test TFTP Server button will only verify that the TFTP server is active, and that the TFTP root folder has been correctly configured. It does not guarantee that SM Autoupdate will function correctly for an SM. In order to determine if an SM can communicate with the TFTP server, telnet into the SM, and ping the TFTP server. If the ping test fails, SM Autoupdate will not be able to function. In this case, it is suggested that the user default to using the Access Point as the File Server. SM Autoupdate will always work in this configuration.

## HPAP Channel Bandwidth Tab

**important** ..... An alternative to the use of this tab exists. The alternative has the advantage of configuring bandwidth without pushing a new image to the elements. See [Bandwidth Updater](#).

Improper use of this tab can result in SMs dropping their connections to the HPAP and not being able to reconnect:

- The PMP 430 Series SM that operates on Release 10.0 or 10.1.1 cannot communicate with an AP that operates on Release 10.2 or later. So, under no circumstances should you

August 2021

upgrade any PMP 430 Series AP to Release 10.2 or later until all of its SMs have first been upgraded to that release.

- Similarly, a Release 10.2 or later HPAP that is set to a channel bandwidth that differs from that of its SMs cannot communicate with its SMs. So, the desired channel bandwidth should never be set in the HPAP until it is set in all the SMs in the sector.
- In the case where you want to downgrade a sector from Release 10.2 or later to Release 10.1 or 10.0, you must first change the sector to the 10-MHz channel bandwidth (SMs first) and then downgrade all the SMs before you downgrade the HPAP.

However, inherent in a sector of any considerable size is the fact that, at any given time (when you would like to cut over to the new release or later to the new channel bandwidth), some of the SMs are likely to be out of service (powered down by the end user or encountering transient RF problems, for example). To avoid or minimize trouble, you can

58. use Prizm to identify the out-of-service SMs by their red icon color.
59. use Prizm to display the correlated customer contact information.
60. ask the end customer to attempt to re-establish the link before you proceed with the operation that has the hazard of stranding SMs.

Proper use of this tab is as sequenced in the following example. The goal in the example case is to have an entire HPAP tower linked at 20-MHz channel bandwidth, and no SMs that are unable to reconnect to the HPAP in case they go out of service for some reason after successful connection at that size of channel. Perform the following steps:

61. Plan your upgrade session to occur at a date and time when historical data suggests that the fewest SMs are not in service.
62. When the date and time arrive, send a blast to all customers, urging them to keep their sessions up.
63. Use alternative means to ask customers whose SMs are out of session to attempt to reconnect the RF link.
64. In the network browser of the main console window, highlight all APs of the tower.
65. From the main menu, select **Update→Manage Packages**.
66. Check only the upgrade package for Release 10.2 or later (in AES or DES) and uncheck any others that are checked in the Package List.
67. Click **Close**.

From the main menu, select **Update→Enable/Disable APs for SM Autoupdate**

68. In the Elements block of the resulting Enable/Disable APs for SM Autoupdate dialog window, select either
  - **Selected Network Elements** for updating only the SMs immediately beneath the APs that you highlighted.
  - **Selected Network Branches** for updating all of the SMs that are under the folders or APs that you highlighted.
69. In the Mode block of this dialog window, select **Enable**.
70. At the bottom of this dialog window, click **OK**.
71. From the main menu, select **Update→Update Selected Network Elements**.

August 2021

72. Click **Yes** to confirm that Network Updater should execute the update operation.  
**RESULT:** All the registered SMs in the sector are upgraded to Release 10.2 and then drop their registrations to the AP.
73. When all in-session SMs have been upgraded, make another attempt to get any that are still running the old release upgraded.  
**IMPORTANT:** Any that you still cannot upgrade will require a truck roll before they will be able to reconnect to the HPAP.
74. From the main menu, select **Update→Enable/Disable APs for SM Autoupdate**.
75. In the Mode block of the resulting Enable/Disable APs for SM Autoupdate dialog window, select **Disable**.
76. At the bottom of this dialog window, click **OK**.
77. From the main menu, select **Update→Update Selected Network Elements**.
78. Click **Yes** to confirm that Network Updater should execute the update operation.  
**RESULT:** The APs are upgraded to Release 10.2 as HPAPs, and then all of the upgraded SMs re-register into their HPAPs.
79. Wait until all of the upgraded SMs have re-registered.
80. From the main menu, select **Update→Configure**.
81. Use the HPAP Channel Bandwidth tab to set the **Target Bandwidth** to **20 MHz** for the **Current Bandwidth**. Click in the Target Bandwidth column at the proper row to expose the drop-down selection list.
82. In the Channel Bandwidth Switch Mode block of this tab, select **Switch Channel Bandwidth Even if SMs are Present**.
83. At the bottom of this tab, click **OK**.
84. From the main menu, select **Update→Enable/Disable APs for SM Autoupdate**.
85. In the Mode block of the resulting Enable/Disable APs for SM Autoupdate dialog window, select **Autoupdate SM Channel Bandwidth**.
86. At the bottom of this tab, click **OK**.
87. From the main menu, select **Update→Update Selected Network Elements**.
88. Click **Yes** to confirm that Network Updater should execute the update operation.  
**RESULT:** The channel bandwidth of all connected SMs is changed to 20 MHz, and they drop their connections to their HPAPs.
89. From the main menu, select **Update→Enable/Disable APs for SM Autoupdate**.
90. In the Mode block of the resulting Enable/Disable APs for SM Autoupdate dialog window, select **Disable**.
91. At the bottom of this tab, click **OK**.
92. From the main menu, select **Update→Update Selected Network Elements**.
93. Click **Yes** to confirm that Network Updater should execute the update operation.  
**RESULT:** The channel bandwidth of the HPAPs is changed to 20 MHz, and all sectors of the tower are operational when all of the SMs have re-registered following the reboot, except for those SMs that were not in session during both the upgrade and the channel bandwidth change, and consequently will require a truck roll.



August 2021

In a second example that follows here, the goal is to downgrade an entire HPAP tower from Release 10.2 or later to Release 10.1.1, and have no SMs that are unable to reconnect to the HPAP. Perform the following steps:

94. Plan your downgrade session to occur at a date and time when historical data suggests that the fewest SMs are not in service.
95. When the date and time arrive, send a blast to all customers, urging them to keep their sessions up.
96. Use alternative means to ask customers whose SMs are out of session to attempt to reconnect the RF link.
97. In the network browser of the main console window, highlight all HPAPs of the tower.
98. In the HPAP Channel Bandwidth tab, click in the Target Bandwidth column at the 5.0 (MHz) Current Bandwidth row to expose the drop-down selection list and select **10.0 (MHz)** for **Target Bandwidth**.
99. Click in the Target Bandwidth column at the 10.0 (MHz) Current Bandwidth row to expose the drop-down selection list and select **10.0 (MHz)** for **Target Bandwidth**.
100. Click in the Target Bandwidth column at the 20.0 (MHz) Current Bandwidth row to expose the drop-down selection list and select **10.0 (MHz)** for **Target Bandwidth**.
101. At the bottom of the HPAP Channel Bandwidth tab, click OK.
102. From the main menu, select **Update→Enable/Disable APs for SM Autoupdate**.
103. In the Elements block of the resulting Enable/Disable APs for SM Autoupdate dialog window, select either
  - **Selected Network Elements** for updating only the SMs immediately beneath the APs that you highlighted.
  - **Selected Network Branches** for updating all of the SMs that are under the folders or APs that you highlighted.
104. In the Mode block of this dialog, select **Autoupdate SM Channel Bandwidth**.
105. At the bottom of this dialog, click **OK**.
106. From the main menu, select **Update→Update Selected Network Elements**.
107. Click **Yes** to confirm that Network Updater should execute the update operation.

**RESULT:** The channel bandwidth is changed to 10.0 MHz in the SMs.

**note** ..... When this occurs, connection between the HPAPs and these SMs is dropped, except where the HPAPs are already operating in 10-MHz channel bandwidth.

108. When all in-session SMs have been reconfigured to 10-MHz operation, make another attempt to get any that are still operating in either the 5- or the 20-MHz channel bandwidth reconfigured to 10 MHz and click **OK** again in the Enable/Disable APs for SM Autoupdate dialog window to reconfigure them.

**important** ..... Any that you still cannot reconfigure to 10 MHz will require a truck roll before they will be able to reconnect to the HPAP.

1. Allow sufficient time for the SMs whose connections were dropped to re-register in their APs after the reboot.
2. From the main menu, select **Update→Manage Packages**.

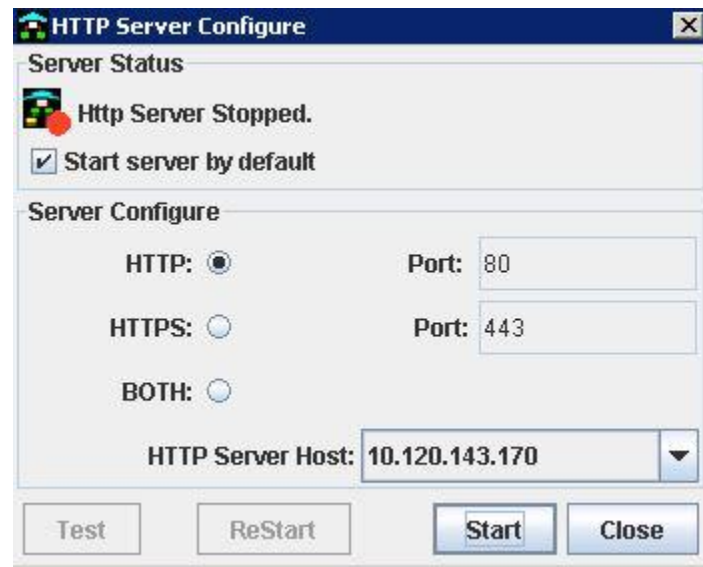
August 2021

3. Check only the **CANOPY101\_1\_Downgrade\_OFDM\_AESorDES.pkg3** package and uncheck any others that are checked in the Package List.
4. Click **Close**.
5. From the main menu, select **Update→Enable/Disable APs for SM Autoupdate**.
6. In the Mode block of this dialog, select **Enable**.
7. Click **OK**.
8. In the main menu, select **Update→Update Selected Network Elements**.  
***RESULT:*** Only the registered SMs (not the HPAPs also) are downgraded to Release 10.1.1. They will drop their connections to the HPAPs and be unable to re-register.
9. Click **Yes** to confirm that Network Updater should execute the update operation.
10. From the main menu, select **Update→Enable/Disable APs for SM Autoupdate**.
11. In the Mode block of this dialog, select **Disable**.
12. Click **OK**.
13. From the main menu, select **Update→Update Selected Network Elements**.
14. Click **Yes** to confirm that Network Updater should execute the update operation.  
***RESULT:*** This time, the HPAPs are downgraded to Release 10.1.1. The SM connections will drop and then be re-established after the reboot, at which point all sectors of the tower will be operating on Release 10.1.1, except for those SMs that were not in session during both the channel bandwidth change and the downgrade, and consequently will require a truck roll.

## Update→Http Server Configure

The SM Autoupdate Configuration section allows the user to specify Network Updater to act as an HTTP/HTTPS server for devices that support this option. It configures Network Updater to push image files to the devices via SNMP commands, to monitor upgrade status via SNMP messages, and to allow the devices to pull image files from the configured HTTP/HTTPS server. Update progress is monitored by SNMP messaging.

August 2021



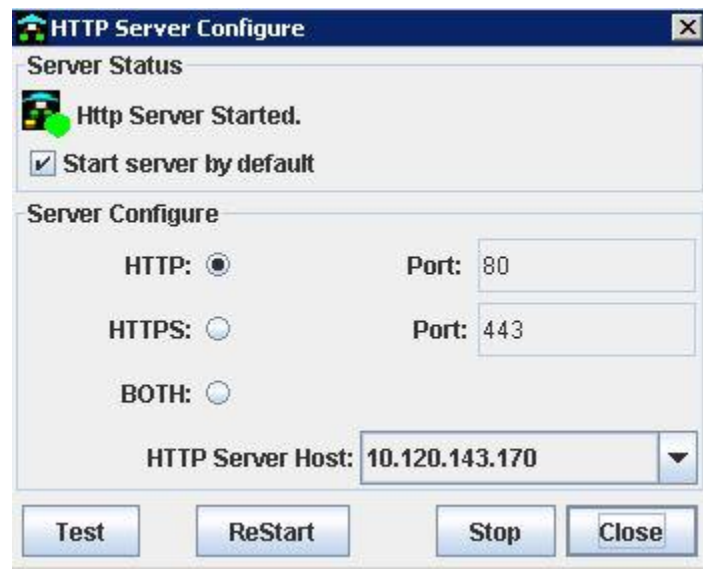
When **CNUT HTTP Server** is selected as the file server type (see [Update→Configure](#)), this interface allows you to specify

- **HTTP** (for updating devices that are operating in their insecure mode)
- **HTTPS** (for updating devices that are in either their secure or insecure mode, under the SM Autoupdate feature)
- **BOTH** (to cover every case). This is the recommended setting.

The port numbers associated with these servers are displayed but not reconfigurable. The IP address that you select in the case of a multi-homed Network Updater computer (one with multiple network interface cards and IP addresses) must be both the address of Network Updater and reachable from every device that will be pulling image files from its file server.

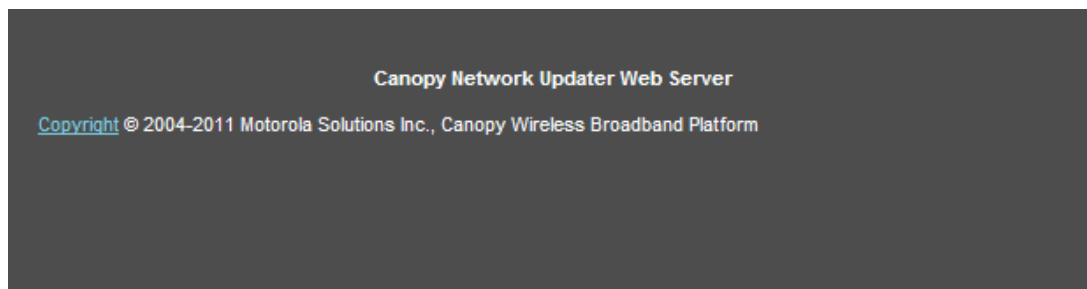
Upon system startup, Network Updater by default attempts to start the file server that is configured here. If you wish to suppress that file server startup attempt, uncheck the **Start server by default** option in this interface.

August 2021



When you change any configured setting in this interface, your change will not take effect unless you apply it by a click of the **Restart** button.

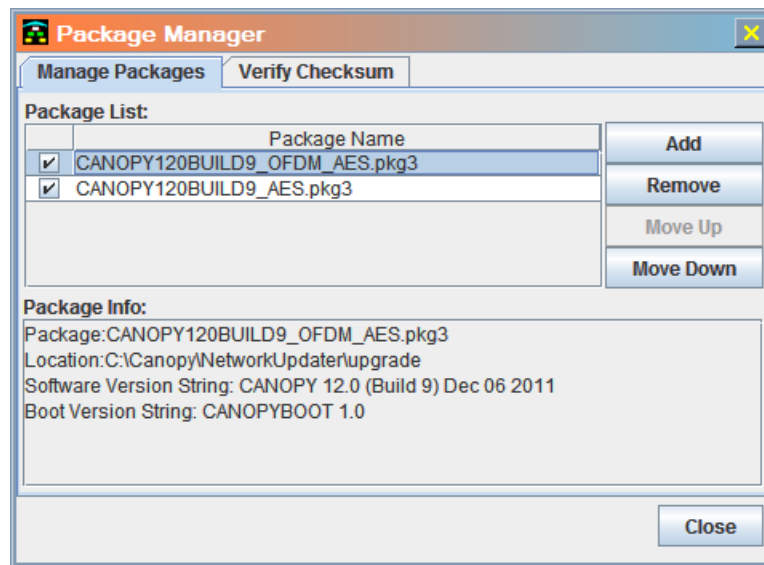
In the Server Status block at the top of this interface, Network Updater indicates the file server status with either `Http Server Stopped` or `Http Server Started`. To start the file server if it is current stopped, click the **Start** button. Whenever the file server is running (started), you can test its connectivity to the Network Updater application by clicking the **Test** button. A successful test returns the following as either [localhost/index.html](http://localhost/index.html) or <https://localhost/index.html>, depending on whether the test is applied to the connection is in HTTP or HTTPS:



## Update→Manage Packages

This operation lets the user tell Network Updater about available upgrade packages that can be used for upgrading the network. Network Updater can be told about unlimited packages, and be told to use one or more of them at a time.

August 2021



New Packages can be added through the **Add** function. The user will be prompted to select the package through a file browser. Packages that are no longer used or out of date can be removed from the Manage Package window by using the **Remove** operation. This can help the user reduce clutter and possible upgrade confusion.

**note** ..... The currently highlighted (versus currently checked) packages are what will be removed. You can only remove one package at a time.

The current packages that Network Updater will use when performing upgrades are indicated by checking the desired packages in the package list. All checked packages will be examined by Network Updater for required software and firmware to perform upgrades from.

The order that the packages appear in the list is the order which Network Updater will examine them to find a software or firmware load to upgrade any network element. Network Updater will continue to look at the packages until it comes upon a component within a package that can be used for a network element. Only the first acceptable component for the network element will be used. In general, most software packages contain software for all types of radios and platforms, so selecting just the latest software package will be sufficient to perform most upgrades.

The user can change the order that Network Updater will examine the packages by highlighting any package and using the **Move Up** or **Move Down** operations.

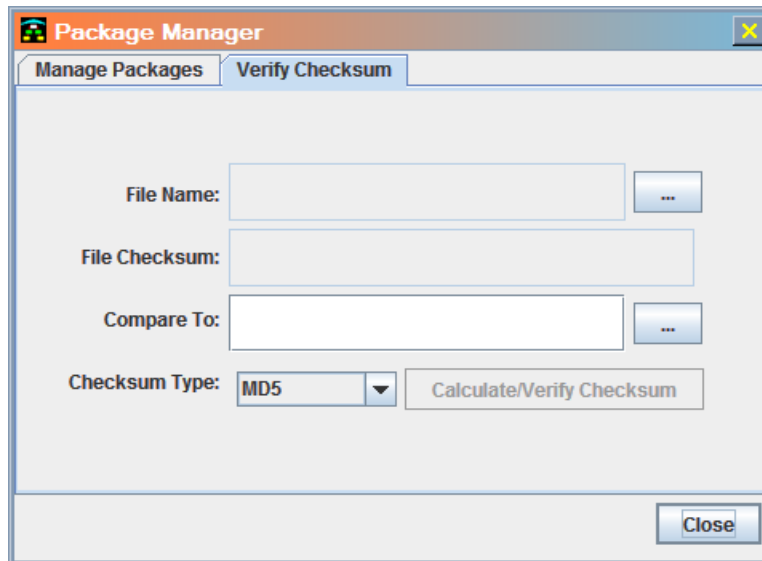
The Package Info window displays the relevant information about the package contents. This window shows the name of the package, file location, and the version names of the following sub-components of a upgrade package, if they are included in the package:

- Software Version String
- Boot Version String
- Hardware Version String (FPGA)
- CMM-Software Version String

After downloading a package file, verifying its checksum value against the value of the companion md5 file is recommended to ensure that the package file did not become corrupted during the

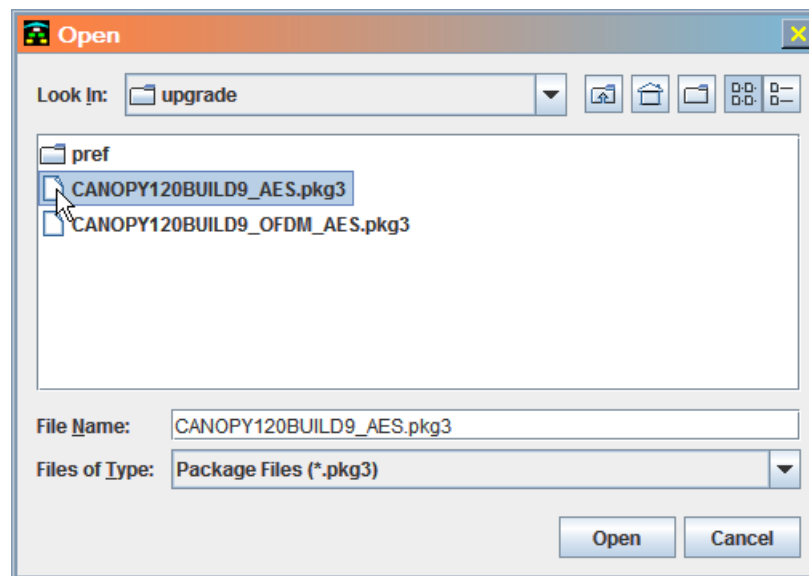
August 2021

download process. Network Updater provides an efficient means for the operator to do this. In the Package Manager interface, click the Verify Checksum tab.

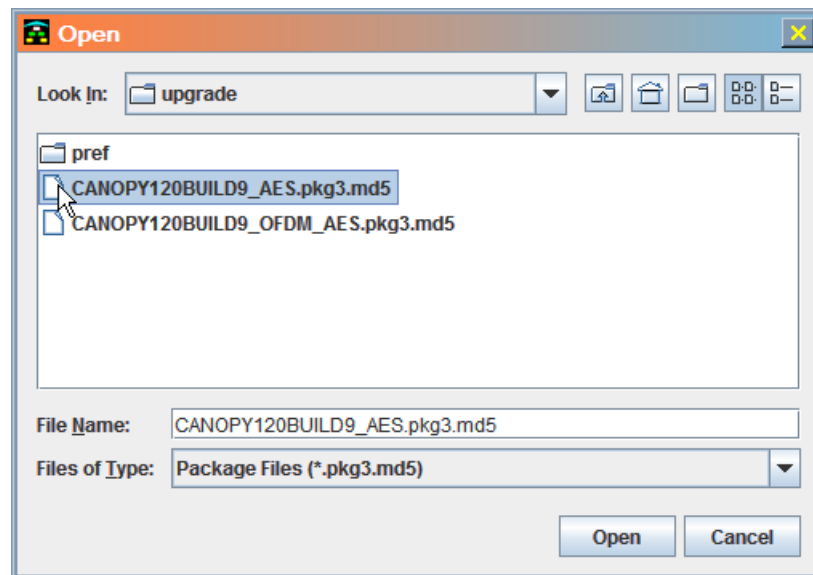


Use this feature as follows:

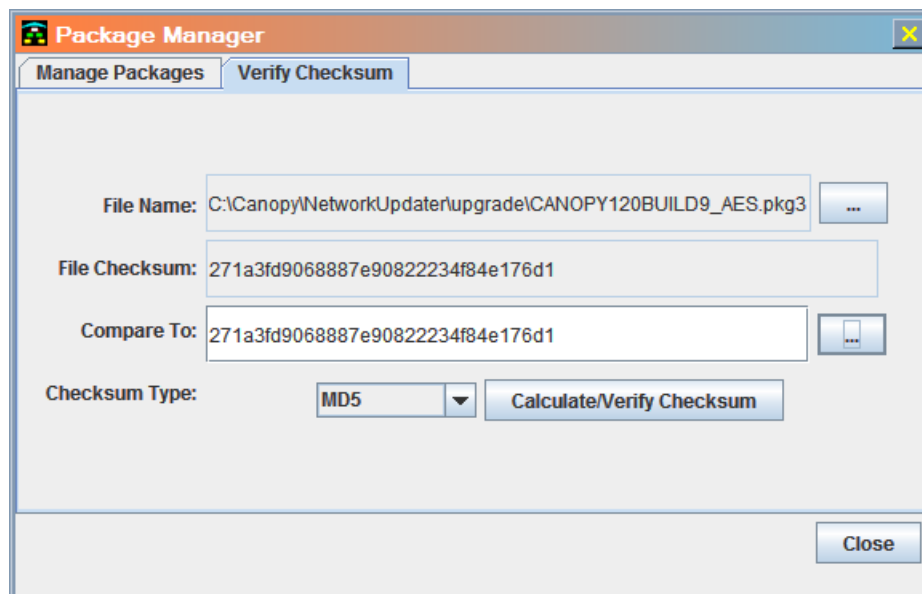
1. For **File Name**, click the associated ellipsis button and browse to and select the package file.



2. Click the **Calculate/Verify Checksum** button.
3. For **Compare To**, click the associated ellipsis button and browse to and select the md5 file.



1. Visually compare the values that are displayed in the **File Checksum** and **Compare To** fields.



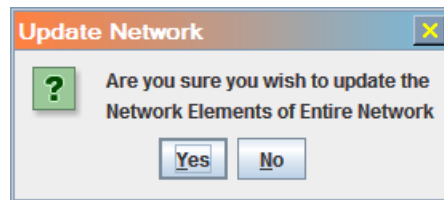
If these values match, the condition of the package file is valid. If they do not, the package file has been corrupted. In this case, repeat the download of the package file and repeat this verification procedure on the newer downloaded file.

**note** ..... The utility of this feature extends to any type of downloaded file that has a companion md5 value. It is not limited to Network Updater package files.

August 2021

## Update→Update Entire Network Root

This operation will cause the Network Updater to access each network element below the Network Root to check its current software, boot, and FPGA versions as applicable. Since this operation will cause changes on the network elements, the user is asked to confirm the operation prior to continuing.



This operation will not operate on any SMs that have been auto-detected. If the versions are not the same as the first set of software, boot, or FPGA files found in the currently active Packages (see [Update→Manage Packages](#)), then an update of the network element will be initiated.

For non-PMP 320 sectors, it is possible to update SMs in the network in two ways, either enabling the SM Autoupdate capability on the APs (see [Update→Enable/Disable APs for SM Autoupdate](#) and [SM Autoupdate Feature](#)), or directly updating the SM from Network Updater. If a SM is selected when this operation is performed, Network Updater will look to see if a routable IP address has been specified for the SM. If an IP address has been specified, then Network Updater will access the SM and perform the upgrade directly. If an IP is not specified, and only LUID through an AP is known, then Network Update will not be able to perform a direct upgrade. In this instance either a routable IP address must be provided for the SM, or the AP that the SM is attached to should have SM Autoupdate enabled to force the SM to upgrade itself.

The user can monitor the progress of the Network Updater updates in the History Log Window. Additionally, the **State** column will show the current status of elements being updated. Network Updater will perform the updates to multiple network elements simultaneously based on the tree structure defined by the user (see [Network Layers and Orders of Updating Equipment](#)) and the maximum number of concurrent updates set within the Update Configuration screen (see [Update→Configure](#)).

Network Updater validates an element's type before performing an update operation, thus ensuring that incorrect or out of date information in the tool does not cause issues on the actual network elements. When all of the selected network elements have been visited and updated, the main Network Updater screen will be refreshed showing the new versions of software, boot, and hardware (FPGA) for each network element, as applicable.

## Update→Update Selected Network Elements

This operation will act like [Update→Update Entire Network Root](#), except it will run against only network elements that are currently selected using the check boxes on each row. This operation does allow the user to select auto-detected SMs to be directly updated by the Network Updater tool.



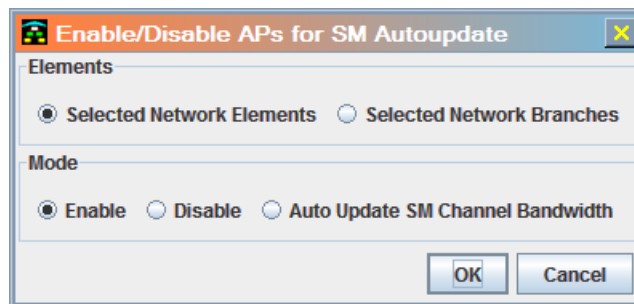
August 2021

## Update→Update Selected Network Branches

This operation will act like [Update→Update Selected Network Elements](#), except it will run against all network elements below any selected Network Branches, even if the network elements themselves are not currently selected. This operation does allow the user to select auto-detected SMs to be directly updated by the Network Updater tool.

## Update→Enable/Disable APs for SM Autoupdate

This operation allows the user to enable or disable SM Autoupdate on the APs (see [SM Autoupdate Feature](#)) within the Network, other than PMP 320 APs.



The user can operate upon Selected Network Elements, or Selected Network Branches. If the user chooses Selected Network Branches, then all elements below the selected network branches will be operated upon even if the network elements themselves are not currently selected. The SM Autoupdate mode will remain in effect on the selected APs until either the user disables it, or the APs are rebooted, whichever comes first.

The Auto Update SM Channel Bandwidth option instructs the PMP 400/430/500 Series High-performance AP to reconfigure the channel bandwidth in its SMs that operate on Release 10.2 or later. This option must be used before the option to switch the channel bandwidth of the HPAP is used. See [HPAP Channel Bandwidth Tab](#).

Network Updater is able to change the state of an AP to **Disable** regardless of whether it is accessible at the time that this selection is enforced by clicking **OK**.

## Update→TimeOut Configurations

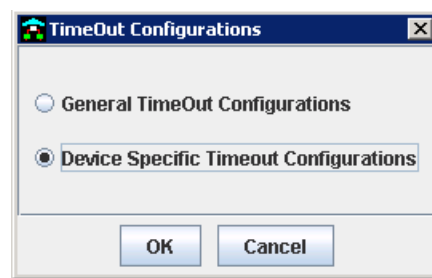
The TimeOut Configurations utility in the Network Updater GUI allows you to configure timeouts specific to device type by providing a way to compensate for the fact that some types of SMs need more time after an update than others do to connect to their APs. This utility includes default timeouts, but the capability to adjust these is further protection against Network Updater upgrading fewer than the full set of targeted SMs.

August 2021

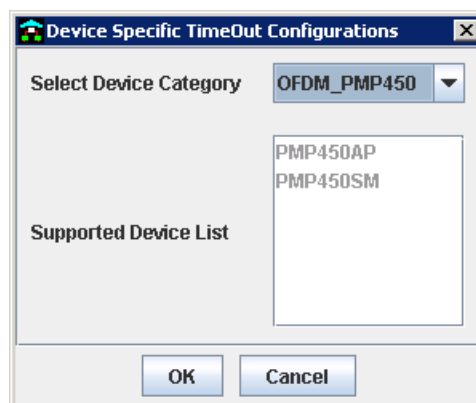
Currently, the adjustment capability is for only PMP 450 sectors, whose SMs have required up to 6 minutes per upgrade and may require up to 10 minutes, but *must be* upgraded before their APs. The settable parameters for timeouts in this case are

- how frequently Network Updater will check whether an SM has reregistered. The new default value for PMP 450 is 20 seconds for each SM.
- how much time will elapse before a timeout stops those queries and throws an error to the Network Updater log. The new default value for PMP 450 is 600 seconds for each SM.

When you select the **Update→TimeOut Configurations** command option, Network Updater opens the TimeOut Configurations window.



Although this window provides a selectable radio button for General TimeOut Configurations, this selection is present for only future use. When you select **Device Specific Timeout Configurations** and click **OK**, Network Updater opens the Device Specific TimeOut Configurations dialog.

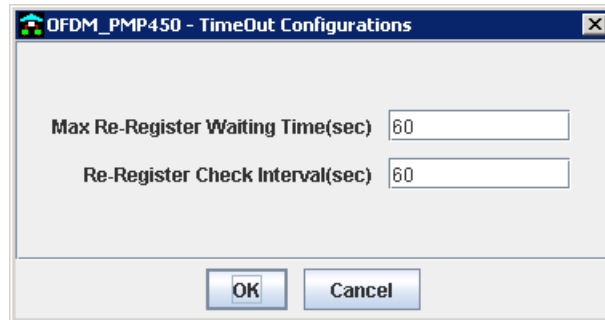


Currently, the only supported item in the Select Device Category drop-down list is **OFDM\_PMP450**.

**note** ..... It is expected that the category list will ultimately include individual device types and groupings of device types. For example, **OFDM\_PMP450** includes both the SM and the AP.

When you select this item and click **OK**, Network Updater opens the OFDM\_PMP450 - TimeOut Configurations dialog.

August 2021



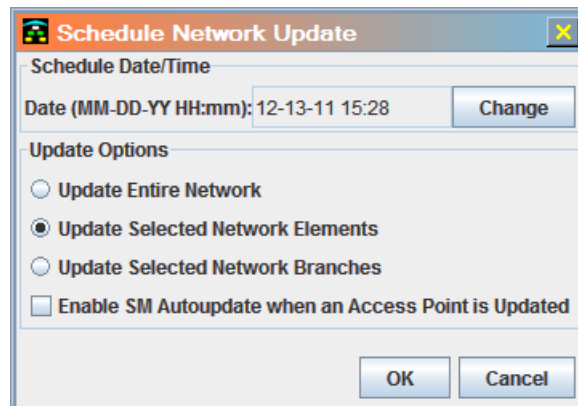
The **Max Re-Register Waiting Time(sec)** is the maximum time for which Network Updater will wait for the SM to reregister in its AP. The default time is 600 seconds. If you find that some sector update operations for this category of device types are failing to update all the SMs

1. check the logs. If errors thrown were for not responding to the OID that starts the update in the SM, then those errors indicate that timeouts occurred during the reboot attempts. In this case, proceed to the next step.
2. reset the value of this parameter to greater than 600.

The **Re-Register Check Interval (sec)** is the interval between attempts that Network Updater will make to find out whether the SM has reregistered in its AP. The default interval is 20 seconds. To reduce management messaging traffic, you can increase the value of this parameter; to speed up sector updates in a network where timeouts are generally not encountered, decrease it. The latter can make the overall process move faster because, by default, Network Updater is updating a maximum of four network elements at a given time. However, the maximum concurrency level can be optionally increased from four to any number fewer than 21.

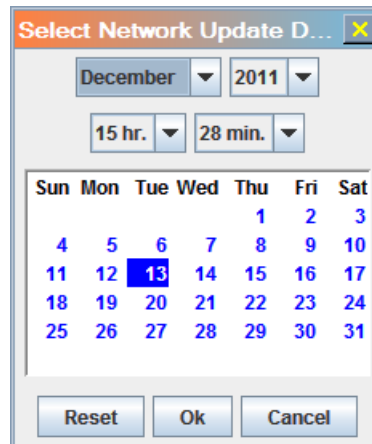
## Update→Schedule Network Update

Network Updater allows the user to setup their network for a full or partial upgrade, and then schedule the actual update operations to start at some time in the future. This is useful when you want to have the actual updates performed at off hours, since there will be slight service interruptions to subscribers as the various network elements are updated.



August 2021

The user can either manually type in the date and time they wish the update operation to commence, or they can click the **Change** button and use the GUI clock and calendar window to specify the start date and time. All reference to start time is in association with the system clock and settings (such as time zone) of the local computer that is running Network Updater.



The user then selects from among the following options the type of update operation to perform:

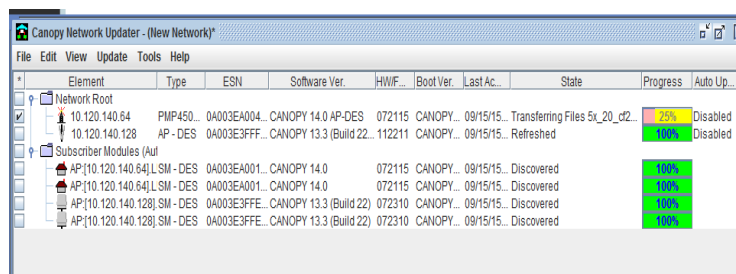
- [View→Refresh/Discover Entire Network](#)
- [View→Refresh/Discover Selected Network Elements](#)

Finally, the user indicates if they would like SM Autoupdate enabled at the completion of the update operation. These operations will perform identically whether the user does them off the Update menu directly, or does them through a scheduled update operation. While the user is still selecting the start time for the scheduled update operation, and the type of operation to be performed, they may still interact with the Network Updater main menu to select and deselect elements and branches that may be affected by the scheduled update operation.

The user puts Network Updater into a Scheduled Update mode by selecting the **OK** button on the Schedule Network Update window. This operation locks Network Updater until the scheduled time is reached, at which time Network Updater will commence with the specified update command.

To cancel the scheduled update, select this operation from the menu and click the **Change** button in the Schedule Network Update interface, then in the calendar interface, click the **Reset** button and then **OK**.

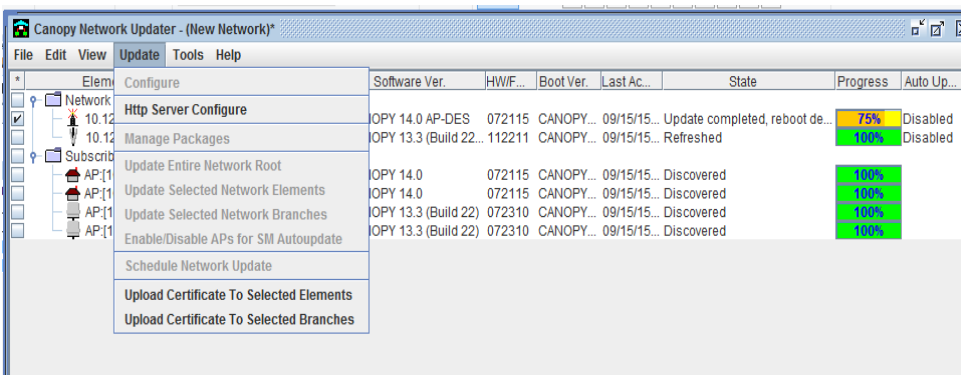
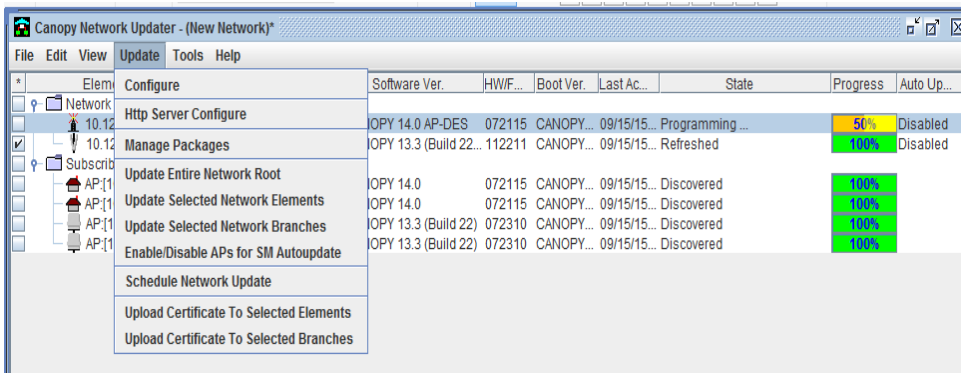
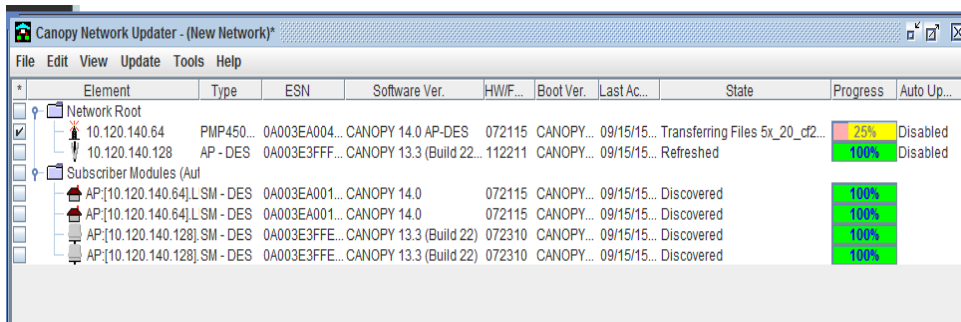
When an update begins, Network Updater shows its status in a Progress pop-up window.



August 2021

## Upgrades are non-blocking

When devices are upgrading, all the key operations like adding network root, manage packages, modify element, refresh, upgrade are not blocked. The user can also start upgrade of other devices. Most operations are blocked only for device in upgrade. For other devices those are not upgrading, all the operations can be performed on them.



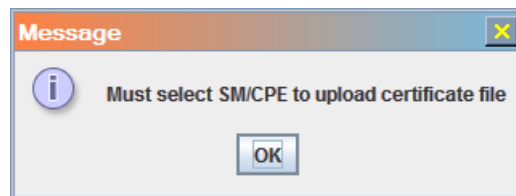
August 2021

## Update→Upload Certificate to Selected Elements

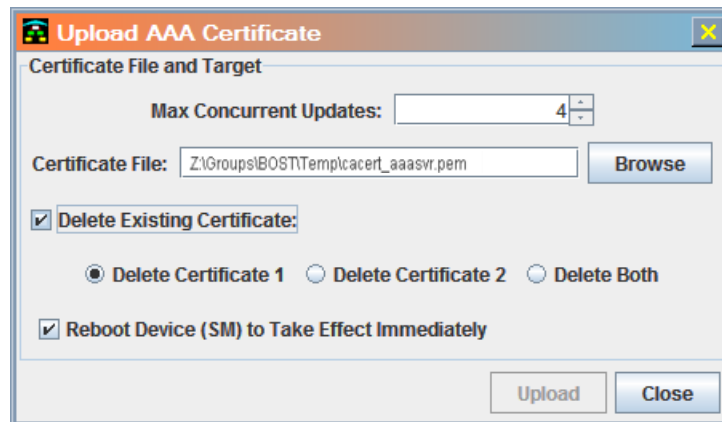
This feature allows the user to apply a AAA (RADIUS) authentication certificate to any one or more selected PMP SMs and/or PMP 320 CPE devices. The target devices do not require IP addresses, since the AP relationship that underlies this function with its registered devices is the LUID assignments for the them within the APs. However, this feature requires that the LUIDs of the target devices is current.

**important** ..... To ensure current LUIDs, refresh the APs before executing this Network Updater command option.

If the user selects this option when no PMP slave devices are selected, then Network Updater returns the following error:



When at least one PMP SM or PMP 320 CPE device is selected before this utility is invoked, Network Updater launches the Upload AAA Certificate dialog:



This utility supports the deletion of either existing certificate before the new certificate upload begins from the same launch. However, when both certificates already exist and neither of these is selected for deletion, the device type determines whether a new upload attempt can succeed:

- In a PMP 320 CPE device, the new certificate overwrites the existing one.
- In a PMP SM, Network Updater aborts the upload process and throws an error that signals the operator that it was aborted due to the lack of an available certificate slot.

Similarly, the device type determines whether a certificate becomes effective upon upload:

- In a PMP 320 CPE device, it does.
- In a PMP SM, it does not until the next reboot of the SM. Given this condition, the user can

August 2021

- select the **Reboot Device (SM)to Take Effect Immediately** option to put the new certificate into effect as soon as the reboot is finished
- leave this option unselected and be aware that it will become effective only after some other reboot event.

For information about AAA authentication, the two certificate positions, and the effect of applying certificates, see the user guide and release notes that support the target device(s). See also [Set SM/CPE Security](#).

## Update→Upload Certificate to Selected Branches

This operation will act like [Error! Reference source not found.](#), except that it will run against all PMP SMs and/or PMP 320 CPE devices beneath all selected network branches, even if the devices at those levels are not currently selected.

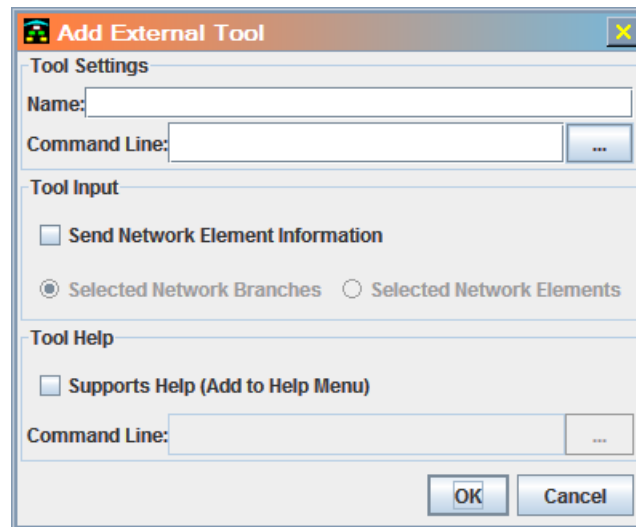
### 5.3.5 Tools Menu

Add external Tool to Menu
Edit External Tool Menu
Launch external Tool
Configure Advantage Platform Scheduler
Gather Customer Support Information
Reboot Unit
Set Access Point Authentication Mode
Set Autoupdate Address on APs
Set SNMP Accessibility
Set SM/CPE Security

## Tools→Add External Tool to Menu

This operation allows the user to associate any script or program with the Network Updater.

August 2021



The first thing a user should do when adding a new External Tool to the Network Updater is identify the core tool executable file. This is done by pressing the file chooser button next to the **Command Line** input box. Based on the External Tool file chosen, the External tool may automatically fill in all other required information on the Add External Tool dialogue. If the External Tool does not automatically fill this information in, then the user will need to supply the rest of the required information before adding the External Tool to the Network Updater.

Each script is given a **Name**, and the user must input either the path and file name for the script that is to be executed, or the actual executable script text. The script will be run one or more times depending on whether the **Send Network Element Information** box is checked.

The **Command Line** attribute can include any application that can be executed (including shell scripts, Perl scripts, and batch files). Command line parameters can be passed as well by including them within the command line.

If the Selected Network Branches option is checked, then the script will be called once for every element under the selected network branches (even if the sub elements are not currently selected), including the root of the branch if it is an element, versus a Element Group.

If Selected Network Elements option is checked, then the script will be called once for every network element selected.

Once a script is associated with the Network Updater through the **Add External Tools to Menu** operation, it will appear in the **Tools** menu for the user to select and run. If the user selects the tool from the **Tools** menu to run, they will have the option of changing the parameter settings (sending parameters, operating on selected branches, or operating on selected elements). Any changes done at that time will only apply to that instance of the script operation.

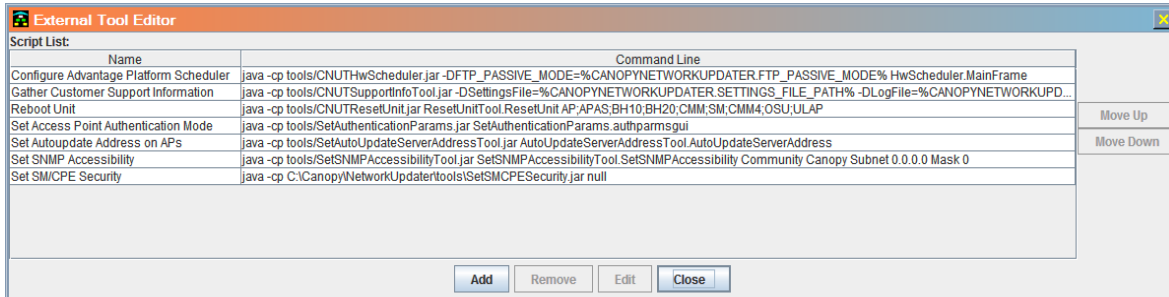
External Tools can either come from Cambium Networks or be custom built by the operator to meet specific needs. See [Building Custom External Tools](#) for details on building and linking in External Tools with the Network Updater.



August 2021

## Tools→Edit External Tool Menu

This operation can be used to edit the configuration settings for an External Tool, or to disassociate a tool from the Network Updater and removes it from the Tools menu. Editing of the External Tool configuration works in a similar manner to adding new External Tools.

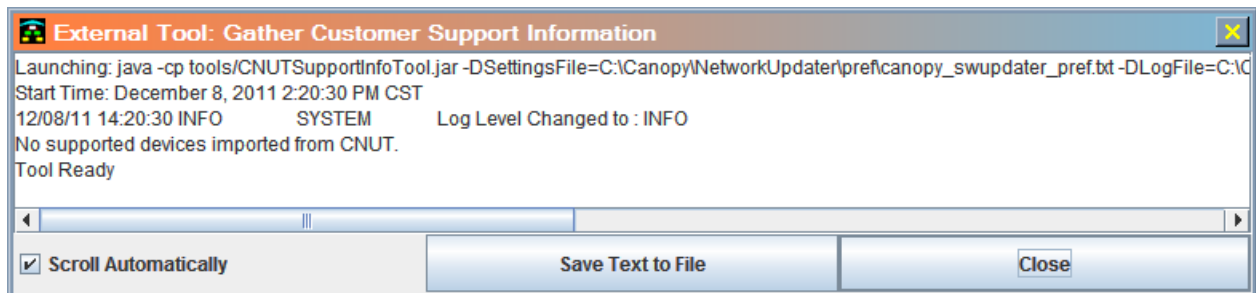


## Tools→Launch External Tool

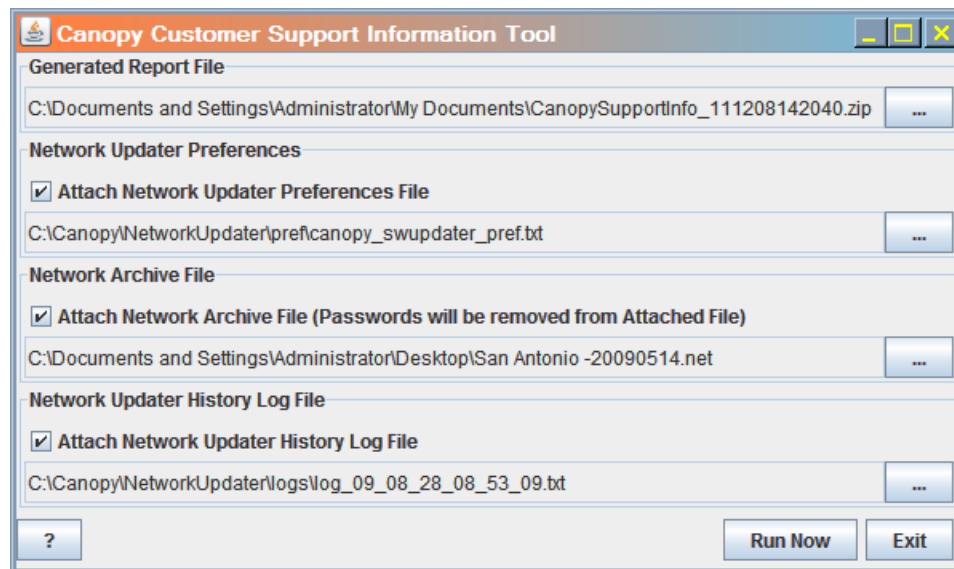
This operation allows the user to run a script one time without associating it with the Network Updater for future use. Since this is a onetime only operation, the user does not need to assign a name to the script. The user must input either the path and file name for the script that is to be executed, or the actual executable script text.

The user indicates if they want parameters passed to the script and if they want to operate on Selected Network Branches or Selected Network Elements in the same fashion as [Tools→Add External Tool to Menu](#).

The External Tool launcher will open a dialogue window to capture all output from the external tool.



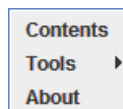
The user may choose to save the External Tools standard output messages into a file by selecting the **Save Text to File** button.



## Included Network Updater External Tools

See [External Tools Included](#) for details on pre-packaged External Tools that are automatically installed when Network Updater is installed.

### 5.3.6 Help Menu



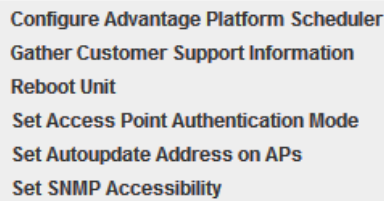
#### Help→Contents

Brings up the Network Updater help files

#### Help→Tools→*ToolName*

This operation shows the user a list of external scripts that support help. This option appears in the **Help** menu only if there are tools identified that support help.

August 2021



Configure Advantage Platform Scheduler  
Gather Customer Support Information  
Reboot Unit  
Set Access Point Authentication Mode  
Set Autoupdate Address on APs  
Set SNMP Accessibility

By selecting any of the script tools from the menu displayed, an external window will appear and the script will be initiated using the help options specified for the script when it was added to the tools menu. When the user is done viewing the script help, they may close the window within which the script was run.

## Help→About

Brings up version and Copyright information for the current installation of the Network Updater tool.

## 5.4 User Convenience Actions

### 5.4.1 Right click to manipulate selected element

The user may perform a right mouse click on the selected network element to access standard actions that can be performed on that single element. These actions include the following:

- Modify Network Element Access (see [Edit→Modify Selected Network Element Access](#))
- Add Network Element (see [Edit→Add Elements to Highlighted Element](#))
- Remove Network Element (see [Edit→Remove Selected Elements](#))
- Change Network Element Type (see [Edit→Change Network Element Type](#))
- Move Network Element (see [Edit→Move Selected Network Elements](#))
- Open Network Element Web Page (see [Edit→Open Highlighted Network Element Web Page](#))

### 5.4.2 Double click to modify element

If the user double clicks on a network element, the Modify Network Element Access window opens for the highlighted network element (see [Edit→Modify Selected Network Element Access](#)).

### 5.4.3 Select all Elements of a branch

The user may cause all the elements below an element group to be selected (or deselected) by checking (or un-checking) the box to the left of the Element Group on the tree display. When any



August 2021

element is currently selected, an asterisk (\*) appears in the title bar above the check box column. This can be helpful to aid users in knowing that some elements may be currently selected even if they are off the current visible portion of the window or in a different tree branch, such as the Discovered SMs.

## **5.4.4      Sorting Network Elements by Column Values**

The user can change the sort order that network elements are displayed by clicking on any of the column headers in the tool, such as Element, ESN, Last Access, etc. Clicking once on a column will cause the elements to be assorted in ascending order based on the values in that column. Clicking a second time on the same column will cause the elements to be resorted in descending order based on the values in that column.

Network elements will be sorted within their current groups. Sorting does not cause elements to change levels within the tree or to have their parent relationships changed.

## **5.4.5      Change Order of Columns Displayed**

The user can change the order of the columns of information displayed for the elements in the tree by dragging any column desired to the right or left of any other desired column.

## **5.4.6      Change Display Size of Column Displayed**

The user may change the screen size allocated to any specific column by dragging the right edge of the column title to make the column either larger or smaller as desired.

## **5.4.7      Last Settings on External Tools Remembered**

Network updater will automatically remember any changes to the command line execution or parameter inputs associated with an external tool when the user clicks on the tool on the Tools menu and choose to run it. In this way, users can essentially modify how scripts are run in their environment for both the current session and future sessions.

## **5.4.8      Mouse-Over Display of Tree Contents**

The user will see a small popup tips display of a cell's contents when the user's mouse rolls over a columns title or any table data in the network element tree. This can be useful when the contents being displayed are too big to be completely seen within the current column width settings.

## 6 Command Line Operations

### 6.1 Introduction

The Command Line Interface (CLI) of Network Updater enables executing firmware update tasks from the command line, using the same packages as the GUI interface. The CLI supports directly updating a device by IP address as well as SM autoupdate of PMP450 family devices.

### 6.2 Usage for Direct Update of device

The CLI is installed at `.../NetworkUpdater/cli`. There are 2 script files for invoking this cli:

- Linux: `updatedevice.sh`
- Windows: `updatedevice.bat`

The syntax of the CLI command line is as follows:

```
updatedevice -ipaddress:IPAddress[:https] -user:user> -password:password
-snmppcommunity:snmppcommunity[:SNMPv3 options] -package:packagepath
[-autoupdateip:autoupdateip] [-channelbandwidth:current:target]
[-forceswitchbandwidth:true/false]
```

where the following rules apply:

Parameter	Description	Default
<code>-ipaddress</code>	Target IP Address or Host name of device to update.	required
<code>[:https]</code>	Add <code>:https</code> only if you want HTTPS to be used instead of HTTP.	optional
<code>-user</code>	Telnet/FTP, HTTP, or TFTP login ID of the device to update.	required
<code>-password</code>	Telnet/FTP, HTTP, or TFTP password of the device to update.	required
<code>-snmppcommunity</code>	SNMP community string of the device to update.	required
<code>[:SNMPv3 options]</code>	Where added, use the following syntax (with no line break): : <code>v3[:auth_nopriv auth_priv:MD5 SHA:authpassphrase</code> : <code>DES AES:privpassphrase]</code>	optional
<code>-package</code>	Path to the package file for updating.	required
<code>-autoupdateip</code>	Autoupdate IP Address to set for Access Points. If null, this is automatically detected.	Auto

August 2021

<b>-channelbandwidth<sup>1</sup></b>	Valid current and target bandwidth values for the HPAP are 5.0, 10.0, and 20.0.	10.0
<b>-forceswitchbandwidth</b>	Quits the switch bandwidth operation by default if at least one SM is registered in the HPAP.	false
<b>NOTES:</b> 9. For information on the proper use of this argument, see <a href="#">HPAP Channel Bandwidth Tab</a> . Improper use of this argument can result in the SMs being dropped and unable to reconnect to their HPAP.		

The exit codes are

- 0: Success
- 1: Error with Arguments
- 2: Error during update

Example:

```
updatedevice.bat -ipaddress:10.40.11.10 -user:root -password:root
-snmppcommunity:Canopy -package:D:/Temp/CANOPY120BUILD9_AES.pkg3
-autoupdateip 10.40.0.254
```

## 6.3 Usage for SM Autoupdate of PMP450 devices

The CLI is installed at .../NetworkUpdater/cli. There are 2 script files for invoking the cli:

- Linux: **deviceAutoUpdate.sh**
- Windows: **deviceAutoUpdate.bat**

The syntax of the CLI command line is as follows:

```
deviceAutoUpdate -ipaddress:<APDeviceIP> -user:<user> -password:<pwd> -
snmpcommunity:<snmpCommunityString> -package:<package> -
enableautoupdate:true -fileservertype:AP -smttype:PMP450SM(P11):PMP430SM(P11)
```

where the following rules apply:

Parameter	Description	Default
<b>-ipaddress</b>	Target IP Address or Host name of AP device to update.	required
<b>[ :https ]</b>	Add :https only if you want HTTPS to be used instead of HTTP.	optional
<b>-user</b>	Telnet/FTP, HTTP, or TFTP login ID of the AP device to update.	required

August 2021

Parameter	Description	Default
<b>-password</b>	Telnet/FTP, HTTP, or TFTP password of the AP device to update.	required
<b>-snmpcommunity</b>	SNMP community string of the device to update.	required
<b>-package</b>	Path to the package file for updating.	required
<b>- enableautoupdate</b>	Boolean value that determines if the auto update is enabled or not on the AP	required

<b>- fileservertype</b>	Determines the file server type for the auto update. Valid values are: 1. AP 2. HTTP:<IP Address of the server where HTTP is started>	required
<b>-smttype</b>	Determines the SM that needs to be upgraded separated by colon. Valid values are: "PMP430SM(P11)", "PMP450SM(P11)", "PMP450bSM(P15)", "PMP450iSM(P13)", "PMP100SM(P7/P8/P9)", "PMP100SM(P10)", "PMP100SM(P11)"	required

The exit codes are

- 0: Success
- 1: Error with Arguments
- 2: Error during update

Example:

```
deviceAutoUpdate -ipaddress:10.40.11.10 -user:eng -password:eng -
snmpcommunity:Canopy -package:D:/Temp/CANOPY120BUILD9_AES.pkg3 -
enableautoupdate:true -fileservertype:AP -smttype:PMP450SM(P11):PMP430SM(P11)
```

OR

```
deviceAutoUpdate -ipaddress:10.40.11.10 -user:eng -password:eng -
snmpcommunity:Canopy -package:D:/Temp/CANOPY120BUILD9_AES.pkg3 -
enableautoupdate:true -fileservertype:HTTP:10.120.143.182 -
smttype:PMP450SM(P11):PMP430SM(P11)
```

August 2021



## Network Updater On-Line Help

### Issue 1

August 2021

#### Output:

```
C:\Cambium\NetworkUpdater\cli>deviceAutoUpdate -ipaddress:10.120.247.1 -user:admin -password:admin -snmpcommunity:Canopy -package:C:\\Users\\sgi010\\Desktop\\packages\\CANOPY151_5BUILDOFFICIAL_PXP45x_S.pkg3 -enableautoupdate:true -fileservertype:AP -smttype:PMP450SM(P11):PMP450iSM(P13):PMP450bSM(P15)
08/02/18 06:53:14 INFO          SYSTEM  Log Level Changed to : INFO
08/02/18 06:53:14 INFO          SYSTEM  Accessing Device- 10.120.247.1
08/02/18 06:53:14 INFO          SYSTEM  SNMP Session Manager pool size = 10
08/02/18 06:53:14 INFO          SYSTEM  SNMP session Listening on 10.120.143.182
/0
08/02/18 06:53:14 INFO          SYSTEM  Device Info- MAC: 0A003EBB012D; TYPE: PMP 450i AP-DES; CURRENT: CANOPY 15.1.5 AP-None
08/02/18 06:53:14 INFO          SYSTEM  Loading Package- C:\\Users\\sgi010\\Desktop\\packages\\CANOPY151_5BUILDOFFICIAL_PXP45x_S.pkg3
08/02/18 06:53:27 INFO          SYSTEM  Host: 10.120.247.1;ESN: 0A003EBB012D;Message: Detect registered slave device link
08/02/18 06:53:27 INFO          SYSTEM  Host: 10.120.247.1;ESN: 0A003EBB012D;Message: Transferring Files upgrade.img to host:10.120.247.1 by http
08/02/18 06:53:47 INFO          SYSTEM  Host: 10.120.247.1;ESN: 0A003EBB012D;Message: Programming ...
08/02/18 06:54:07 INFO          SYSTEM  Host: 10.120.247.1;ESN: 0A003EBB012D;Message: Update completed, reboot device...
08/02/18 06:54:07 INFO          SYSTEM  Session with ID=1 already in pool
Retrying to connect 10.120.247.1 ...
Retrying to connect 10.120.247.1 ...
Retrying to connect 10.120.247.1 ...
Retrying to connect 10.120.247.1 ...
Retrying to connect 10.120.247.1 ...
Retrying to connect 10.120.247.1 ...
Retrying to connect 10.120.247.1 ...
Retrying to connect 10.120.247.1 ...
Retrying to connect 10.120.247.1 ...
Retrying to connect 10.120.247.1 ...
08/02/18 06:56:21 INFO          SYSTEM  Host: 10.120.247.1;ESN: 0A003EBB012D;Message: Verify update.
08/02/18 06:56:26 INFO          SYSTEM  Host: 10.120.247.1;ESN: 0A003EBB012D;Message: Waiting max 600 secs to re-register ..
08/02/18 06:57:06 INFO          SYSTEM  Host: 10.120.247.1;ESN: 0A003EBB012D;Message: Completed Success
08/02/18 06:57:06 INFO          SYSTEM  Host: 10.120.247.1;ESN: 0A003EBB012D;Message: Disabling Auto-Update
08/02/18 06:57:06 INFO          SYSTEM  Host: 10.120.247.1;ESN: 0A003EBB012D;Message: Auto-Update Disabled.
08/02/18 06:57:07 INFO          SYSTEM  Host: 10.120.247.1;ESN: 0A003EBB012D;Message: Transferring Files actionList.acl;5x_cat120.img;upgrade.img;upgrade-p15.img; to host:10.120.247.1 by http
08/02/18 06:57:54 INFO          SYSTEM  Host: 10.120.247.1;ESN: 0A003EBB012D;Message: Enabling Auto Update...
08/02/18 06:57:55 INFO          SYSTEM  Host: 10.120.247.1;ESN: 0A003EBB012D;Message: Auto-Update Enabled
08/02/18 06:58:02 INFO          SYSTEM  Host: AP:[10.120.247.1]LUID:[2];ESN: 0A03E703881;Message: Auto-Update Started(status:120).
08/02/18 06:58:02 INFO          SYSTEM  Host: AP:[10.120.247.1]LUID:[3];ESN: 0A03EBB0117;Message: Update Not Applicable.
08/02/18 06:58:02 INFO          SYSTEM  Host: AP:[10.120.247.1]LUID:[4];ESN: 0A03EA000BC;Message: Update Not Applicable.
```

## Network Updater On-Line Help

### Issue 1

August 2021

```
08/02/18 06:58:02 INFO      SYSTEM  Host: AP:[10.120.247.1]LUID:[5];ESN: 0A0
03EB0028B;Message: Auto-Update Started(status:120).
08/02/18 06:59:57 INFO      SYSTEM  Host: AP:[10.120.247.1]LUID:[2];ESN: 0A0
03E703881;Message: Auto-Update In Progress(status:132).
08/02/18 07:03:27 INFO      SYSTEM  Host: AP:[10.120.247.1]LUID:[2];ESN: 0A0
03E703881;Message: Auto-Update Completed.
08/02/18 07:03:57 WARN      SYSTEM  Host: AP:[10.120.247.1]LUID:[5];ESN: 0A0
03EB0028B;Message: Invalid image(s) selected Or Failed to set max file size(stat
us:256).
Disabled autoupdate on device
Device upgrade monitoring is completed
```

August 2021

## 7 Building Custom External Tools

Operators can create their own External Tools to be used with the Network Updater tool. The following information provides details about parameters passed to External Tools, Network Updater configuration information available to External Tools, and how external tools can provide information back to the Network Updater for automated linking into the External Tools interface.

### 7.1 Parameters Passed to External Tools

Assuming the **Send Network Element Information** box is checked in the Launch External Tool dialog, the following information is passed to the script for each network element encountered (depending on if Selected Network Branches or Selected Network Element option is specified). These parameters are passed as a semi-colon delimited list in the order shown here.

#### Host Address

This is the element IP address or hostname in the case of a local hosts file or DNS lookup.

#### ESN (Element Serial Number)

This is the value entered by the user for undiscovered elements, so therefore either host name or IP address.

For auto-discovered SMs, this is a string identifying the AP that the SM is attached to, and the LUID the SM is currently accessed through on the AP. This string will have the format of:

**AP:** [*Host\_Name\_or\_IP*] .LUID: [#]

Where *Host\_Name\_or\_IP* is the host name or IP address as specified by the user when they entered the AP information into Network Updater, and *#* is the LUID number assigned to the SM by the AP.

This parameter cannot be blank.

#### MAC Address

This is the 12-digit hexadecimal string representing the MAC address of the network element. This is passed without any hyphens. This parameter can be blank.

August 2021

## Element Type

This is a character string representing the type of network element being identified. Valid values include:

Element Type	String
10 Mbps Backhaul	<b>BH</b>
20 Mbps Backhaul	<b>BH20</b>
30 Mbps or 60 Mbps High Speed Backhaul	<b>HSBH 30/60</b>
150 Mbps or 300 Mbps High Speed Backhaul	<b>HSBH 150/300</b>
Access Point	<b>AP</b>
Access Point with Authentication Security enabled	<b>APAS</b>
Subscriber Module	<b>SM</b>
Cluster Management Module micro	<b>CMM</b>
Cluster Management Module-4	<b>CMM4</b>

This parameter cannot be blank.

## Encryption Type

This is a character string representing the type of encryption being used by the network element. Valid values include:

Encryption Type	String
DES encryption is currently enabled	<b>DES</b>
AES encryption is currently enabled	<b>AES</b>
Indicates encryption is possible, but currently disabled	<b>None</b>
Used for CMMs	null

## SNMP Community String

The SNMP community string for the specific element. This value can be blank, indicating the community string is not known and/or not specified.

August 2021

### **Device Login ID/Password**

The read/write account parameters for the specified element. These parameters can be blank, meaning there is either no password or the password is not known. This password should be the one associated with the **root** account.

### **Software Version String**

String with the software version currently loaded on the element. This parameter can be blank, indicating the software version is not known.

### **Software Boot String**

String with the Software Boot version currently loaded on the element. This parameter can be blank, indicating the software boot version is not known, or does not apply (as in the case of CMMs).

### **FPGA Version String**

String with the FPGA version currently loaded on the element. This parameter can be blank, indicating the FPGA version is not known, or does not apply (as in the case of CMMs).

### **Site Name**

This is the text string from the network elements Site Name field. This is passed as a quoted string.

### **Site Contact**

This is the text string from the network elements Site Contact field. This is passed as a quoted string

### **Site Location**

This is the text string from the network elements Site Location field. This is passed as a quoted string

### **Detected Parent**

This is the content of the Detected Parent column for the element. This will be blank for all elements except auto-discovered SMs.

### **Detected Parent Password**

This is the password for the Detected Parent. This is passed in case the External Tool needs to access the element through its parent (proxy), and therefore needs parent access.

The parameters are passed in the above order, separated by a semi-colon. The following are example full strings of input parameters to a script:

August 2021

```
169.254.1.4;0A003E000CEA;BH;DES;Canopy;secure;CANOPY4.1.3 Jan 22 2004
10:38:11;CANOPYBOOT 2.3;06240307;"Main BH";"John Smith";"Schaumburg";

169.254.1.10;0A003EE00026;CMM;;Canopy;secure;CANOPY CMM 2.0.10 Mar 18 2004
15:36:49;;5;"Main Cluster";"Administrator";"Main POP";

AP: [169.254.1.1].LUID: [2];0A003E000B31;SM;DES;Canopy;secure;CANOPY4.1.3 Jan 22
2004 10:38:11;CANOPYBOOT 2.3;06240307;"123 Main Street";"Jane
Customer";"Schaumburg";AP: [169.254.1.1].LUID: [2];secure
```

## 7.2 External Tool Help

Optionally, the script may also support a help capability. If the script supports this option, the user should indicate this by checking the **Supports Help** checkbox on the Add External Tool to Menu

window, and the calling sequence to initiate the help for the script must be supplied (including the script name and any parameters required). The help script should perform no actual operations other than displaying the help information. Using this technique, it is possible for the script help to be accessed either by a parameter option into the core script, or by accessing a separate script or help tool that can provide information for the script. See [Help→Tools→ToolName](#) for information on the user accessing the help capabilities of a specific external tool.

## 7.3 External Tool Extended Attributes

It is also possible to have the External Tool itself provide the information about its appropriate name, commands for launching the tool, commands for accessing its help, and identifying if it works with branches of elements or elements directly. This is supported for both Java-based (files ending with .jar) and Perl-based (files ending with .pl) External Tools. For java based external tools this is done through the Extended Manifest Attributes in the JAR file. For Perl tools, lines within the Perl script itself beginning with #@ are used to identify these extended attributes values. If these extended attributes are provided by the external tool, the Network Updater will automatically extract these from the External Tool and load them into the **Add External Tool** dialogue box when the External Tool main file is selected. The following are the details on these extended attributes.

### 7.3.1 Java Extended Manifest Attributes

- **Tool-Name**  
This value will automatically be loaded into the name of the tool field
- **Main-Class**  
Is the class file name to start the tool and parameter to be passed to the tool
- **Help-Class**  
Is the class file name and parameters to be passed to the tool to launch help
- **Send-Elements-Info**  
Should be **Branches** to send element info on selected branches, or **Elements** to send element info only on selected elements.

August 2021

**note** ..... do not include quotes for branches and element values.

Example from the **Configure Advantage Platform Scheduler** external tool included with Network Updater (see [Configure Advantage Platform Scheduler](#)):

```
Manifest-Version: 1.0
Tool-Name: Advantage Platform Scheduler Configuration
Main-Class: src.MainFrame
Send-Element-Info: Elements
Help-Class: src.MainFrame -help
```

The Resulting Command Line from the above Main-Class attribute will be

```
java -cp jarfile.jar src.MainFrame
```

The Resulting Help Command from the above Help-Class line will be

```
java -cp jarfile.jar src.MainFrame -help
```

The External Tool will by default send network element Information for selected elements.

## Acronyms and Abbreviations

<b>AES</b>	Advanced Encryption Standard: Encryption used by some radios; uses a 128-bit encryption key.
<b>AP</b>	Access Point: Infrastructure radio for a point-to-multi-point system.
<b>APAS</b>	Access Point with Authentication Services: An AP that is licensed and enabled to communicate with a BAM server.
<b>BAM</b>	Bandwidth and Authentication Manager: Server software used to manage network element access and bandwidth allocations in a network.
<b>BH</b>	Backhaul: Point-to-Point radios.
<b>CMM</b>	Cluster Management Module: Centralized power, synch, switching for infrastructure deployment. CMM acronym alone may mean all classes of CMMs, or it may refer to the CMMmicro specifically. CMM-4 is used to refer to only the CMM-4 unit.
<b>CNUT</b>	Network Updater Tool.
<b>CPE</b>	Customer Premise Equipment: Equipment deployed at customer location.
<b>DES</b>	Data Encryption Standard: Encryption used by standard radios; uses a 56-bit encryption key.
<b>ESN</b>	Element Serial Number: Unique identifier to access a network element. Can take the form of an IP address, MAC address, or LUID and AP combination.
<b>FPGA</b>	Field Programmable Gate Array: Programmable hardware portion of Module.

August 2021

<b>GUI</b>	Graphical User Interface.
<b>HSBH</b>	High-speed Backhaul: OFDM based Point-to-Point radios.
<b>IP</b>	Internet Protocol: Addressing and routing scheme used on the Internet.
<b>LUID</b>	Logical Unit ID: Used by AP to reference registered SMs.
<b>MAC</b>	Media Access Control: Unique 12-digit hexadecimal value assigned to a networkable device by the manufacturer.
<b>MDU</b>	Multi Dwelling Unit (apartments, condos, etc).
<b>OS</b>	Operating System.
<b>OSU</b>	Outdoor Subscriber Unit – SM portion of the 3.5GHz based OFDM point to multipoint product.
<b>POP</b>	Point of Presence.
<b>SM</b>	Subscriber Module: CPE module for a point to multi-point system.
<b>SNMP</b>	Simple Network Management Protocol.
<b>TFTP</b>	Trivial File Transfer Protocol: Protocol used by SMs pulling upgrade files for a network file server.
<b>UDP</b>	User Datagram Protocol: A messaging protocol used for some command traffic within a network.
<b>ULAP</b>	Ultra-Light Access Point – AP portion of the 3.5GHz based OFDM point to multipoint product.



# Legal Notices and License Agreement

## **CAMBIUM NETWORKS, LTD** **END USER LICENSE AGREEMENT**

CAMBIUM NETWORKS, LTD (“Cambium”) is willing to license its CNUT™ Network Updater Tool software and the accompanying documentation (collectively, the “Software,” as further defined below) to you only on the condition that you accept all the terms in this End User License Agreement (this “Agreement”).

**IMPORTANT: READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THE SOFTWARE AND ANY EQUIPMENT AND/OR PRODUCTS THAT ACCOMPANY THE SOFTWARE.**

**BY CLICKING ON THE “ACCEPT” BUTTON DURING INSTALLATION, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT.**

**IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, CAMBIUM IS NOT WILLING TO LICENSE THE SOFTWARE TO YOU AND YOU SHOULD CLICK ON THE “DO NOT ACCEPT” BUTTON TO DISCONTINUE THE INSTALLATION PROCESS. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, YOU MAY, FOR A FULL REFUND: (I) RETURN THE SOFTWARE TO THE ENTITY FROM WHOM YOU PURCHASED IT; OR, (II) FOR DOWNLOADED SOFTWARE, PROVIDE TO THE ENTITY FROM WHOM YOU PURCHASED THE SOFTWARE YOUR WRITTEN VERIFICATION OF DELETION OF ALL COPIES OF THE SOFTWARE.**

**1. Definitions.** In this Agreement, the word “Software” refers to the set of instructions for computing devices, in executable form and in any media (which may include diskette(s), CD-ROM(s), downloadable Internet file(s), hardware, firmware, etc.), and includes without limitation interfaces, content, fonts, images, photographs, animations, video, audio, music text, “applets” and included data, as well as the accompanying documentation, such as manuals and instructional aids, whether in printed or electronic form, for the software product identified above.

August 2021

2. **General.** The Software is licensed, and not sold, to you by Cambium for use only under the terms of this Agreement. Cambium and/or Cambium's licensor(s) retain all right, title and interest in and to the Software, and the copyrights and other intellectual property rights therein and thereto, and reserve all rights not expressly granted to you in this Agreement. The terms of this Agreement will govern any update(s) and/or upgrade(s) to the Software provided by Cambium that replace and/or supplement the original Software, unless such update(s) and/or upgrade(s) are accompanied by a separate license in which case the terms of that license will govern.

3. **Grant of License.** Cambium grants you ("Licensee" or "you") a limited, personal, nonexclusive and non-transferable (except as otherwise provided herein) license to use the Software subject to the Conditions of Use set forth in Section 4 and the remaining terms and conditions of this Agreement. Any terms or conditions appearing on the face or reverse side of any purchase order, purchase order acknowledgment or other order document that are different from, or in addition to, the terms of this Agreement will not be binding on the parties, even if payment is accepted.

4. **Conditions of Use; Restrictions on Use.** The Software is protected by international intellectual property laws and treaties, and other applicable laws. Any use of the Software in violation of the terms and conditions set forth in this Agreement is strictly prohibited and will be deemed a breach of this Agreement. In addition to the other terms and conditions of this Agreement, you agree to the following specific conditions and restrictions:

4.1. You will use the Software in compliance with all applicable laws, including local laws of the country or region in which you reside or in which you use the Software.

4.2. Only you, your employees or agents may use the Software. You will take all necessary steps to ensure that your employees and agents abide by the terms of this Agreement.

4.3. You will use the Software: (i) only for your internal business purposes; (ii) only as described in the Software; and, (iii) in strict accordance with this Agreement.

4.4. You will install and use the Software on a single computing device.

4.5. To the extent the Software includes features involving maps, you will take all reasonable efforts not exceed 20,000 map page views per year. Cambium reserves the right to disable the usage of features involving maps if your annual usage of map page views exceeds 20,000 map page views.

4.6. You will not, and you will not enable others to, copy (except for back-up purposes as expressly permitted by this Agreement), decompile, bootleg, reverse engineer, disassemble, attempt to derive the source code of, decrypt, modify, translate, or create derivative works from the Software, or any part thereof (except as, and only to the extent, any foregoing restriction is prohibited by applicable law). Any attempt to do so is a violation of the rights of Cambium and/or its licensor(s) in the Software.

4.7. You will not attempt to defeat any copy protection device included with the Software.

4.8. If the Software is provided on multiple types of media, you will use only the media that best meets your specific needs, and you will not loan, rent, lease or transfer the other media contained in the package without Cambium's written consent.

4.9. You will not remove any proprietary notices, marks, labels, or logos from the Software.

4.10. Unless otherwise provided herein, you will not rent, lease, sublicense or transfer the Software, or any part thereof, to any other party without Cambium's prior written consent.

4.11. You will not use the Software on any virtual computing device.

4.12. You will not use the Software for any purposes prohibited by applicable law, including without limitation the development, design, manufacture or production of nuclear, missiles, or chemical or biological weapons.

USE OF THE SOFTWARE IN ANY MANNER OTHER THAN AS PROVIDED HEREIN IS STRICTLY PROHIBITED AND MAY INFRINGE ON THE INTELLECTUAL PROPERTY RIGHTS OF CAMBIUM AND/OR ITS LICENSOR(S),

August 2021

SUBJECTING YOU TO CIVIL AND CRIMINAL PENALTIES, INCLUDING WITHOUT LIMITATION MONETARY DAMAGES AND IMPRISONMENT FOR COPYRIGHT INFRINGEMENT.

5. **Back-Ups.** Notwithstanding anything to the contrary in this Agreement, you may make one (1) copy of the Software in machine-readable form for back-up purposes only. If the documentation for the Software is in printed form, it may not be copied. With regard to all copies of the Software permitted herein, you agree to reproduce on such copies all Cambium copyright notices, and other proprietary notices appearing on and in the original Software.

6. **Export.** You may not export, re-export or transfer, directly or indirectly, the Software except as authorized by United States law or by the laws of the jurisdiction(s) in which the Software was obtained. By way of example, but without limitation of the foregoing, if your Software was obtained in the United States, the Software may not be exported, re-exported or transferred: (a) into any U.S. embargoed countries; or, (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce Denied Person's List or Entity List. By using the Software, you represent and warrant that you are not located in any such country or on any such list.

7. **Confidentiality.** You acknowledge that the Software contains valuable proprietary information and trade secrets and that unauthorized or improper use of the Software will result in irreparable harm to Cambium for which monetary damages would be inadequate and for which Cambium will be entitled to immediate injunctive relief. Accordingly, you will limit access to the Software to those of your employees and agents who need to use the Software for your internal business purposes, and you will take appropriate action with those employees and agents to preserve the confidentiality of the Software, using the same degree of care to avoid unauthorized or improper disclosure as you use for the protection of your own proprietary software, but in no event less than reasonable care. You have no obligation to preserve the confidentiality of any information that: (i) was in the public domain at the time of disclosure; (ii) entered the public domain through no fault of yours; (iii) was given to you free of any obligation to keep it confidential; (iv) is independently developed by you; or, (v) is disclosed as required by law provided that you notify Cambium prior to such disclosure and provide Cambium with a reasonable opportunity to respond.

8. **Right to Use Cambium's Name.** Except as required in Section 5 above, you will not, during the term of this Agreement or thereafter, use any trademark of Cambium, or any word and/or symbol likely to be confused with any Cambium trademark, either alone or in any combination with other words and/or symbols.

9. **Transfer.** In the case of Software designed to operate on Cambium equipment, you may not transfer the Software to another party except: (i) if you are an end-user, when you are transferring the Software together with the Cambium equipment on which it operates; or, (ii) if you are a Cambium authorized distributor, when you are transferring the Software either together with such Cambium equipment or are transferring the Software as a licensed duly paid-for upgrade, update, patch, new release, enhancement or replacement of a prior version of the Software. If you are a Cambium authorized distributor, when you are transferring the Software as permitted in this Agreement, you agree to transfer the Software with a license agreement having terms and conditions no less restrictive than those contained in this Agreement. All transfers of the Software under this Section 9 are strictly subject to the conditions precedent that: (iii) the other party agrees to accept the terms and conditions of this Agreement; and, (ii) you destroy any copy of the Software you do not transfer to that party. Unless otherwise provided herein, the Software may not be transferred, and this Agreement may not be assigned, by you without Cambium's prior written consent.

10. **Upgrades and Updates.** If the Software is licensed to you as an upgrade or update to software previously licensed to you, you must destroy the software previously licensed to you, including any copies, within 30 days of your receipt of the Software.

11. **Maintenance and Support.** Cambium is not responsible for maintenance or support of the Software, or the equipment on which the Software resides or is used, under this Agreement. By accepting the license granted under this Agreement, you agree that Cambium will be under no obligation to provide any support, maintenance or

August 2021

service in connection with the Software or such equipment. Maintenance and support of the Software and/or such equipment by Cambium may be available under the terms of a separate agreement.

**12. Limited Warranty.** All physical media, such as diskettes or CD-ROMS, on which the Software is furnished by Cambium (the "Media") are warranted to be free from manufacturing and material defects for ninety (90) days after the shipment date of the Media to you. Media that becomes defective during such period will be repaired or, at Cambium's option, replaced. This limited warranty is contingent upon proper use of the Media and does not cover Media that has been tampered with, modified or subjected to unusual physical or electrical stress.

Tampering with or removing any factory seal or label on any Media voids this warranty and releases Cambium from any and all liability. The entire liability of Cambium, and your exclusive remedy under the warranty provided in this Section 12 will be, at Cambium's option, to repair or replace any Media found to be defective within the warranty period, or to refund the purchase price and terminate this Agreement. To seek such a remedy, you must return the Software to Cambium, with a copy of the original purchase receipt, within the warranty period.

**13. Disclaimer.** EXCEPT FOR THE ABOVE EXPRESS LIMITED WARRANTY FOR THE MEDIA, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE SOFTWARE IS PROVIDED "AS IS" AND "AS AVAILABLE", WITHOUT WARRANTY OF ANY KIND, AND CAMBIUM ON BEHALF OF ITSELF AND ITS LICENSOR(S) HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE SOFTWARE, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, OF SATISFACTORY QUALITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF ACCURACY, OF QUIET ENJOYMENT, AND OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS. CAMBIUM ALSO DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN, PERFORMED AND/OR PROVIDED BY THE SOFTWARE WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE, THAT THE SOFTWARE WILL BE COMPATIBLE OR WORK WITH ANY THIRD-PARTY SOFTWARE, APPLICATIONS OR DEVICES, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. CAMBIUM MAKES NO WARRANTY WITH RESPECT TO THE CORRECTNESS, ACCURACY, OR RELIABILITY OF THE SOFTWARE, AND YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT, TO THE EXTENT PERMITTED BY APPLICABLE LAW, YOUR USE OF THE SOFTWARE IS AT YOUR SOLE RISK AND THAT THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH YOU. YOU FURTHER ACKNOWLEDGE AND AGREE THAT THE SOFTWARE IS NOT INTENDED OR SUITABLE FOR USE IN SITUATIONS OR ENVIRONMENTS WHERE THE FAILURE OR TIME DELAYS OF, OR ERRORS OR INACCURACIES IN THE CONTENT, DATA OR INFORMATION PROVIDED BY THE SOFTWARE COULD LEAD TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL

OR ENVIRONMENTAL DAMAGE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY CAMBIUM OR AN AUTHORIZED CAMBIUM REPRESENTATIVE SHALL CREATE A WARRANTY.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES OR LIMITATIONS ON APPLICABLE STATUTORY RIGHTS OF A CONSUMER, SO THE ABOVE EXCLUSION AND LIMITATIONS MAY NOT APPLY TO YOU.

**14. Limitation of Liability.** THE TOTAL LIABILITY OF CAMBIUM FOR ANY DAMAGES UNDER THIS AGREEMENT WILL NOT EXCEED THE TOTAL AMOUNT PAID BY YOU FOR THE SOFTWARE LICENSED UNDER THIS AGREEMENT. TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, IN NO EVENT SHALL CAMBIUM BE LIABLE FOR PERSONAL INJURY, OR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR USE OR INABILITY TO USE THE SOFTWARE, OR ANY THIRD PARTY SOFTWARE, APPLICATIONS AND/OR DEVICES IN CONJUNCTION WITH THE SOFTWARE, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF CAMBIUM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF LIABILITY FOR PERSONAL INJURY, OR OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU.

**15. U.S. Government End Users.** The Software is a "Commercial Item," as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48

August 2021

C.F.R. §227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users: (i) only as Commercial Items; and, (ii) with only those rights as are granted to all other end users pursuant to the terms and conditions herein, notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which this Agreement may be incorporated or which Cambium may provide to Government end user. Use of the Software constitutes agreement by the U.S. Government that the Software is Commercial Computer Software and Commercial Computer Software Documentation, and constitutes acceptance of the rights and restrictions herein. Unpublished rights ARE reserved under the copyright laws of the United States. The name and address of the contractor for United States Government end users is: Cambium Networks, Ltd, a company registered in England and Wales under company number 07752773, with an address at 1299 E. Algonquin Road, Schaumburg, IL 60196.

**16. Term and Termination.** This Agreement, and your right to use the Software, will begin when you click the “ACCEPT” button, which constitutes acceptance of the terms and conditions in this Agreement, and will continue in perpetuity unless terminated as follows. This Agreement will terminate immediately and automatically without notice upon a breach of this Agreement by you. You may also terminate this agreement by ceasing use of the Software. Upon the termination of this Agreement for any reason, you must cease all use of the Software and destroy all copies of the Software in your possession or control.

**17. Governing Law and Severability.** This Agreement is governed by the laws of the United States of America, to the extent that they apply, and otherwise by the laws of the State of Illinois, excluding its conflicts of laws principles. This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. If for any reason a court of competent jurisdiction finds any provision of this Agreement, or portion thereof, to be unenforceable, the remainder of this Agreement shall continue in full force and effect.

**18. Survival.** The parties agree that where the context of any provision indicates an intent that it survives the term of this Agreement, then it will survive.

**19. Entire Agreement.** This Agreement constitutes the entire agreement between you and Cambium relating to the Software licensed hereunder and supersedes all prior or contemporaneous understandings regarding such subject matter. No amendment to or modification of this Agreement will be binding unless in writing and signed by Cambium, except that Cambium may modify and/or translate this Agreement as necessary to comply with applicable laws. In the event of a dispute between the English version and any non-English versions, the English version of this Agreement shall govern, to the extent not prohibited by the local law in your jurisdiction.

**20. Third-Party Software.** The Software may contain one or more items of third-party software supplied by third-party suppliers (collectively, “Third-Party Software”). The terms of this Agreement govern your use of any Third-Party Software UNLESS A SEPARATE THIRD-PARTY SOFTWARE LICENSE IS INCLUDED, IN WHICH CASE YOUR USE OF THE THIRD-PARTY SOFTWARE WILL THEN BE GOVERNED BY THE SEPARATE THIRD-PARTY LICENSE. By using the Software, you are agreeing be bound by the terms of use for all Third-Party Software.

**IF THE FOREGOING TERMS AND CONDITIONS ARE ACCEPTABLE TO YOU, PLEASE INDICATE YOUR AGREEMENT AND ACCEPTANCE BY CLICKING ON THE BUTTON LABELED “ACCEPT.” IF THE FOREGOING TERMS AND CONDITIONS ARE NOT ACCEPTABLE TO YOU, PLEASE CLICK ON THE “DO NOT ACCEPT” BUTTON.**

CNUT™, CAMBIUM™, CAMBIUM NETWORKS™ and the Cambium Networks Logo are trademarks of Cambium Networks, Ltd.

© Copyright 2018 Cambium Networks, Ltd All rights reserved.

# Troubleshooting

## **Autoupdate source address is not set on APs**

All Access Points have a parameter on their web pages for setting the Autoupdate Application Address. If this parameter is not set, Network Updater will be unable to configure the Access Point for performing SM Autoupdate.

- By default, Network Updater will set this value when it updates an Access Point.
- An External Tool is also provided for performing this operation. Once this operation is completed, it is necessary to reboot the AP. An External Tool for rebooting radios remotely is also provided. See [Included Network Updater External Tools](#) for more details on these tools.

## **An error is thrown when I try to enable SM Autoupdate on an AP**

There are four reasons an SM Autoupdate enable command might fail, resulting in an error message on a specific AP:

- The AP being enabled is not currently on the network (turned off)

August 2021

- The AP being enabled cannot be accessed by the Network Updater computer. In this situation you may have a network configuration issue. See [Network Communications](#) for more information on required communication protocols and ports.
- The AP being enabled does not have its Autoupdate IP address set to the IP address of the Network Updater server. See [Autoupdate source address is not set on APs](#) for information on addressing this problem.
- The AP being enabled does not support SM Autoupdate. This is the case in PMP 320 sectors.

### **Update of network elements works, but SM Autoupdate never activates on APs**

Network Updater makes use of an UDP command to enable SM Autoupdate on the APs in the network. It is necessary to ensure that the appropriate port is open between the Network Updater computer and the Network Elements to allow the UDP command to be passed to the network elements. See [Network Communications](#) for more information on required communication protocols and ports.

### **Network Updater server IP address changed, and SM Autoupdate no longer works**

The Network Updater tool will automatically configure the AP with the correct Autoupdate Source Address to ensure that it can enable and disable SM Autoupdate on the AP as needed. This configuration of the AP is generally done at the time when the AP is itself upgraded. By setting this value in conjunction with upgrading the AP, the Network Updater prevents having to reboot the AP an extra time just to set the Autoupdate Source Address.

If the IP address of the Network Updater computer changes after the APs have been upgraded, and the user attempts to directly enable SM Autoupdate on some of the APs on their network, it is likely that the operation will fail. This is because the APs still have the old IP address for the Network Updater computer in their Autoupdate Source Address. To fix this issue the user can use the

**Tools\*Set Autoupdate Address on AP** the external tool included with the Network Updater (see [Set](#)

[Set Autoupdate Address on APs](#)). Also see [Autoupdate source address is not set on APs](#) for additional information on this issue.

### **SM Autoupdate with external TFTP server is not working**

- Ensure SM can ping the TFTP server (Routing issue)
- Check the TFTP Root Folder (Ensure Packages are there)
- Use the **Test TFTP Server** button.
- Check for a Firewall software (TFTP Port may be protected on the server. Be sure two way communication is enabled). See [Network Communications](#) for more information on required communication protocols and ports.

August 2021

### **AP telnet Interface shows Autoupdate disabled after Network Updater enables it**

The user should be aware that since Network Updater uses the UDP command method for enabling and disabling of SM Autoupdate on APs, the user may not get an accurate status response from the AP if they are using the Telnet interface on an AP to inquire on the status of Autoupdate on the AP. This is because the Telnet interface will only report on the status of Autoupdate based on previous Telnet commands – without considering if the AP received a separate UDP command for Autoupdate. See [SM Autoupdate Feature](#) for more details on how Network Updater makes use of the SM Autoupdate capabilities on the AP.

### **Network Updater tries to update an already updated SM when using SM Autoupdate**

It is a known issue that some radios may attempt to perform an upgrade even if they are already up to date on their software and FPGA releases. This issue affects newer SMs only. Newer SMs are those that show the HW/SW scheduler option directly on the configuration page (do not require a separate FPGA to be loaded to initiate HW scheduler operation). This issue is a result of the need for separate FPGA releases being distributed by the SM Autoupdate command to support the older radios on a network. Newer radios no longer use a separate FGPA file, but the reference to the Older FGPA file causes the newer radio to incorrectly believe it needs to perform an update. This may cause a reboot of the newer SM once or more during the period when SM Autoupdate is enabled on the AP. For this reason it is not recommended that operators repeatedly enable and disable SM Autoupdate on the same AP. SM Autoupdate should be used initially to perform the majority of a network upgrade, and then turned off (disabled). The user can then use direct update capabilities to radios that require special attention to complete their upgrade actions.

### **Update of radio devices works fine, but updates of CMM micro platforms fail**

CMM3 based platforms, such as the CMMmicro, use the TFTP service to perform upgrades. If basic communication to the CMM is available (verify through a [ping](#)) then the issue may be on the TFTP communications port settings on any routers or firewalls between the Network Updater and the CMM3 in the network. Be sure that two-way communications on the TFTP port is enabled. See [Network Communications](#) for more information on required communication protocols and ports.

### **I am applying an update to an unsupported release**

- Network Updater does not explicitly check whether an unsupported Release is being updated.
- Symptoms of this include: SM Autoupdate does not function correctly (SMs may not have a recent enough software version that supports SM Autoupdate).
- In most cases, Network Updater will function with all elements above Release 4.1. For versions prior to that, it may be necessary to manually update the elements.

### **Network Updater does not discover or update SMs**

- Make sure all APs are loaded.



August 2021

- Make sure that SNMP is accessible by the Machine executing Network Updater.
- The AP SNMP configuration needs to be set to support SNMP from the Machine executing Network Updater.
- A script is also provided for performing this. (However, it will be necessary to reboot the Access Point after this parameter is set).

### **An AP goes down during an update**

- If the order of Updates is not specified, an update process may be interrupted due to a loss of network connectivity to the specified element.
- Typically, reinitiating the update will resolve this problem. (Since the element that caused the loss of connectivity has already been updated, it will not be re-updated).
- It is advisable to re-configure the network archive now to avoid the problem in future.

### **If my radio web interface is locking up, will Network Updater still work?**

On some version of software, an HTTP lock-up error can occur which prevents an AP module web interface from responding. When this error happens, the radio continues to function and manage user traffic. The web interface will not return until the AP is rebooted. If you are experiencing this problem on your network, it will NOT affect Network Updater performance. Network Updater will reboot the AP module as a part of the upgrade process, clearing the HTTP lock up problem on any radios that currently are experiencing it. In addition, Network Updater installation packages contain some specific checks to ensure that the HTTP interface on the radio is working correctly, and if not, it will restore the radio to working order as a part of the upgrade process, while ensuring the upgrade completes correctly.

### **I cannot downgrade my R8.x radios to R7.x**

Two different issues could be applicable here:

- When downgrading from R8.x, which are hardware scheduler only releases, you can only downgrade to hardware scheduler versions of 7.x. If you do not have Advantage APs, then the only release you can downgrade to is 7.3.6. Once you have downgraded to a 7.x release successfully, it is possible to switch over to software scheduler mode if desired.
- Due to third-party licensing restrictions radios that are shipped from the factory with R8.x or higher on them cannot ever be downgraded below R8.0. If the user attempts to install a pre-8.0 release on such a radio through the Network Updater tool, the error message `Cannot downgrade below 8.0` will appear in the History Log file as well as in the State column for the element.

### **An HSBH link dropped during an upgrade, and the far-end HSBH does not respond**

If the near side of a HSBH link is upgraded first the network link between the radios will be lost. This will prevent communications with the far side of the link. If this occurs, the near side of the link will need to be downgraded back (using the same update procedure through Network Updater) to the

August 2021

original software load to restore communications with the far side of the link. See [Upgrading High-speed Backhauls](#) for proper procedures on upgrading these units without losing communications.

### Network Updater hangs loading packages or performing an update

To initiate a Network Update, the Network Updater tool will look at the list of current selected packages you have in the Manage Packages window. For each package that is selected, the tool will need to load this package into memory to inspect it. It is possible that if you have many packages selected, and a very limited amount of memory on the computer running the network updater tool, that the tool may run out of available memory and stop functioning. In this instance you will continue to have the progress bar displayed, but no additional History entries show up in the History window. If you run into this situation, the way to address it is to be sure you only select the packages needed for the current update activity. You can have other packages in the manage Packages list, if they aren't selected. If you still have the issue, then you may need to segment your upgrade activity so that you can limit the number of active packages needed to complete the upgrade.

**note** ..... This situation would likely only occur if the user is using a computer with very limited memory (such as 128MB and restricted or no file paging), and if they were loading many system release packages (10 or more).

## Resources for Support

### Network Updater Help

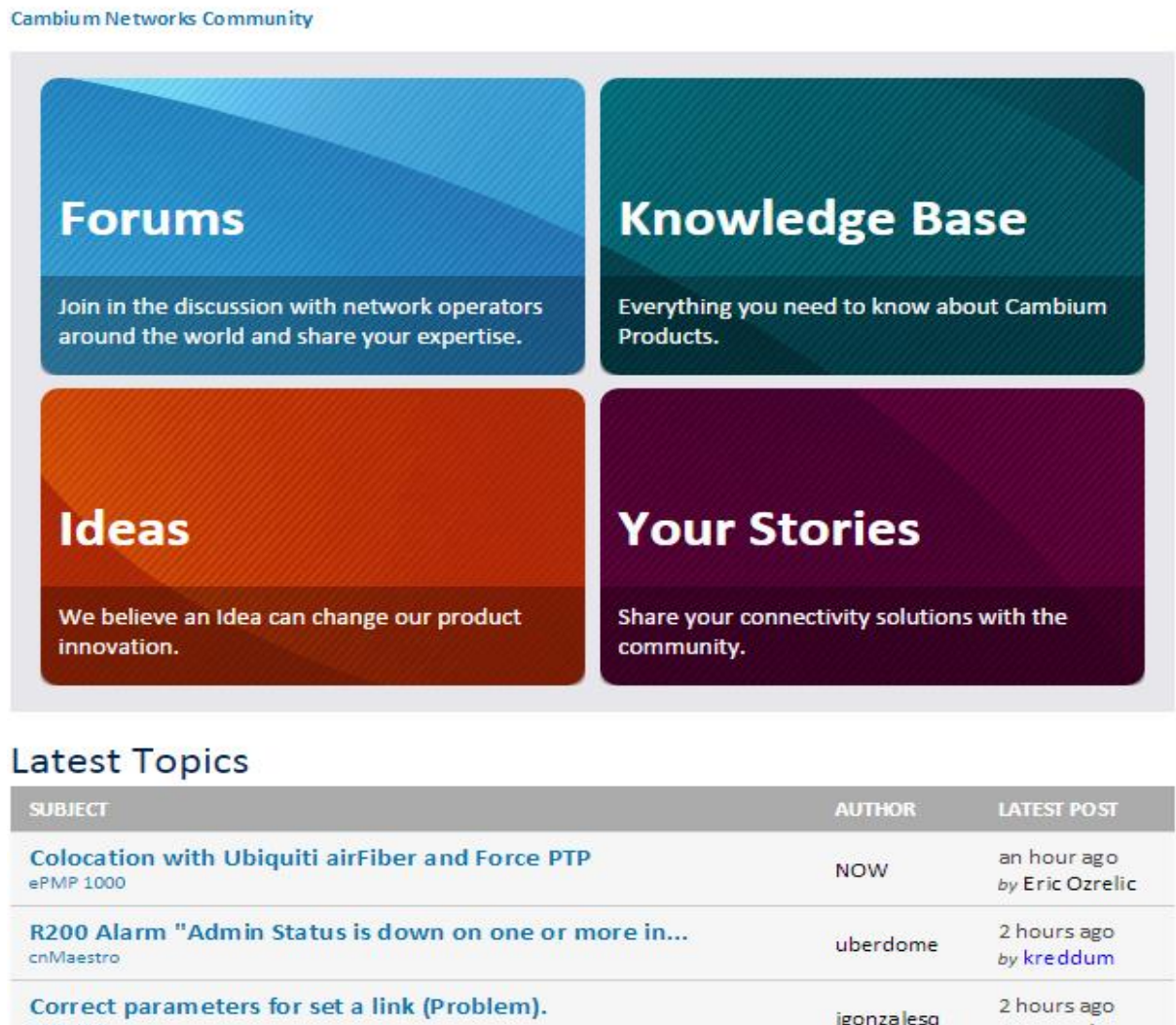
This help document is the main support media for the Network Updater tool. The user should search this document for information before consulting other sources of information. See [Help→Contents](#).

### 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/>. The contents of this page is shown below..

August 2021

Cambium Networks Community



## Forums

Join in the discussion with network operators around the world and share your expertise.

## Knowledge Base

Everything you need to know about Cambium Products.

## Ideas

We believe an Idea can change our product innovation.

## Your Stories

Share your connectivity solutions with the community.

### Latest Topics

SUBJECT	AUTHOR	LATEST POST
<b>Colocation with Ubiquiti airFiber and Force PTP</b> ePMP 1000	NOW	an hour ago by Eric Ozrelic
<b>R200 Alarm "Admin Status is down on one or more in..."</b> cnMaestro	uberdome	2 hours ago by kreddum
<b>Correct parameters for set a link (Problem).</b> R200-1000	jgonzalessq	2 hours ago

After clicking on forum on the above page, or directly clicking on the link <http://community.cambiumnetworks.com/t5/Forums/ct-p/Forums> , forum page gets open.

The following is an example of the contents of the forum page:

Cambium Networks Community > [Forums](#)

## Forums

### Products

#### ePMP

- > ePMP 1000



#### PMP

- > PMP 450
- > Other PMP Solutions



#### PTP

- > PTP 450
- > PTP 650
- > PTP 700
- > PTP 820 Licensed Microwave
- > Other PTP Licensed Microwave Solutions
- > Other PTP Solutions



#### WiFi

- > cnPilot
- > ePMP 1000 Hotspot

#### Planning & Management

- > cnMaestro
- > LINK Planner
- > Other Management Solutions

#### General Discussions

- > Welcome Board
- > WISP Business
- > Regulatory and Homologation

This forum requires authentication for posting.

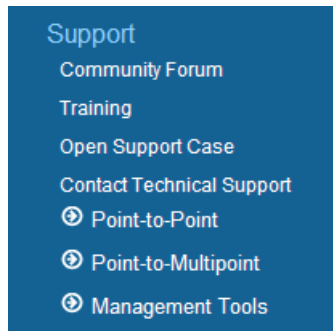
## Technical Support

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

- Network Updater Online Help guide and release notes.

August 2021

- 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. Visit <http://community.cambiumnetworks.com>. See [Community Forum](#).
- 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/>.
- A technical support case, which you can open at <http://www.cambiumnetworks.com/support/contact-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.