

G5 Upgrade Tool

Table of Contents

- [G5 Upgrade Tool](#)
 - [Table of Contents](#)
 - [Description](#)
 - [Support](#)
- [G5 Upgrade Tool Graphical User Interface \(GUI\)](#)
 - [Common workflow for the G5 Upgrade Tool GUI](#)
 - [“Start Upgrade”: Performing a Firmware Upgrade](#)
 - [Firmware Version](#)
 - [“Start conf.ini”: Apply a common conf.ini File to all chosen PDUs](#)
 - [Starting a conf.ini upgrade using the GUI](#)
 - [“Start config.csv”: Perform a Per-device Attribute Configuration](#)
 - [Starting a config.csv upgrade using the GUI](#)
 - [config.csv \(CSV\) File Format](#)
 - [config.csv Notes and Special Cases](#)
 - [names.csv: Perform a single device name and outlet configuration](#)
 - [names.csv Details](#)
 - [File Open, File Save Configuration File \(CSV\) File Format](#)
 - [Verbose Information](#)
- [G5 Upgrade Tool Command Line Interface \(CLI\)](#)
 - [CLI Usage](#)
 - [Common workflow for the G5 Upgrade Tool CLI](#)
 - [“--fwversion”: Performing a Firmware Upgrade using the CLI](#)
 - [“--conffile”: Applying a common conf.ini File to chosen PDUs using the CLI](#)
 - [“--namecfg”: Performing a single device name and outlet configuration using the CLI](#)
 - [“--lbtconfig”: Performing a Per-device Attribute Configuration using the CLI](#)
 - [Example automation script](#)
 - [Using passwords with special characters on a command line](#)
- [Known Issues](#)
 - [GUI Side effects](#)
 - [CLI Side effects](#)
- [Security](#)
- [Appendix A: Software Licenses](#)
- [Appendix B: TCP and UDP Ports used by G5-Upgrade-Tool](#)

- [Release History](#)

Applies to: Panduit G5 Power Distribution Units

Objective: Perform automated operations to PDUs: firmware upgrade, common configuration upload (conf.ini) and per-PDU customized configuration (config.csv).

Pre-requisites:

- Panduit G5 PDU
 - Microsoft Windows:
 - G5-Upgrade-Tool-#-#-#-Windows.zip contains:
 - G5-Upgrade-Tool.exe software
 - pduReleases directory (firmware updates)
 - completeCSV_g5mvp-template.csv (template config.csv file)
 - UserGuide-G5-Upgrade-Tool.pdf (User Guide as PDF)
 - UserGuide-G5-Upgrade-Tool.txt (User Guide as text)
 - For Linux X Window System distributions compatible with CentOS Linux release 7.9.2009 (Core) using “/lib64/libc.so.6 GNU C Library (GNU libc) stable release version 2.17”
 - G5-Upgrade-Tool-#-#-#-Linux.zip contains:
 - G5-Upgrade-Tool software
 - pduReleases directory (firmware updates)
 - completeCSV_g5mvp-template.csv (template config.csv file)
 - UserGuide-G5-Upgrade-Tool.pdf (User Guide as PDF)
 - UserGuide-G5-Upgrade-Tool.txt (User Guide as text)

Use of this software is subject to the terms of the Panduit EULA:

<https://www.panduit.com/content/panduit/na/en/legal-information/end-user-license-agreement.html>

Description

The G5 Upgrade Tool automates three functions useful for managing one or more G5 PDUs.

- Apply a Firmware Upgrade
- Apply a common configuration (conf.ini)
- Apply unique per-PDU configuration (config.csv). Note: The config.csv feature requires PDU firmware version 3.1.10 or newer.
- Apply PDU and outlet names, and set outlet states (names.csv)

The G5 Upgrade Tool runs with a GUI when one is available. To use the tool without the GUI, see “Appendix A: GUT CLI”.

Support

Please report issues with this software to Panduit Customer Support: cs@panduit.com.

G5 Upgrade Tool Graphical User Interface (GUI)

The application window layout has these primary areas:

- Window title bar: shows the path to the open/saved configuration and the name: G5 Upgrade Tool.
- Menu bar: lists short cuts and common functions.
- Left-top: the Configuration entry area.
- Middle-top: Primary functions of the tool and per-function specific configuration/options.
- Right-top: the Device List shows IP Addresses, the function to be performed, and the status of the operation.
- Right-middle: Actions performed on the Device List
- Bottom: Results text area.

The window can be resized and will adjust the user interface elements appropriately.

The menu system has these menus and menu items:

- File
 - Open... : Open a CSV file that uses the G5 Upgrade Tool schema.
 - Save : Save the current configuration to a new file if previously unsaved, or to the same file if previously opened/save.
 - Save as... : Save the current configuration to a new file.
- Edit: This menu provides standard clipboard operations for configuration data entry fields.
 - Cut : cannot be used on the Results field.
 - Copy
 - Paste : cannot be used on the Results field.
 - Select All
- Actions:
 - Select conf.ini: Choose a conf.ini file.
 - Select config.csv: Choose a config.csv file.
 - Start Upgrade : Perform a firmware upgrade function on the configured PDUs.
 - Start conf.ini: Perform an upload of the conf.ini file to the configured PDUs.
 - Start config.csv: Perform an upload of configuration specified in the config.csv file to the configured PDUs.
- Help:
 - Documentation... : this documentation.
 - Licenses... : Panduit and Third Party Open Source Software License disclosures.

- About G5 Upgrade Tool... : Information about the tool, including the version number.

Note: only one Scan Network and Start Upgrade operation can be performed at a time.

Common workflow for the G5 Upgrade Tool GUI

WARNING: Do not interact with the daisy chain, network connections, button interfaces, FTPS, HTTPS, SSH or SNMP interfaces while this software is in use. Interacting with the PDU that is being upgraded WILL interfere with the upgrade process and cause the process to stop unexpectedly! Restarting the upgrade process without interruption will allow it to complete.

1. Run the G5-Upgrade-Tool software (G5-Upgrade-Tool.exe on Windows, G5-Upgrade-Tool on Linux) by double clicking it.
2. If you have a gutconfig.csv file, use the File / Open... dialog to load it.
 - a. Note that File / Open... will read in a Password if one is provided, but File / Save... does not write the Password back to the file. This is also the case for authentication key and privacy key for SNMP settings.
3. If not already entered, enter the UserName and Password for an Admin role user to access the managed devices by SSH/HTTPS.
4. If you are only performing a “config.csv” operation, skip to the section on “Start config.csv”.
5. Choose the “Add Device” or “Scan Network” notebook tab.
6. Enter the required paramters.
 - a. Scan Network uses ICMP Ping and SNMP v2c/v3 credentials string to identify only G5 PDUs and adds them to the Device List. SNMP Settings opens a popup window that allows the user to enter the SNMP version and credentials needed to ping the PDU.
 - b. Add Device just adds the device to the Device List. It does not verify the IP Address is a G5 PDU nor that it is reachable.
7. Click the “Add Device” or “Scan Network” button. The result of the operation is shown in the Results text area.
 - a. Note: “Add Device” and “Scan Network” are not used with “Start config.csv”.
8. The G5 Upgrade Tool is ready to perform a “Start” operation.
9. Execute each function, one at a time:
 - a. Apply a Firmware Upgrade to chosen PDUs:
 - Choose the desired Firmware Version. By default, the ‘Automatic’ version is selected, which will automatically upgrade the PDU to the latest firmware version for that hardware revision.
 - Next, click “Start Upgrade”.
 - b. Apply a conf.ini (common configuration) to chosen PDUs:
 - Click “Select conf.ini”, locate a conf.ini file to be uploaded to all chosen PDUs.
 - Next, click “Start conf.ini”.

- c. Apply a config.csv (unique per-device configuration) to PDUs:
 - Click the “Select config.csv” button and select a config.csv file that defines the PDUs which will be operated upon.
 - Next, click “Start config.csv”.
- d. Note: Apply a names.csv (PDU and outlet naming, outlet states) to PDUs:
 - This is a CLI only function and only operates on one PDU at a time.
10. The progress bar thumb will move across the screen indefinitely until the operation is complete.
 - a. Note that PDU upgrades take several minutes to complete.
 - Please be patient. A PDU with max daisy-chain PDUs can take up to 45 minutes to complete firmware update.
11. The Results window shows the current progress of the chosen function.
12. When complete, a line will report: “Upgrade results: 1 PASS, 1 FAIL, 0 previously passed” where the numbers are replaced with the actual status of the operation.
 - a. Note: “previously passed” devices are not upgraded on subsequent upgrade attempts.
13. If any units FAIL, you may click the “Start” button for the same function again. Sometimes there are transient errors. It is safe to repeat any of the “Start” functions of this tool.
14. You may Save or Save as... when the function is complete. The per-device status is preserved in the saved file.
 - a. Note: the per-device status is replaced with ‘ready’ when you Open the file.

“Start Upgrade”: Performing a Firmware Upgrade

The “Start Upgrade” operation performs a firmware upgrade using HTTPS, SSH and FTPS protocols.

1. Review the “Common workflow for the G5 Upgrade Tool GUI” section on general use of the G5 Upgrade Tool GUI.
2. Review “Firmware Version” section on which Firmware Version to choose. Most customers will be using the latest 3.x.x firmware.
3. Click “Start upgrade...”.

Note that PDU upgrades take several minutes to complete.

Please be patient. A PDU with max daisy-chain PDUs can take up to 45 minutes to complete firmware update.

Firmware Version

The pduRelease directory contains the supported firmware upgrade paths for this tool. For example, the pduRelease directory may contain:

- pduReleases/2.3.27/PANDUIT.FW
- pduReleases/3.3.6/PANDUIT.FW

Unless you were directed to not use a 3.x.x firmware release, please always use the latest 3.x.x firmware included with this software.

NOTE: *DO NOT* upgrade to or actively use the firmware upgrade helper 2.3.x version. This special firmware version is specifically designed for two purposes:

- to transition from 2.x to 3.x.
- to support an older door Security Handle.

To add a new firmware upgrade version:

1. Make a new directory inside the pduReleases directory with the name of the firmware release.
2. Copy the PANDUIT.FW file into the new directory.
3. Start or restart the tool.

“Start conf.ini”: Apply a common conf.ini File to all chosen PDUs

The “Start conf.ini” operation uploads a conf.ini file to the Managed Devices using the FTPS protocol and the operation is started using the SSH CLI.

A conf.ini file is produced by the G5 PDU.

1. Log in to the web UI.
2. From the Settings menu (gear icon) choose System Management menu item.
3. From the Actions menu, choose Download Config File.
4. The conf.ini file is downloaded. The file contains configuration data.

When the conf.ini file is uploaded to a PDU, all settings except for the Network settings are applied to the PDU.

Starting a conf.ini upgrade using the GUI

1. Review the “Start conf.ini: Apply a common conf.ini File to all chosen PDUs.” on creating a conf.ini file.
2. Review the “Common workflow for the G5 Upgrade Tool GUI” section on general use of the G5 Upgrade Tool GUI.
3. Click “Select conf.ini”.
4. Choose a conf.ini file.
5. Click “Start conf.ini”.

“Start config.csv”: Perform a Per-device Attribute Configuration

The “Start config.csv” operation configures each PDU identified in the config.csv file with the specific settings in the config.csv file. The settings are applied using these protocols: SSH, FTPS, HTTPS/HTTP, SNMPv2c.

Follow these steps to create a config.csv file:

1. Copy “completeCSV_g5mvp-template.csv” to a new filename such as “ZoneA-G5config.csv”.
 - a. For each PDU to configure, enter an IP Address in “Cabinet Number”, starting in Column E.
2. Each PDU column must provide configuration values for each Attribute that is being configured.
 - a. Attributes that have multiple valid values use “|” to separate the choices. Example: “DHCP | Static” means the acceptable values are “DHCP” or “Static”.
 - b. Any attribute with a field format that is a string must be entered to be within the maximum length acceptable for that field.
 - c. Any attribute with a field format that is an integer must be entered to be within the valid range of values acceptable for that field.
 - d. Any value field that is an empty string will be skipped/ignored. (You cannot set a field name to an empty string.)
 - e. Any attribute that specifies a PDU, Outlet, Breaker, Sensor, etc instance that is not actively communicating with the PDU is skipped/ignored. eg. If the PDU has a daisy chain of 2 PDUs, but the config.csv specifies a PDU 3, the PDU 3 configuration is skipped/ignored.
3. Delete the entire Row where no change is to be made to that configuration attribute.
 - a. The config.csv file is now ready for use with the G5 Upgrade Tool.

Note: The tool will modify all of the specified configuration settings. If the CSV file chooses to modify these items, the CSV file must be reconfigured later to use the new configuration parameters:

- SNMP v2c read and write community.
- SNMP v3 user name, security level, authentication protocol and key, privacy protocol and key
- The username and/or password used to apply the changes via SSH and HTTP/HTTPS.

Note: The config.csv feature requires PDU firmware version 3.1.10 or newer.

Starting a config.csv upgrade using the GUI

1. Review the “Start config.csv: Perform a Per-device Attribute Configuration” section on creating a config.csv file.
2. Review the “Common workflow for the G5 Upgrade Tool GUI” section on general use of the G5 Upgrade Tool GUI.
3. Click “Select config.csv”.
4. Choose a config.csv file.
5. Click “Start config.csv”.

config.csv (CSV) File Format

Row	Column A	Column B	Column C	Column D	Column E	Column F	...
1	Panduit Detailed Monitoring Device Configuration						
2	1						
3	Cabinet Number				192.0.2.30	192.0.2.31	...
4	CABINET TYPE				Zone A	Zone B	...
5	Network	IP Configuration	Boot Mode	DHCP Static	Static	Static	...
6+

- Row 1: Title
 - Column A contains “Panduit Detailed Monitoring Device Configuration”. This must not be changed.
- Row 2: Version
 - Column A contains “1”. This must not be changed.
- Row 3: Cabinet Number
 - Column A contains “Cabinet Number”.
 - Starting in Column E. Each column describes a configuration for a PDU. The “Cabinet Number” used with the G5 Upgrade Utility is the IP Address of the PDU to configure with all of the configuration values in the same column.
- Row 4: Cabinet Type
 - Column A contains “CABINET TYPE”.
 - Column E may be used as a comment on the configuration or use of the configuration. This row is ignored by the software.
- Row 5: Configuration Data
 - Rows 5 and greater describes the configuration values to be applied to the PDU IP address in Row 3.
 - Columns A through D describe the configuration Section, Sub-Section, Attribute, and Field Format of the value to be changed by each PDU starting in Column E. Do not change Columns A through D. The naming convention is similar to what you see in the web interface.
 - Column A: Section
 - The top level menu grouping of configuration.
 - Column B: Sub-Section
 - A second-level grouping of configuration.
 - Column C: Attribute
 - The Attribute to change.
 - Column D: Field Format

- The format of the Attribute being changed.
 - Column E and higher: Per-PDU configuration values
 - A value to apply to each per-PDU.

config.csv Notes and Special Cases

- Configuring Sensors:
 - A sensor configuration block specifies two names: Default Name and Configure Name.
 - The Default Name in the sample CSV shows the name of a sensor as provided by Panduit. Please do not change this value.
 - The Configure Name is the new name that you want the sensor to be given.
 - The sensors are located by sensor type and the Default Name. If the Default Name is not found, the sensor is located by the Configure Name.
 - If the Default Name (config.csv) is different from the current Sensor Name (web UI), the software will rewrite the Configure Name to the Sensor Name.
 - All other sensor configuration is applied to the located sensor.
- When “Network,IP Configuration,Boot Mode,” is set to “DHCP”, delete IPv4 Address, Network Mask and Default Gateway under “Network,IP Configuration”. Only provide static IP configuration when “Boot Mode” is “Static”.
- When the Field Format is ‘string’ followed by a number, the number represents the maximum number of characters that can be entered into this field.
- When the Field Format is ‘int’, a reasonable integer value must be supplied. Always double check values first with the G5 PDU web UI to verify the data will be accepted. The config.csv may accept and tolerate invalid values and may not always report errors for invalid or out of range data.
- When a PDU is updated, the Date/Time are set to the local Date/Time of the computer running the G5-Upgrade-Tool.
- The Time Zone is configured with the Network,NTP,Region attribute. It can be configured with three different possible value formats:
 - A Region “Number” integer. eg. 601
 - A Region “Name” string. eg. International Date Line West
 - A Region “Offset” “UTC+###:##” or “UTC-##:##” value. eg. UTC-12:00
- The first found Region is the Region Number that will be configured.
- The Region table follows:

Number	Offset	Name
601	UTC-12:00	International Date Line West
3902	UTC+13:00	Samoa
801	UTC-10:00	Hawaii
901	UTC-09:00	Alaska
1001	UTC-08:00	Baja California
1002	UTC-08:00	Pacific Time (US & Canada)
1101	UTC-07:00	Arizona

Number	Offset	Name
1102	UTC-07:00	Chihuahua, La Paz, Mazatlan
1103	UTC-07:00	Mountain Time (US & Canada)
1201	UTC-06:00	Central America
1202	UTC-06:00	Central Time (US & Canada)
1203	UTC-06:00	Guadalajara, Mexico City, Monterrey
1204	UTC-06:00	Saskatchewan
1301	UTC-05:00	Bogota, Lima, Quito, Rio Branco
1302	UTC-05:00	Eastern Time (US & Canada)
1303	UTC-05:00	Indiana (East)
1401	UTC-04:30	Caracas
1501	UTC-04:00	Asuncion
1502	UTC-04:00	Atlantic Time (Canada)
1503	UTC-04:00	Cuiaba
1504	UTC-04:00	Georgetown, La Paz, Manaus, San Juan
1505	UTC-04:00	Santiago
1601	UTC-03:30	Newfoundland
1701	UTC-03:00	Brasilia
1702	UTC-03:00	Buenos Aires
1703	UTC-03:00	Cayenne, Fortaleza
1704	UTC-03:00	Greenland
1705	UTC-03:00	Montevideo
1801	UTC-02:00	Mid-Atlantic
1901	UTC-01:00	Azores
1902	UTC-01:00	cape Verde Is.
2001	UTC+00:00	Casablanca
2002	UTC+00:00	Coordinated Universal Time
2003	UTC+00:00	Dublin, Edinburgh, Lisbon, London
2004	UTC+00:00	Monrovia, Reykjavik
2101	UTC+01:00	Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
2102	UTC+01:00	Belgrade, Bratislava, Budapest, Ljubljana, Prague
2103	UTC+01:00	Brussels, Copenhagen, Madrid, Paris
2104	UTC+01:00	Sarajevo, Skopje, Warsaw, Zagreb
2105	UTC+01:00	West Central Africa
2106	UTC+01:00	Windhoek
2201	UTC+02:00	Amman

Number	Offset	Name
2202	UTC+02:00	Athens, Bucharest, Istanbul
2203	UTC+02:00	Beirut
2204	UTC+02:00	Cairo
2205	UTC+02:00	E. Europe
2206	UTC+02:00	Harare, Pretoria
2207	UTC+02:00	Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius
2208	UTC+02:00	Jerusalem
2301	UTC+03:00	Baghdad
2303	UTC+03:00	Kuwait, Riyadh
2304	UTC+03:00	Nairobi
2503	UTC+04:00	Moscow, St. Petersburg, Volgograd
2506	UTC+04:00	Tbilisi
2401	UTC+03:30	Tehran
2501	UTC+04:00	Abu Dhabi, Muscat
2502	UTC+04:00	Baku
2504	UTC+04:00	Port Louis
2507	UTC+04:00	Yerevan
2601	UTC+04:30	Kabul
2701	UTC+05:00	Islamabad, Karachi
2702	UTC+05:00	Tashkent
2801	UTC+05:30	Chennai, Kolkata, Mumbai, Delhi
2802	UTC+05:30	Sri Jayawardenepura
2901	UTC+05:45	Kathmandu
3002	UTC+06:00	Ekaterinburg
3001	UTC+06:00	Astana
3202	UTC+07:00	Novosibirsk
3101	UTC+06:30	Yangon (Rangoon)
3201	UTC+07:00	Bangkok, Hanoi, Jakarta
3302	UTC+08:00	Krasnoyarsk
3301	UTC+08:00	Beijing, Chongqing, Hong Kong, Urumqi
3303	UTC+08:00	Kuala Lumpur, Singapore
3304	UTC+08:00	Perth
3305	UTC+08:00	Taipei
3307	UTC+08:00	Irkutsk
3401	UTC+09:00	Osaka, Sapporo, Tokyo

Number	Offset	Name
3402	UTC+09:00	Seoul
3605	UTC+10:00	Yakutsk
3501	UTC+09:30	Adelaide
3502	UTC+09:30	Darwin
3601	UTC+10:00	Brisbane
3602	UTC+10:00	Canberra, Melbourne, Sydney
3603	UTC+10:00	Guam, Port Moresby
3604	UTC+10:00	Hobart
3702	UTC+11:00	Vladivostok
3701	UTC+11:00	Solomon Is., New Caledonia
3801	UTC+12:00	Auckland, Wellington
3803	UTC+12:00	Fiji
3804	UTC+12:00	Petropavlovsk-Kamchatsky - Old
3901	UTC+13:00	Nuku'alofa

names.csv: Perform a single device name and outlet configuration

This operation is only available in the CLI.

The “names.csv” operation applies a PDU Name, per-outlet names, and per-outlet on/off states to a PDU.

Create a names.csv file for the PDU “NAME” and all other rows are Outlets. Example names.csv content:

```
NAME,PDU-20201203-093613
1.1,20201203-093613-out-01.01-78901
1.2,20201203-093613-out-01.02-78901
1.3,20201203-093613-out-01.03-78901
1.4,20201203-093613-out-01.04-78901
1.7,20201203-093613-out-01.07-78901
```

Assuming this is an 8 outlet PDU, this example will:

- Name the PDU “PDU-20201203-093613”.
- Set names for outlets 1, 2, 3, 4 and 7 on PDU 1.
- Turn on outlets outlets 1, 2, 3, 4 and 7 on PDU 1.
- Turn off outlets outlets 5, 6 and 8 on PDU 1.

The names.csv changes are applied using the SNMPv2c and HTTPS protocols.

names.csv Details

When the first column is “NAME”, that will change the PDU name at that offset. The PDU offset is incremented for each occurrence.

NAME,{PUT PDU NAME HERE}

All other lines are of this form, to change the pdu.outlet's name:

{PDUNUMBER}. {OUTLETNUMBER}, {OUTLETNAME GOES HERE}

Example: 1 PDU, 24 outlets. Only rename 3 outlets:

```
NAME,My PDU
1.1,laptop
1.2,switch
1.24,router
```

Example: Rename 4 PDUs, with a few sparse outlets to rename:

```
NAME,CORE PDU 1
1.1,Core Switch A Plug 1
1.2,Server RU 1 PSU 1
1.3,Server RU 2
NAME,CORE PDU 2
2.1,Server RU 1 PSU 2
NAME,CORE PDU 3
3.3,Server RU 3
NAME,CORE PDU 4
4.1,Core Switch A Plug 2
```

You cannot skip renaming PDUs. They are always renamed in the order of appearance, and they can be anywhere in the file:

```
1.1,Core Switch A Plug 1
1.2,Server RU 1 PSU 1
1.3,Server RU 2
NAME,CORE PDU 1
NAME,CORE PDU 2
NAME,CORE PDU 3
NAME,CORE PDU 4
2.1,Server RU 1 PSU 2
3.3,Server RU 3
4.1,Core Switch A Plug 2
```

Other constraints:

- If the number of NAME's are more than there are PDUs, the config is rejected.
- If the biggest outlet offset is greater than the max outlets on the unit, the config is rejected.

- If you specify a {PDUNUMBER}.{OUTLETNUMBER} and the PDUNUMBER doesn't exist, the line is ignored. (No error in this case.)
- The config file may rename fewer than the total number of daisy chained PDUs, but never more.
- The "NAME," line may be omitted. No PDUs need to be renamed with NAME. PDU renaming is optional.
- All outlets with configured NAMEs are turned ON. All other outlets are turned OFF.

File Open, File Save Configuration File (CSV) File Format

The G5 Upgrade Tool uses a CSV configuration file for configuration data entered in the user interface. The file is used for rapid reconfiguration of the G5 Upgrade Tool's settings, as well as a way to Save the result of each function performed using the tool.

An example of the CSV configuration file used by the tool is:

```
'#ConfigFileVersion','3.0.1.0'  
'#ConfigFileSchema','2'  
'#UserName','admin'  
'#FWVersion','Automatic'  
'#AddIP','192.168.2.25'  
'#StartIP','192.168.2.30'  
'#EndIP','192.168.2.30'  
192.0.2.2,'upgrade','ready'  
192.0.2.3,'upgrade','ready'  
'#snmpVersion','v3'  
'#SNMPv2Com','public'  
'#WriteCom','private'  
'#snmpUser','admin'  
'#SecLevel','NoAuthNoPriv'  
'#AuthSecLevel','MD5'  
'#PrivSecLevel','AES'  
'#AddIP',''  
'#StartIP',''  
'#EndIP',''  
'#SelectedINI',''  
'#SelectedLBT',''
```

The '#' prefixed items are common configuration items as seen in the user interface. 'AddIP' belongs to "Add Device" and "StartIP"/"EndIP" belong to "Scan Network".

If a Configuration Item is not present, or the tool will use empty values or default values (only FWVersion) in their place.

The '#ConfigFileVersion' and '#ConfigFileSchema' are necessary for future upgrades to this tool, to maintain backward compatibility.

The Device List are the entries that start with an IP Address. Duplicate entries are only operated on ONCE when the upgrade operation is applied.

The Device Lines are generally of the form:

```
IPAddress,'function','status'
```

where 'function' is 'upgrade' and 'status' may be "PASS", "FAIL", or 'ready'.

Verbose Information

Extra information is shown in the text console if the GUI application is run in a shell (Windows: cmd.exe, Linux: sh, etc).

G5 Upgrade Tool Command Line Interface (CLI)

The G5 Upgrade Tool can execute the same operations as the GUI from a Command Line Interface.

The CLI has two modes:

- Non-interactive mode: all arguments are supplied on the command line.
- Batch/Interactive mode: a command shell with commands is provided.

CLI Usage

Executing the tool with the --help paramter produces this help information:

G5 Upgrade Tool v3.0.1.0

Use of this software is subject to the terms of the Panduit EULA: <https://www.panduit.com/content/panduit/na/en/legal-information/end-user-license-agreement.html>
Copyright © 2021-2023 Panduit Corp.
All Rights Reserved.

```
usage: G5-Upgrade-Tool      [--user admin] [--pass password]
                             [--addr [ipaddress ...]] [-v] [-h]
                             [--fwversion version] [--conffile conf.ini]
                             [--nameconfig names.csv new_outlet_state]
                             [--lbtconfig config.csv] [--nogui]
                             [--passedFilename filename]
                             [--failedFilename filename]
                             [BATCH_COMMAND ...]
```

positional arguments:

BATCH_COMMAND	Absence of a BATCH_COMMAND command enters interactive CLI mode. Otherwise, execute a single CLI command.
---------------	--

optional arguments:

--user admin	Admin Role username
--pass password	Admin Role password
--addr [ipaddress ...]	

At least one IP address. If none are specified, the

existing ip.txt file is used.

-v, --version show the version exit

-h, --help show this help message and exit

--fwversion version Upgrade Firmware to this version number (SSH, FTPS)

--conf file conf.ini Upload a conf.ini file (SSH, FTPS)

--nameconfig names.csv new_outlet_state
Set PDU name, outlet names, new outlet state. (SSH, SNMPv2c/v3, HTTP[S])

--lbtconfig config.csv
Upload the config.csv configuration to the PDU IPs contained within (SSH, FTPS, HTTP[S], SNMPv2c)

--nogui Do not present a GUI; do not attempt to connect to the window manager.

--passedFilename filename
A file to store "#IP, '{command}', 'PASS'" results for each device modifying function that was successful. Only useful when one function is performed at a time.

--failedFilename filename
A file to store "--addr ip " results for each device modifying function that failed. Only useful when one function is performed at a time.

Note: --user, --pass are required for: --fwversion, --conf file, --lbtconfig, --nameconfig.

Note: Dashed commands take precedence over the BATCH_COMMAND interface.

BATCH_COMMANDS:

add <IP address>
Add an IP address to the IP list

delete <IP address>
Remove an IP address from the IP list

list
Display the IP list

clear
Clear the IP list

version
Show the version number of this tool

upgrade <version> <user> <password>
Upgrade all items in the IP list to version <version> (SSH, FTPS)

putconf <conf.ini> <user> <password>
Upload a conf.ini file (SSH, FTPS)

namecfg <names.csv> <user> <password> <new_outlet_state> [snmpVersion] [readComStr] [writeComStr] [secName] [secLevel] [authProtocol] [authkey] [privProtocol] [privkey]
Configure the IP List hosts with the csv file defining the PDU name and per-outlet names (SSH, HTTP[S], SNMPv2c)

new_outlet_state:
None = No change.

All_On = Set all on.
 All_Off = Set all off.
 Specified_On_Others_Off = If a name is given, set to on,
 else set outlet off. (DEFAULT)

snmpVersion:

SNMPv2c = Use SNMPv2c to communicate with PDU(s) and requires [readComStr] and [writeComStr] to follow it.

SNMPv3 = Use SNMPv3 to communicate with PDU(s) and requires [username] and [secLevel] to follow it. Any further arguments depend on [secLevel].

readComStr = Allows reading information from the PDU.

writeComStr = Allows writing information to the PDU.

secName = The name of a SNMPv3 user that exists in the PDU.

secLevel:

NoAuthNoPriv = If the user account has NoAuthNoPriv, no further arguments are required for SNMPv3.

AuthNoPriv = If the user account has AuthNoPriv, SNMPv3 requires the authentication protocol [authProtocol] and the authentication passphrase [authkey] set for the account.

AuthPriv = If the user account has AuthPriv, SNMPv3 requires the authentication protocol [authProtocol], the authentication passphrase [authkey], the privacy protocol [privProtocol], and the privacy passphrase [privkey] set for the account.

authProtocol = (MD5|SHA)

authkey = Used when there is an authentication protocol.

privProtocol = (AES|AES128|AES192|AES256)

privkey = Used when there is a privacy protocol.

putlbtconf <config.csv> <user> <password>

Configure the IPs listed in the CSV file with the configuration in the same column. (SSH, HTTP[S], SNMPv2)

exit

quit

Exit the application

Upon completion, the shell exit code is 0 to indicate all requested operations were successful/passed.

A non-zero shell exit code indicates at least one requested operation failed.

More than one operation at a time can be specified on the command line. The sequence of operations when multiple operations are given is:

- --fwversion: upgrade firmware of all specified IP --addr.
- --conf file: apply common configuration, conf.ini, to all specified IP --addr.
- --nameconfig: apply the name.csv to all specified IP --addr.

- `--lbtconfig`: apply per-device configuration, `config.csv`, if it applies to each specified IP -
`-addr`.

Common workflow for the G5 Upgrade Tool CLI

1. Prepare a list of IP addresses of target devices. Start with an initial group of 5 or 10 PDUs.
 - This tool will simultaneously work on 5 target PDUs at a time.
 - Once the initial group of PDUs has had an operation upgraded successfully, scale up the number of target devices passed to the tool at a time as your deployment process allows.
 - Please make sure target PDUs are powered on and have network connectivity to the computer running this tool.
2. Each IP address must be on a single line in a file called "ip.txt". Alternatively, pass an `--addr` address for each IP Address which the operation will be applied.
3. Add authentication arguments to the command line.
4. Add output arguments as desired for `--passedFilename` and `--failedFilename`.
5. Add operations arguments to execute that operation. Note: `lbtconfig` handles the specified IP addresses differently than other operations.

"--fwversion": Performing a Firmware Upgrade using the CLI

1. Choose a firmware version. The newest version included with this tool should be found in the `pduReleases` directory, *DO NOT* upgrade to nor actively use the firmware upgrade helper 2.3.27 version.
2. Run the G5-Upgrade-Tool software with arguments for the username, password, firmware upgrade version number, `passedFilename` and `failedFilename`.
 - Example: `./G5-Upgrade-Tool --user admin --pass myPassword --fwversion 3.1.16 --passedFilename pass.txt --failedFilename fail.txt`
 - Note: Extra status information is printed with the "-v" verbose command line argument.
3. During tool runtime, the tool has many operations that may print out temporary or transient error messages. Please ignore those messages.
4. When complete, the shell exit code ("?" in most shells) will provide a 0 result indicating all units were upgraded successfully. A non-zero result indicates at least one failure.
5. The user may save a copy of the example `pass.txt` file to track which PDUs were successfully upgraded and continue upgrading additional PDUs.
6. If any PDUs failed, they will be listed in the example "fail.txt" file. The user may re-run the software against these PDUs a few times, as some upgrade failures may be transient/temporary.

"--conffile": Applying a common conf.ini File to chosen PDUs using the CLI

1. Review the "Start conf.ini: Apply a common conf.ini File to all chosen PDUs." on creating a `conf.ini` file.

2. Review the “Common workflow for the G5 Upgrade Tool CLI” section on general use of the G5 Upgrade Tool CLI.
3. Add the `--conf file conf.ini` argument to the command line. The `conf.ini` file is the name of the file produced by the instructions in “Start `conf.ini`: Apply a common `conf.ini` File to all chosen PDUs.”.
4. Execute the command as described in the “Common workflow for the G5 Upgrade Tool CLI” section.

“--namecfg”: Performing a single device name and outlet configuration using the CLI

1. Review the “`names.csv`: Perform a single device name and outlet configuration” section on creating a `conf.ini` file.
2. Review the “Common workflow for the G5 Upgrade Tool CLI” section on general use of the G5 Upgrade Tool CLI.
3. Add the `--namecfg names.csv` argument to the command line.
4. (Optional) Prepare SNMP credentials to pass through as arguments.
5. Execute the command as described in the “Common workflow for the G5 Upgrade Tool CLI” section.

“--lbtconfig”: Performing a Per-device Attribute Configuration using the CLI

1. Review the “Start `config.csv`: Perform a Per-device Attribute Configuration” section, focusing only on the parts describing the content of the `config.csv` file.
2. Review the “Common workflow for the G5 Upgrade Tool CLI” section on general use of the G5 Upgrade Tool CLI.
3. Add the `--lbtconfig config.csv` argument to the command line.
4. Execute the command as described in the “Common workflow for the G5 Upgrade Tool CLI” section.

Note: The `config.csv` feature requires PDU firmware version 3.1.10 or newer.

Example automation script

This bash script (Linux or Cygwin or WSL) fills `ip.txt`, attempts a firmware upgrade and then tries two more times to upgrade PDUs that failed.

```
set -x
cat << EOF > ip.txt
192.0.2.100
192.0.2.101
198.51.100.200
198.51.100.201
203.0.113.30
203.0.113.31
EOF
```

```
tries=1
while [ $tries -le 3 ]; do
    ./G5-Upgrade-Tool --user admin --pass myPassword --fwversion 3.1.16 \
        --passedFilename pass-$tries.txt --failedFilename fail-$tries.txt
    if [ $? -eq 0 ]; then
        echo "Successfully upgraded:"
        exit 0
    fi
    echo "Some PDUs failed... trying again:"
    cat fail-$tries.txt
    cp fail-$tries.txt ip.txt
    tries=$((tries+1))
done
```

Using passwords with special characters on a command line

Passwords may contain special characters that are interpreted by shells. Please apply the appropriate escaping rules to the command line for the target command shell. For example, in bash, prefix each special character with a backslash character:

```
\ " double quote
\' quote
\\ backslash
\* asterisk
\? question mark
\! exclamation mark
\$ dollar sign
\{ open brace
\} close brace
\( open parenthesis
\) close parenthesis
```

Example password with lots of special characters:

```
Is!a*$(COMPLEX)\password?*{txt}
```

On the command line:

```
--pass Is\!a\*\$(COMPLEX)\password\?\*\{txt\}
```

Also, please be aware that storing escaped characters in variables can lead to other complications, which are beyond the scope of this introduction.

Known Issues

The software must run from a writable directory, so it can create some temporary files.

You cannot run multiple instances of this software from the same directory, because of the non-unique filenames that are created/modified by this software in the same directory.

Occasionally an ERROR may be reported in the Results text area while applying a config.csv file and the result will be a PASS. In this case, the config.csv may not have been fully applied. Please click “Start config.csv” up to two more times until it provides a PASS result and no ERROR messages are shown. Please contact Panduit Customer Support if the ERROR continues to occur.

Please contact Panduit Customer Support if any PDUs fail to upgrade after a few attempts on each failing PDU, or if there are new unexpected issues after performing an operation with the G5 Upgrade Tool.

The Scan Network operation sends sequential ICMP ping requests on hosts between the start and end address. Scan Network will send a SNMP v2c/v3 request to each host that sends a ICMP ping response, in order to accurately identify G5 PDUs. Note: some network firewalls may detect this as suspicious activity and attempt to block this operation.

GUI Side effects

The tool creates/overwrites these files:

- ssh-debug.log
- g5-upgrade-tool-log.txt

The tool uses the FTPS, SNMPv2c/v3, HTTPS and SSH protocols to perform the necessary operations. When necessary, the tool temporarily reconfigures the last SNMP Manager entry to use random credentials and the IP Address of the computer running the G5 Upgrade Tool.

CLI Side effects

The tool modifies these files using the --addr, clear, add, delete commands:

- ip.txt

When --failedFilename or -passedFilename are used, the passed filenames are deleted before appending new results.

The tool creates/overwrites these files:

- ssh-debug.log

Each command/function of the tool specifies the protocols it may use to perform an operation. The tool uses SSH, HTTP[S] and/or FTPS (encrypted FTP) protocols to perform most operations. HTTP[S] means that HTTP is only used if HTTPS is not enabled. PDUs default to shipping with HTTPS enabled. If SNMPv2c/v3 is specified by the operation (firmware upgrade does not use SNMPv2c/v3), the tool will temporarily reconfigure SNMPv2c to use ‘public’ and ‘private’ credentials.

Security

This software requires the username and password credentials of an Admin Role user on the managed devices. The user must protect the credentials according to their security requirements.

The tool will use HTTPS when HTTPS is enabled. HTTPS is enabled by default on G5 PDUs. However, if the device has HTTP only enabled, the tool will use HTTP instead.

The conf.ini and config.csv files MAY contain user-entered sensitive information (credentials such as usernames, passwords or secrets; or any user entered information that the customer considers sensitive for their G5 PDU configuration). The user must protect any sensitive information and/or credentials according to their security requirements.

The tool requires usernames and passwords of the target PDUs to operate. Status information emitted to the screen or the ssh-debug.log may include these credentials.

When using the command line arguments --user and --pass, please be aware that a user running “ps” on the same computer may be able to observe these command line arguments.

When contacting tech support, please remove usernames and passwords from any data that may be requested.

This software has a code signature, so the user can verify authenticity and integrity of the executable code. On the Windows operating system, the signature is automatically verified.

On Linux operating systems, the outermost .zip file has a corresponding .zip.sig file as well as the ZIP file inside containing the software. To verify the signature (digest), download the Panduit-G5-Upgrade-Tool-public.pem key file. The Panduit-G5-Upgrade-Tool-public.pem key file will either change very infrequently or not at all.

An example of the command to verify the outer digest (signature) is:

```
openssl dgst -verify Panduit-G5-Upgrade-Tool-public.pem -sha256 -keyform PEM \  
-signature GUT_v3_0_0_0-CentOs7_9.zip.sig \  
-binary GUT_v3_0_0_0-CentOs7_9.zip
```

An example of the command to verify the inner digest (signature) is:

```
openssl dgst -verify Panduit-G5-Upgrade-Tool-public.pem -sha256 -keyform PEM \  
-signature G5-Upgrade-Tool-3-0-0-0-Linux.zip.sig \  
-binary G5-Upgrade-Tool-3-0-0-0-Linux.zip
```

Each openssl digest verification command will produce a message indicating success:

Verified OK

If the digest could not be verified, please contact Panduit technical support.

Appendix A: Software Licenses

The GUI provides a Help / Licenses... menu item that lists copyrights and software licenses that apply to software used to build the product or are integrated components of the product.

Appendix B: TCP and UDP Ports used by G5-Upgrade-Tool

The G5-Upgrade-Tool connects to these ports on the target G5 PDU.

Port, Protocol	Description
ICMP Ping	For the Scan Network operation.
TCP 22	SSH for performing commands related to firmware update and conf.ini.
TCP 20, 21	FTPS Control & Data for firmware update and conf.ini upload.
TCP 'high' port #s	FTPS Data.
TCP 80, 443	HTTP/HTTPS for PDU status. Configuration for config.csv and names.csv operations.
UDP 162	SNMP v2c for configuration that is not available in the web server (config.csv, names.csv) and performing a Scan Network operation.

Release History

v3.0.1.0:

- AS-89: SNMPv3 workaround for G6.
- AS-88: SNMPv3 settings bug fix.
- AS-86: SNMPv3 settings bug fix.
- AS-84: G6 exception bug fix.

v3.0.0.0:

- AS-77: GUT SNMPv3 Support
- AS-76: GUT IPv6 Support
- AS-73: Add G6 support to GUT

v2.3.0.0:

- AS-70: Add 'Automatic' firmware version feature.

v2.2.2.0:

- AS-48: Handle G5 beta firmware release versions in GUI. Handle upgrading from a beta to another beta.

v2.2.1.0:

- AS-49: Downgrade option must work correctly for GUI and CLI incantations of the CLI.
- AS-44: Document ports and protocols used by G5-Upgrade-Tool.
- AS-40: CLI: If no --addr is specified and no 'ip.txt' file exists, do not start an operation that requires an IP address.
- AS-27: Remove --loadexternallib.
- AS-44: Add port/protocol information to documentation.
- AS-28: Add Linux package signing enduser docs.
- AS-38: Fix copy/paste in CentOS documentation window.
- AS-21: Fix copy/paste in documentation/licenses.
- AS-20: Fix copy/paste in Results box.

v2.2.0.1:

- AS-42: Document config.csv Network Configuration caveat about DHCP & Static IP configuration.
- AS-43: Add sensor name configuration.

v2.2.0.0:

- AS-32: Primary GUI features were added to the CLI.
- AS-32: The --namecfg names.csv feature was added to the CLI.
- AS-31: config.csv: SNMP v2c configuration now writes to all 5 Managers, instead of always writing the first one.
- AS-31: SNMP v2c access security has been improved. When SNMP v2c is required to perform an operation, the GUT tool discovers the IP of the GUT host as seen by the PDU and uses it; also, the GUT tool generates random READ/WRITE community strings and then restores the community strings when done.
- AS-26: If no --addr are passed to the GUT CLI and there are empty lines in the ip.txt file, the tool will generate an erroneous failure message. Workaround: Do not put empty lines in ip.txt.
- AS-18: Only emit an error message if the written outlet name change did not match.
- AS-17: State management of login/logout was improved to fix and authentication issue.
- AS-16: In config.csv, the Cabinet Number field is only processed if it has an IP address.

v2.1.1.0: Firmware downgrade error message corrected. Firmware filename detection error message improved. The SelectedINI and SelectedLBT are now saved/restored from the GUT File Open/Save config file. Linux build.

v2.1.0.0: Update the transitional G5 upgrade firmware to 2.3.27.

v2.0.0.0: Add "conf.ini" (bulk common configuration) and "config.csv" (per-PDU unique configuration customization) functions.

v1.0.4.0: Support x.y.z and x.y.z.w firmware version numbers.

v1.0.3.0: Eliminate sleep after mkfs. Proactive workaround (switch to non-blocking socket before ssh close) to try to avoid a socket timeout/shutdown race condition when the PDU is known to abruptly reboot.

v1.0.2.0: Updated 2.3.22 transitional upgrade firmware image.

v1.0.1.0: First release based on PG5-F1-GUT Requirements.

Copyright © 2021-2023 Panduit Corp. All Rights Reserved.