ROOT TIM HUB DGA4132 AND ANSUEL GUI - VERSION AGTHP 2.3.3

This guide has been written to have a simple and immediate reference point in case you want to proceed with the enabling of the root user of the TIM HUB DGA4132 modem router (hereinafter "router") and the subsequent installation of the Ansuel GUI. All the steps have been taken and adapted from the websites listed in the paragraph below, then grouped on this page and set up in the correct order.

This guide is available in the following formats:

- Markdown (`TIM_HUB_guide_IT.md`)
- PDF (`TIM_HUB_guide_IT.pdf`)
- HTML (`TIM_HUB_guide_IT.html`)

WEBSITES

- Hacking Technicolor Gateways: Material for MkDocs
- IlPuntoTecnico GUI Ansuel
- GitHub GUI Ansuel
- GitHub AutoFlashGUI
- WinSCP

USEFUL FILES

The `autoflashgui-master_timhub.zip` file contains the `16.02.2018` version of the AutoFlashGUI tool developed by Mark Smith (mswhirl). Once extracted, inside the *autoflashgui-master/firmware* folder you can find the following files needed for this guide:

- `AGTHP_1.0.3_CLOSED.rbi.torrent`: torrent file to start the download of the firmware version AGTHP 1.0.3 downloaded from the website "Hacking Technicolor Gateways: Material for MkDocs". Move the downloaded file into the *autoflashgui-master/firmware* folder
- `AGTHP_2.3.3_CLOSED.rbi.torrent`: torrent file to start the download of the firmware version AGTHP 2.3.3 downloaded from the website "Hacking Technicolor Gateways: Material for MkDocs". Move the downloaded file into the *autoflashgui-master/firmware* folder
- `GUI.tar.bz2`: stable version 9.6.65 of the Ansuel GUI downloaded from Ansuel's `gui-dev-build-auto` GitHub repository. Please check for new versions before proceeding

---

GUIDE - PART 1

- Update the router to version 2.3.3 (you can do this using the "TIM Modem" smartphone app available for Android and iOS)
- From the first *Gateway* tab in the web GUI, if necessary, backup configuration in `.bin` via the *Export* button. A file named "config.bin" will be downloaded
- Reset the router via the *Reset* button
- After reboot, login to the web page (`admin/admin`), don't change the password and activate the *Extended configuration* mode

> WARNING: To enable the Extended Configuration it's necessary to click on a tab that appears ONLY at the first login immediately after a reset. If you log out of the web GUI or close the browser window, you will need to perform another router reset to trigger the Extended configuration prompt again. Furthermore, the router must NOT be connected to the Internet in any way: disconnect the RJ11 cable, the Ethernet cable in the WAN port or the FTTH connection.

- To log in again in the GUI, the password is the **ACCESS KEY** on the label located at the base of the router (under the last barcode in the left column)
- Enter the first *Gateway* tab and perform the downgrade to version 1.0.3 from the third tab. To do this, load the `AGTHP_1.0.3_CLOSED.rbi` file by clicking on *Choose file* and then on *Update* in the *Firmware update* section
- After reboot, you won't be able to login. Reset router from the button on the back (hold for **10-12 sec.**)
- After the second reboot, login to the web page (`admin/admin`) without changing the password
- Run the `autoflashgui.exe` program inside *autoflashgui-master* folder

AUTOFLASHGUI.EXE

Set the following parameters with their respective values

- Load default: *Generic (Advanced DDNS)*
- Target IP: ip router
- Username: user GUI web
- Password: password GUI web
- **DO NOT** select *Firmware File Name* and *Flash firmware?*
- Check *Split the given command on semicolons [...]* if not already selected
- Leave the other settings unchanged
- Click on *Run*
- Wait for result on the shell
- Close the program (it will no longer be necessary)
- Connect with SSH to the router and try to authenticate with `root/root`

GUIDE - PART 2

- Enable the Serial Console Port from the router's root shell
  - `sed -i -e 's/#//' -e 's#askconsole:.*\$#askconsole:/bin/ash#' /etc/inittab`
- Check the banks status
  - `find /proc/banktable -type f -print -exec cat {} ';' -exec echo ';'`
- Take note of the following parameters

```
...
/proc/banktable/booted
<take note of this>
proc/banktable/active
```

```
<take note of this>
...
```

- To achieve our goal, the result of the previous command must become as follows

```
/proc/banktable/active
bank_1
/proc/banktable/activeversion
Unknown
/proc/banktable/booted
bank_2
```

- Then proceed to the next step to set `bank_1` as active and then delete it to always boot the `bank_2`

SCRIPT

- Create a script using `vim` with the following commands

```
# Ensure two banks match in sizes
[ $(grep -c bank_ /proc/mtd) = 2 ] && \
[ "$(grep bank_1 /proc/mtd | cut -d' ' -f2)" = \
"$(grep bank_2 /proc/mtd | cut -d' ' -f2)" ] && {
# Clone and verify firmware into bank_2 if applicable
[ "$(cat /proc/banktable/booted)" = "bank_1" ] && {
mtd -e bank_2 write /dev/$(grep bank_1 /proc/mtd | cut -d: -f1) bank_2 && \
mtd verify /dev/$(grep bank_1 /proc/mtd | cut -d: -f1) bank_2 || \
{ echo Clone verification failed, retry; exit; } }
# Make a temp copy of overlay for booted firmware
cp -rf /overlay/$(cat /proc/banktable/booted) /tmp/bank_overlay_backup
# Clean up jffs2 space by removing existing old overlays
rm -rf /overlay/*
# Use the previously made temp copy as overlay for bank_2
cp -rf /tmp/bank_overlay_backup /overlay/bank_2
# Activate bank_1
echo bank_1 > /proc/banktable/active
# Make sure above changes get written to flash
sync
# Erase firmware in bank_1
mtd erase bank_1;
# Emulate system crash to hard reboot
echo c > /proc/sysrq-trigger; }
# end
```

- Run the following command to make it executable
  - `chmod +x script.sh`
- Run the new script
  - `./script.sh`

GUIDE - PART 3

- Now we can proceed with the firmware upgrade to return to version 2.3.3
- Open WinSCP (or similar software) and connect with SCP protocol to the router with `root/root` credentials
- Upload the `AGTHP_2.3.3_CLOSED.rbi` file inside the `/tmp` router directory and rename it in `new.rbi`
- Run the following command from the shell
  - `cat "/tmp/new.rbi" | (bli_parser && echo "Please wait..." && (bli_unseal | dd bs=4 skip=1 seek=1 of="/tmp/new.bin"))`
- It's necessary to proceed with a clean-up of files and configurations
- Create a backup with the following command and save it on your PC via WinSCP
  - `tar -C /overlay -cz -f /tmp/backup-$(date -I).tar.gz $(cat /proc/banktable/booted)`
- Run the following command to completely clear the currently booted bank overlay
  - `rm -rf /overlay/$(cat /proc/banktable/booted)`
- If you change the firmware version, the root may be lost. DO NOT restart and then proceed to the next step

PRESERVING ROOT ACCESS

- Run the following block of commands via SSH to prepare a script that will only need to be run once on next boot to grant root access

> COPY AND PASTE INTO THE TERMINAL. PRESS ENTER TO EXECUTE THE LAST COMMAND.

```
mkdir -p /overlay/$(cat /proc/banktable/booted)/etc
chmod 755 /overlay/$(cat /proc/banktable/booted) /overlay/$(cat
/proc/banktable/booted)/etc
echo -e "echo root:root | chpasswd
sed -i 's#/root:.*\$#/root:/bin/ash#' /etc/passwd
sed -i -e 's/#//' -e 's#askconsole:.*\$#askconsole:/bin/ash#' /etc/inittab
uci -q set \$(uci show firewall | grep -m 1 \$(fw3 -q print | \
egrep 'iptables -t filter -A zone_lan_input -p tcp -m tcp --dport 22 -m comment --
comment \"!fw3: .+\" -j DROP' | \
sed -n -e 's/^iptables.\+fw3: \(.\+\)\".\+/\1/p') | \
sed -n -e \"s/\(.\+\).name='.\+'$/\1/p\").target='ACCEPT'
uci add dropbear dropbear
uci rename dropbear.@dropbear[-1]=afg
uci set dropbear.afg.enable='1'
uci set dropbear.afg.Interface='lan'
uci set dropbear.afg.Port='22'
uci set dropbear.afg.IdleTimeout='600'
uci set dropbear.afg.PasswordAuth='on'
uci set dropbear.afg.RootPasswordAuth='on'
uci set dropbear.afg.RootLogin='1'
uci set dropbear.lan.enable='0'
uci commit dropbear
/etc/init.d/dropbear enable
/etc/init.d/dropbear restart
```

```
rm /overlay/\$(cat /proc/banktable/booted)/etc/rc.local
source /rom/etc/rc.local
" > /overlay/$(cat /proc/banktable/booted)/etc/rc.local
chmod +x /overlay/$(cat /proc/banktable/booted)/etc/rc.local
sync
```

- If the root password has been changed, it will be reset to `root/root`
- The gateway is now clean. Root access via SSH will be enabled again permanently on the next boot

FLASHING FIRMWARE

- Run the following commands one at a time to write the `/tmp/new.bin` file to the booted bank and to cause a hard reboot
  - `mtd -e $(cat /proc/banktable/booted) write "/tmp/new.bin" $(cat /proc/banktable/booted)`
  - `echo c > /proc/sysrq-trigger`

HARDENING GAINED ACCESS

- Run the following in the SSH terminal to prevent your Gateway loosing root access unexpectedly

> COPY AND PASTE INTO THE TERMINAL. PRESS ENTER TO EXECUTE THE LAST COMMAND.

```
# Disable CWMP
uci delete cwmpd.cwmpd_config
uci delete firewall.cwmpd
uci del_list watchdog.@watchdog[0].pidfile='/var/run/cwmpd.pid'
uci del_list watchdog.@watchdog[0].pidfile='/var/run/cwmpevents.pid'
uci commit
/etc/init.d/watchdog-tch reload
/etc/init.d/cwmpd disable
/etc/init.d/cwmpd stop
/etc/init.d/cwmpdboot disable
/etc/init.d/cwmpdboot stop
/etc/init.d/zkernelpanic disable
/etc/init.d/zkernelpanic stop

# Disable CWMP - extra, in case you think it may resurrect
uci set cwmpd.cwmpd_config.state=0
uci set cwmpd.cwmpd_config.acs_url='https://127.0.1.1:7547/'
uci set cwmpd.cwmpd_config.use_dhcp=0
uci set cwmpd.cwmpd_config.interface=loopback
uci set cwmpd.cwmpd_config.enforce_https=1
uci commit cwmpd

# Disable Telstra monitoring
uci delete tls-vsparc.Config
uci delete tls-vsparc.Passive
uci delete autoreset.vsparc_enabled
uci delete autoreset.thor_enabled
uci delete wifi_doctor_agent.acs
uci delete wifi_doctor_agent.config
uci delete wifi_doctor_agent.as_config
uci commit

# Disable Telstra Air/Fon WiFi
/etc/init.d/hotspotd stop
/etc/init.d/hotspotd disable
uci delete dhcp.hotspot
uci delete dhcp.fonopen
uci commit

# Remove any default SSH pubkey
echo > /etc/dropbear/authorized_keys
# Disable SSH access over wan
uci set dropbear.wan.enable='0'
uci commit dropbear

# Free space for gateways with small flash
find /rom/usr/lib/ipk -type f |xargs -n1 basename | cut -f 1 -d '_' |xargs opkg --force-removal-of-dependent-packages remove
```

- If you get one or more error messages from running these commands, you can ignore them: it means the command was not needed for your firmware version

GUI ANSUEL

- Connect with WinSCP to the router as described above
- Copy the `GUI.tar.bz2` file to the `/tmp` directory
- Connect in SSH to the router with root user
- Run the following command to extract the GUI
  - `bzcat /tmp/GUI.tar.bz2 | tar -C / -xvf - && /etc/init.d/rootdevice force`
- Wait until the procedure is finished. If necessary, the router may reboot itself. Ignore the latest error messages
- In case of *Error 9* restart the router and the problem will be solved

CHANGE ROOT AND GUI PASSWORD

- Run the `passwd` command in the terminal to change the login password for the root user. This procedure is strongly recommended
- Once the Ansuel GUI is installed, the username and password will be `admin/admin` again. It is also reccomended to change this password in order to prevent unauthorized access to the administration web page. To do this, after after you log into the web GUI, click on the *Advanced* button at the top right next to the username *admin* and then on *Profile settings*

RESULT

Now you have a TIM HUB DGA4132 modem router updated to AGTHP version 2.3.3 with root permissions enabled and the Ansuel GUI.