Information about Images and Flashing

For those accessing the router after flashing using Wifi the default password is **rooter2017**.

In the Zip archive for your router there may be several images you can use to flash your router. These include *factory*, *upgrade, full factory, flash* and *full upgrade*. Here is a list of what these images are for.

- Images come in two flavors, those without Load Balancing and those with. If the image name has ***full*** in it then it has Load Balancing installed. If you are not using two or more Internet sources (wired, hotspot or both modems) then you don't need Load Balancing and may chose the image with out ***full*** in it's name. You can use the image with Load Balancing in it even if you are only using a single modem without any issues. Some people want it, some don't so a choice is given.
- Images with ***factory*** in their name are used to flash the router from the factory firmware to the ROOter firmware. These images will work with the factory GUI upgrade page. Not all routers will have a ***factory*** image as many don't allow flashing to ROOter this way.
- When a router already runs ROOter then you use the image with ***upgrade*** in it's name to flash to the new version of ROOter. In some cases when upgrading from an older ROOter to a newer one you will be told the router does not support that image file. If you are upgrading from an image made with OpenWrt 18.06 to an image made with OpenWrt 19.07 or 21.02 you may have to use other methods explained later. In most cases you can flash to a newer revision without any problems.
- On routers that have 16meg of flash but only 64meg of RAM there is a special image with ***flash*** in it's name. Once one of these routers has been flashed to ROOter there is not enough free RAM to flash to a newer version. Instead you must first flash to the smaller ***flash*** image and then use that image's GUI to flash to the new ROOter firmware using the ***upgrade*** image.
- If your router is already running a newer ROOter firmware you may still see a message saying the image information does not match the current router's firmware. Select the *Force Upgrade* option and allow the new image to be used. Do this only if you are sure the new image is for your router.
- In most cases deselect the Keep Setting box when it appears as not doing so may cause some problems with the way the router operates. If you are not making a large change in OpenWrt revisions keeping the settings is not a problem.
- In some browsers. after you flash to a new ROOter firmware and you go to access the GUI. You may see a warning page appear. OpenWrt uses a self signed signature certificate and these browsers do not think that is safe and attempt to block you from going to the web page. This is not the case for ROOter routers so

you can go ahead and access the GUI any way.

Here are Chrome and Firefox giving the unsafe warning and the places you need to click to get ROOter access. You normally only need to do this once for a given firmware.

This is what Chrome shows.

Your connection is not private

Attackers might be trying to steal your information from **192.168.1.1** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

💡   To get Chrome's highest level of security, turn on enhanced protection
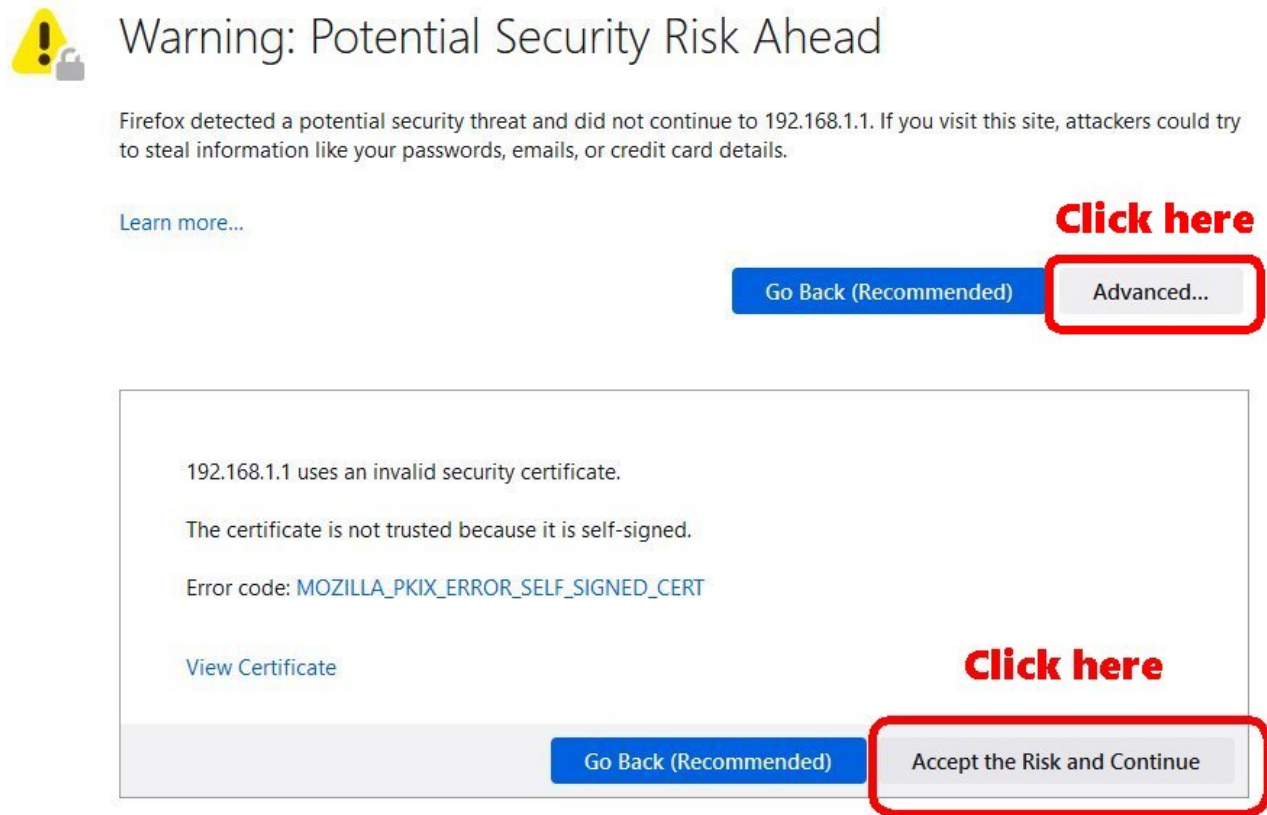
Hide advanced   **Click here**

Back to safety

This server could not prove that it is **192.168.1.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.1.1 (unsafe)   **Click here**

This is what Firefox shows.

Flashing Methods

There are a number of different ways of flashing a router to a ROOter firmware. Some are simple, some are more complicated, while some can use several different methods.

ROOter GUI

Once a router has been flashed to ROOter you can always use the GUI page at *System->Backup/Flash Firmware* to upgrade your router. You may, in some instances, have to force the flash but everything can be done from the GUI.

Forcing is only needed if the new image has a different type than the one currently on the router. This happens with ZBT WG1608 routers that were flashed using the WG3526 firmware. When you go to flash these to a newer image made especially for the WG1608 you will see a message that the router has an image for a WG3526 on it but the image you want to flash is for a WG1608. The same thing can happen with the DualQ H721.

Here is what you see.

Factory GUI

On some routers there is **factory** ROOter firmware that can be used to flash the router from the factory GUI's Update page. This simply a matter of pointing their GUI to the new ROOter firmware and doing an upgrade.

Recovery GUI

Many routers have what is known as a Recovery GUI or a Bootloader GUI. These are designed to allow flashing the router with an image that the factory firmware does not

accept or when the router is not working at all.

These GUI all work in a similar manner.

1. Unplug the router's power supply.
2. Hold in the reset button.
3. Plug in the power supply while still holding in the reset button.
4. Wait until the Leds on the router settle into a fixed patteren. This may be certail Leds are lit or certain ones are flashing. This may take 10 seconds or more.
5. Release the reset button. Some routers require you to release the reset button after the Leds flash a ceertain number of times.
6. **Use your browser to go to http://192.168.1.1/index.html**
7. There you will be greeted with a web page that allows you to upload and flash a new firmware to the router. Many of these pages are in Chinese but are usually simple enough to follow.
8. No checks are made of the image you are flashing so care must be taken to use the correct firmware.

At its simpliest the recovery GUI would be like this. Select the firmware file and update.

OEM Firmware Recovery

You are going to upload new firmware to the device.
Choose a proper file from your local hard drive and click **"Update firmware"** button.
Please, do not power off the device during update, if everything goes well, the device will restart.

Choose File | No file chosen   Update firmware

In other cases it is in Chinese but still simple. Upload the firmware and then confirm you want to flash.

固件恢复模式

恢复   备份

Click here

恢复

- -

192.168.1.1

是否进行恢复?   **Click here**

OK   Cancel

Then there is the more complex one, also in Chinese, that requires navigating several menus.

Breed Web 恢复控制台

系统信息	CPU	Qualcomm Atheros QCA953X rev 2
固件更新	内存	128MB DDR2
Click here	Flash	Winbond W25Q128 @ 25MHz (16MB)
	以太网	Atheros AR8228/AR8229 rev 1
频率设置	时钟频率	CPU: 550MHz, DDR: 400MHz, AHB: 200MHz, Ref: 25MHz
	编译日期	2019-12-29 [git-2153931]
恢复出厂设置	版本	1.1 (r1274)
LSDK/QSDK 设置		

Breed Web 恢复控制台

系统信息	常规固件	编程器固件
固件更新		
固件备份	☐ Bootloader Browse... No file selected.	
频率设置	☑ 固件 Browse... No file selected.	
	☐ ART Browse... No file selected.	
恢复出厂设置	**Check** 内存布局 自动识别	
LSDK/QSDK 设置	☑ 自动重启	
TP-LINK 设置	上传 **Click here**	

Breed Web 恢复控制台

更新确认

文件已上传，请确认下方列出的信息

类型	固件
文件名	openwrt-InterWave-WE826-Q-GO2021-07-28.bin
大小	9.63MB (10092548B)
MD5 校验	aa5e7a23a13299b7709e0988f1ce8c7d

[更新] **Confirm**

TFTP Recovery

Some routers don't have a Recovery GUI but instead use a method called TFTP to load and flash an image on the router. These require a TFTP program on your computer like TFTP32 and some knowledge of what the router expects.

The router has a static IP Address like 192.168.2.119 and it expects the computer to also have a static IP like 192.168.2.88. These IP Addresses vary according to the router involved.

In most cases the Firwall on the computer must be disabled while the upload and flash procedure takes place.

The router also expects the firmware file to have a specific name so it can ask the TFTP program for that file by name.

To flash this way do the following.

1. place the properly named firmware file in the same directory as the TFTP program and start it running.
2. Unplug the router and hold in the reset button.
3. Plug in the power while still holding in the reset button.
4. Wait until you see the TFTP program start to upload the firmware file and then release the reset button.

The firmware file will be uploaded to the router and it will be flashed to it then rebooted.

Command Line

This method is only for those that are comfortable working with the Linux command line and understand the risks involved.

These methods can be used when you can get Telnet or SSH access to a router that does not have a **factory** ROOter image and also does not have a Recovery GUI or TFTP Recovery.

There are two command line methods that can be used to flash a router. Which one is used depends on what packages are available on the factory firmware and how the firmware is laid out.

Sysupgrade

If the factory firmware is based on a version of OpenWrt or is Linux based it will have a package called **sysupgrade** available. This is what is used by the OpenWrt GUI to do the flashing.

To use this you must either copy the firmware file over to the **/tmp** folder or, if the factory firmware supports it, flash from a USB memory stick.

Files can be copied to the router using WinScp if you have SSH access. If you only have Telnet access then copy the file to a USB memory stick, plug it into the router and execute the following at the command line.

mkdir /mnt
mount /dev/sda1 /mnt

This will mount the USB memory stick and make it available for use.

At this point the firmware file will be at either **/tmp/firmware.file** or **/mnt/firmware.file** depending on the method used.

You can test if the flash will work by executing

sysupgrade –test /tmp/firmware.file

and it will tell you the results of a possible flash.

To do the actual flash you would execute

sysupgrade /tmp/firmware.file

The router will reboot after this and run the new firmware. If you find that the sysupgrade test fails but you know the firmware will work then execute

sysupgrade –force /tmp/firmware.file

This will force the firmware to be flashed even if it fails the test. **This is very dangerous and can brick your router.**

MTD

The other method of flashing involves a package called **mtd** which will copy files into partitions on the router. This is not always available and can be used only in certain circumstances.

First, execute the following command.

cat /proc/mtd

The output from this will look similar to this.

dev: size   erasesize   name
mtd0: 00030000 00010000 "u-boot"
mtd1: 00010000 00010000 "u-boot-env"
mtd2: 00010000 00010000 "factory"
mtd3: 00fb0000 00010000 "firmware"
mtd4: 00255bad 00010000 "kernel"
mtd5: 00d5a453 00010000 "rootfs"
mtd6: 00300000 00010000 "rootfs_data"

If you do not see a partition named **firmware** then do not proceed any farther. What we are looking for is the **mtd block** associated with the **firmware** partition. In this case it is **mtd3** but will vary from router to router.

As with the **sysupgrade** method, the firmware file must either be copied to the **/tmp** folder or use a USB memory stick and mount that.

To flash the **firmware** partition with our firmware file execute

mtd -r write /tmp/firmware.file firmware

The partition will be flashed to the firmware file and the router will reboot. **Again this is very dangerous and can brick your router.**

Command line flashing is normally a last resort and should not be attempted by unskilled users.

Other methods

The are other methods that certain routers use to flash a new firmware and are unique to that particular router. These methods will not be covered here but links will be given to sites that have the instructions.