Manual Upgrade of AP Firmware

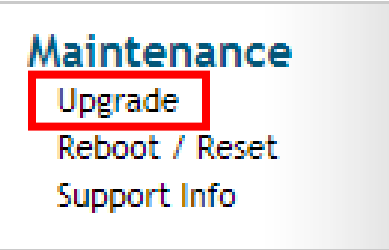
The upgrade or changing of the firmware of an AP can be accomplished from the CLI or the GUI. Below are the steps to perform this task.

GUI:

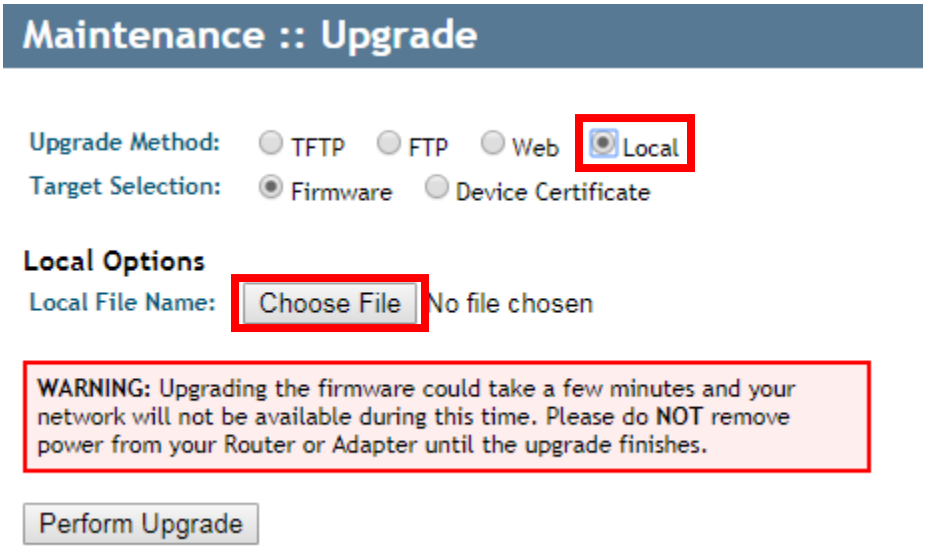
The default login to a Ruckus AP is

Username: super
Password: sp-admin

After login, go to Maintenance -> Upgrade

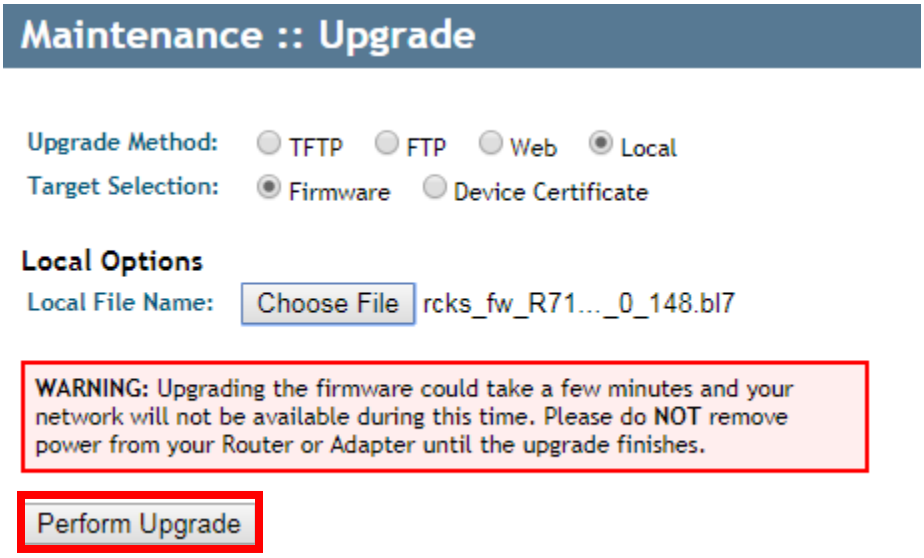


There are several options to upgrade the firmware, but I am going to use Local as the file is on the local computer. Select Local and Choose File.

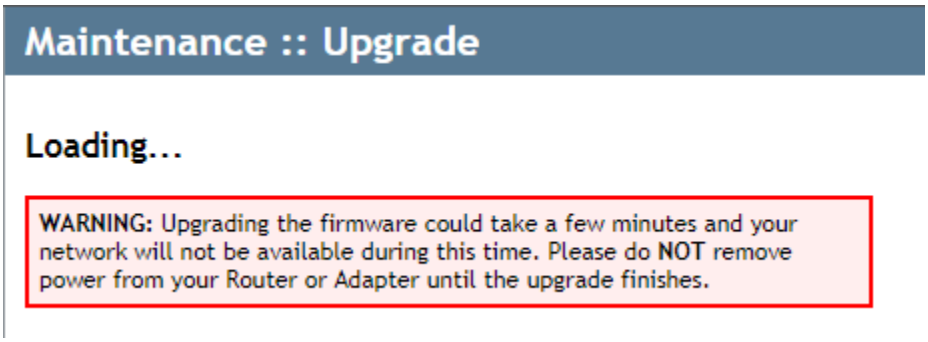


You will be prompted to select the location of the file. The file format is a rcks_fw_*.bl7 where the * is the model and revision number. An example for the R710 is rcks_fw_R710_100_2_1_0_148.bl7.

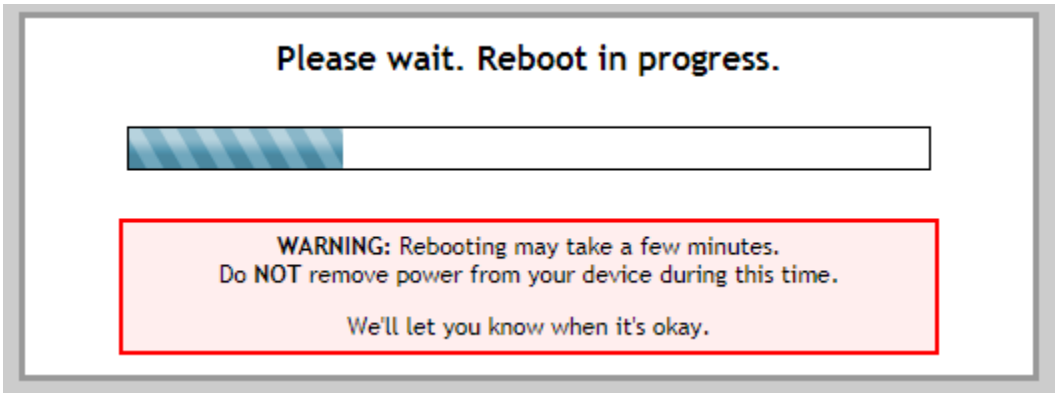
Select Perform Upgrade.



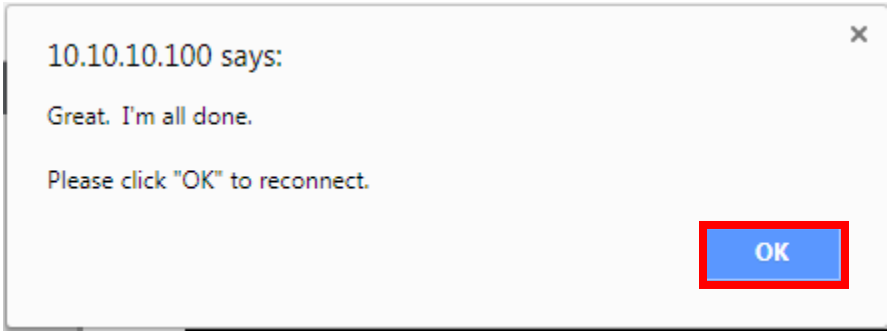
The firmware will be uploaded to the AP.



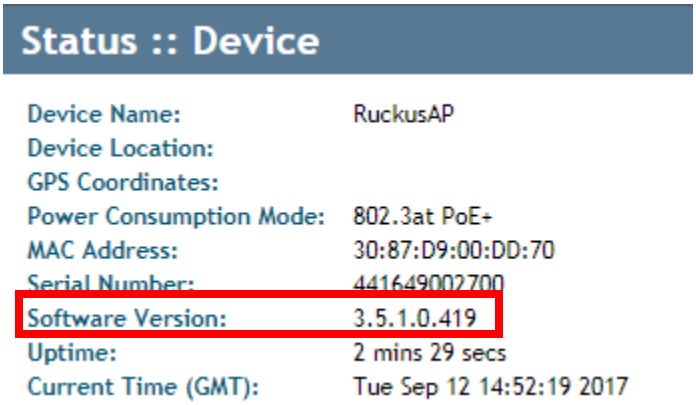
The AP will reboot and apply the firmware.



When the upgrade is complete, click OK.



Now you can login and verify the upgrade.



CLI:

SSH into the AP and login with the same credentials as the GUI.

Username: super
Password: sp-admin

This upgrade will use TFTP for the upload, so you will need to have a TFTP server available and the firmware to load to the AP.

Enter the following commands in the AP CLI:

fw set control ****.bl7
fw set proto tftp
fw set host x.x.x.x
fw update
reboot

Where ****.bl7 is the name of the firmware to upload and x.x.x.x is the IP address of the TFTP server.

Below are the commands entered for the update:

```
rkscli:
rkscli: fw set control R610_104.1.0.0.298.bl7
OK
rkscli: fw set protocol tftp
OK
rkscli: fw set host 10.10.10.101
OK
rkscli: fw update
```

Below is an example of the upgrade process.

```
rkscli:
rkscli: fw set control R610_104.1.0.0.298.bl7
OK
rkscli: fw set protocol tftp
OK
rkscli: fw set host 10.10.10.101
OK
rkscli: fw update
fw: Updating rcks_wlan.main ...
vS4_fw_update: download 10.10.10.101 section=rcks_fw.main image=Image1 ctl_file=R610_104.1.0.0.298.bl7 (/writable/fw/main.cntl)
net_get_flash_ubi(10.10.10.101, R610_104.1.0.0.298.bl7, rcks_wlan.main,, 0)
flash id is 0
imghdr.{hdr_len=160, bin_len=1D571612}
fw_flash_read_open: kernel open(/dev/ubi1_0) rootfs open(/dev/ubi1_1)
flash id is 0

Image1 FW check ...

read failed, remaining=2044 rc=0
vS4_fw_check: md5 check failed
tail_offset 1D569568 bin_len 1D571612 sign 1.
net_get_flash_ubi, Upgrading from Intermediate Signed Image(ISI) to Intermediate Signed Image(ISI) image.
fw_ubi_write_open: kernel open(/dev/ubi1_0)
fw_ubi_write_open: rootfs open(/dev/ubi1_1)


Flashing KERNEL image(1.94MB)
[==========================================================================================================] 100

Flashing RDOTFS image(8.14MB)
net_get_flash_ubi: Receive last block buf 4092==========================================================> ] 98
net_get_flash_ubi: hdr_fsize=8538112, real_fsize=8536064
[==========================================================================================================] 100

Reading Image TAIL:-
TLV No-1.TLV INFO
  Number of TLVS in Tail is 2.
  Size of Tail is 2044.
len 9 tail_len = 9
2. SIGNATURE OBTAINED SUCCESSFULLY
len 259 tail_len = 268
        cert len 1773 pass
3. CERTICATE OBTAINED SUCCESSFULLY
len 1776 tail_len = 2044
```

```
MD5 Checksum successful!!!!!!!!!

Checking Image hash:-
1. Obtaining public key from Certificate.
        Executing openssl x509 -in /tmp/in_cert.pem -pubkey -noout >/tmp/pubkey.pem
        line: Certificate will not expire
  Certificate validity verified.
        line: /tmp/in_cert.pem: OK
2. Public key verified.
3. Decrypting the Image signature.
        Executing openssl rsautl -verify -pubin -inkey /tmp/pubkey.pem -in /tmp/signsure.bin -out /tmp/ext_sha256.
4. Comparing the signatures:-
  IMAGE TAIL SHA256 :
        601b54c9e8c49edd1af6084fbd7028014d5531ce97b5d4a602dd6378c63fcd73
  CALC SHA256 :
        601b54c9e8c49edd1af6084fbd7028014d5531ce97b5d4a602dd6378c63fcd73
        HASH CHECK PASSED.

AIS cleanup : Removing /tmp/ext_sha256...
AIS cleanup : Removing /tmp/in_cert.pem...
AIS cleanup : Removing /tmp/signsure.bin...
AIS cleanup : Removing /tmp/pubkey.pem...
AIS cleanup : Completed
bdSave: sizeof(bd)=0x7c, sizeof(rbd)=0xd0
  caching flash data from /dev/mtd14 [ 0x00000000 - 0x00010000 ]
  updating flash data [0x00008000 - 0x000080d0] from [0xbeac7240 - 0xbeac7310]
_erase_flash: offset=0x0 count=1
Erasing 64 Kibyte @ 0 -- 100 % complete
  caching flash data from /dev/mtd14 [ 0x00000000 - 0x00010000 ]
  verifying flash data [0x00008000 - 0x000080d0] from [0xbeac7240 - 0xbeac7310]
**fw(2456) : Completed
rkscli:
```

When the AP completes the upgrade, Use the following command to verify the upgrade:

get version