

# 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.

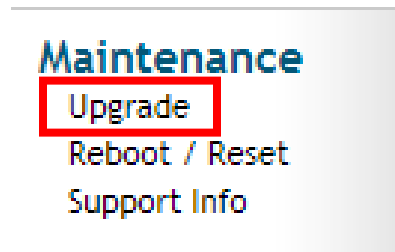
## GUI:

The default login to a Ruckus AP is

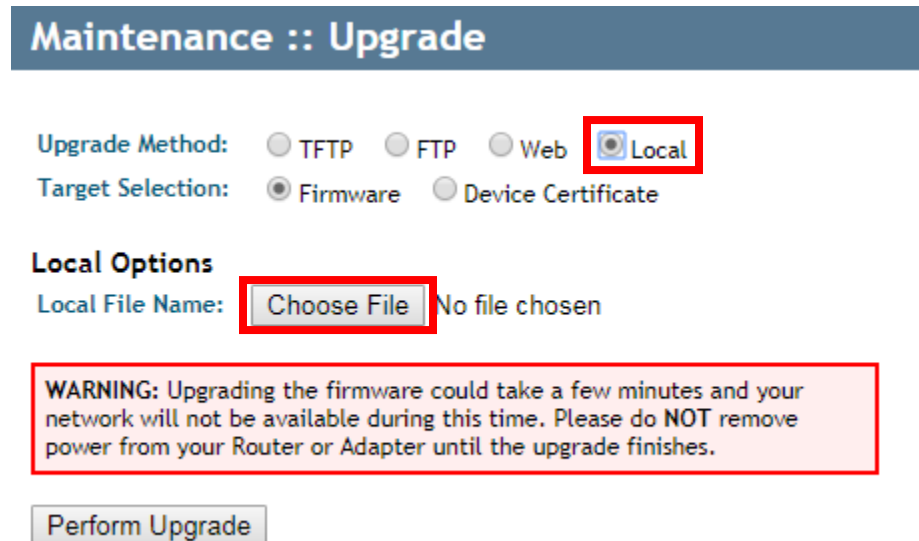
Username: super

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.

A screenshot of the 'Maintenance :: Upgrade' configuration page. The page has a dark blue header with the text 'Maintenance :: Upgrade'. Below the header, there are two rows of radio button options. The first row is 'Upgrade Method' with options: TFTP, FTP, Web, and Local. The 'Local' option is selected and highlighted with a red box. The second row is 'Target Selection' with options: Firmware and Device Certificate. Below this, there is a section titled 'Local Options' with a label 'Local File Name:' and a 'Choose File' button highlighted with a red box, followed by the text 'No file chosen'. A red-bordered warning box contains the text: 'WARNING: Upgrading the firmware could take a few minutes and your network will not be available during this time. Please do NOT remove power from your Router or Adapter until the upgrade finishes.' At the bottom of the form is a 'Perform Upgrade' button.

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.

## Maintenance :: Upgrade

Upgrade Method:  TFTP  FTP  Web  Local

Target Selection:  Firmware  Device Certificate

### Local Options

Local File Name:  rcks\_fw\_R71...\_0\_148.bl7

**WARNING:** Upgrading the firmware could take a few minutes and your network will not be available during this time. Please do NOT remove power from your Router or Adapter until the upgrade finishes.

The firmware will be uploaded to the AP.

## Maintenance :: Upgrade

Loading...

**WARNING:** Upgrading the firmware could take a few minutes and your network will not be available during this time. Please do NOT remove power from your Router or Adapter until the upgrade finishes.

The AP will reboot and apply the firmware.

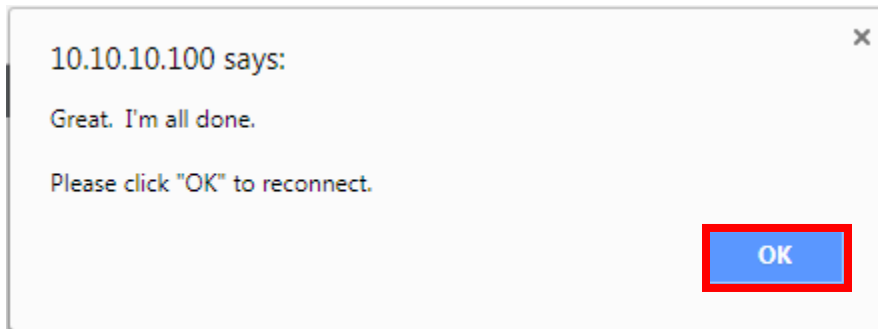
**Please wait. Reboot in progress.**



**WARNING:** Rebooting may take a few minutes.  
Do NOT remove power from your device during this time.

We'll let you know when it's okay.

When the upgrade is complete, click OK.



Now you can login and verify the upgrade.

Status :: Device	
Device Name:	RuckusAP
Device Location:	
GPS Coordinates:	
Power Consumption Mode:	802.3at PoE+
MAC Address:	30:87:D9:00:DD:70
Serial Number:	441649002700
Software Version:	3.5.1.0.419
Uptime:	2 mins 29 secs
Current Time (GMT):	Tue Sep 12 14:52:19 2017

### 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:

```
rksccli:
rksccli: fw set control R610_104.1.0.0.298.b17
OK
rksccli: fw set protocol tftp
OK
rksccli: fw set host 10.10.10.101
OK
rksccli: fw update
```

Below is an example of the upgrade process.

```
rksccli:
rksccli: fw set control R610_104.1.0.0.298.b17
OK
rksccli: fw set protocol tftp
OK
rksccli: fw set host 10.10.10.101
OK
rksccli: fw update
fw: updating rcks_wlan.main ...
v54_fw_update: download 10.10.10.101 section=rcks_fw.main image=Image1 ctrl_file=R610_104.1.0.0.298.b17 (/writable/fw/main.cnt1)
net_get_flash_ubi(10.10.10.101, R610_104.1.0.0.298.b17, rcks_wlan.main,, 0)
flash id is 0
imghdr.(hdr_len=160, bin_len=10571612)
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
v54_fw_check: md5 check failed
tail_offset 10569568 bin_len 10571612 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 ROOTFS 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. CERTIFICATE 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
rksccli:
```

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

get version

```
rkscli: get version  
Ruckus R610 Multimedia Hotzone Wireless AP  
Version: 104.1.0.0.298  
OK  
rkscli: █
```