Grandstream Networks, Inc.

GRP26XX Carrier-Grade IP Phones

Firmware Upgrade Guide

Table of Contents

INTRODUCTION 4

SCENARIO 1: UPGRADE USING GRANDSTREAM PUBLIC HTTP SERVER 5

SCENARIO 2: UPGRADE USING A LOCAL SERVER 6

Local Upgrade via HTTP Server 6

Installing HTTP Server and Uploading Firmware File(s) 6
Configuring Grandstream devices for local HTTP upgrade 8

Local Upgrade via HTTPS Server 9

Installing HTTPS Server 9
Uploading firmware file(s) to XAMPP HTTPS Server 10
Configuring Grandstream devices for a local HTTPS upgrade 11

Local Upgrade via TFTP Server 12

Installing the TFTP Server 12
Uploading the firmware file 13
Configuring Grandstream devices for local TFTP upgrade 15

ADVANCED OPTIONS 16

Automatic Upgrade 16

Firmware File Prefix and Postfix 16

HTTP/HTTPS User Name and Password 17

Table of Figures

Figure 1: Option "Firmware Upgrade and Provisioning" 5
Figure 2: Firmware Web GUI section 5
Figure 3: Starting the HTTP server 6
Figure 4: Selecting the firmware file to upload on the HTTP server 7
Figure 5: Uploading the firmware file to the HTTP Server 7
Figure 6: Firmware upgrade progress 8
Figure 7: Firmware File Fully Downloaded 8
Figure 8: Download XAMPP for windows 9
Figure 9: XAMPP Installation 9
Figure 10: XAMPP Control Panel 10
Figure 11: Apache Module Started 10
Figure 12: XAMPP Directory 10
Figure 13: Index of XAMPP Files 11
Figure 14: Example of Configuring the Upgrade via HTTPS on GRP26XX 11
Figure 15: Downloading the TFTP server 12
Figure 16: Selecting Install Version 12
Figure 17: TFTP Server Installation 13
Figure 18: TFTP Server Interface 13
Figure 19: Selecting TFTP Server Services 14
Figure 20: Selecting Local Directory containing Firmware File 14
Figure 21: Firmware File Upload Verification 15
Figure 22: TFTP Server Configuration 15
Figure 23: Example of Configuring Automatic Upgrade on GRP26XX 16
Figure 24: Screenshot of Firmware file Prefix and Postfix fields 16
Figure 25: Configuring the Firmware File Prefix 17
Figure 26: Configuring the Firmware File Postfix 17
Figure 27: Firmware Files with Prefix/Postfix on local directory 17
Figure 28: Screenshot of HTTP / HTTPS Username and Password Fields 17

INTRODUCTION

All Grandstream products' firmware are improved and updated on a regular basis. Latest firmware versions are available in http://www.grandstream.com/support/firmware

Published firmware versions in Grandstream official website have passed QA tests and included new enhancements implemented, reported issues fixes for better user experience; all changes are logged in Release Notes documents.

Provided Firmware package is specific to a single product or product series, same as release notes document. For example, *Release_GRP261x_1.0.0.31.zip* and *Release_Note_GRP261x_1.0.0.31.pdf* are specific to GRP26XX Carrier Grade IP Phones.

Grandstream recommends to read Release Notes document which may include special firmware upgrade notices and always keep your devices up-to-date by upgrading their firmware versions regularly.

This document describes steps needed to upgrade the GRP26XX devices firmware version and covers the following scenarios:

- **Scenario 1:** Upgrade using Grandstream Public HTTP Server.
- **Scenario 2:** Upgrade using a local Server.
- **Advanced options.**

Scenario 1: Upgrade using Grandstream Public HTTP Server

Grandstream is hosting latest firmware files in a public HTTP server so customers can use it to directly upgrade their Grandstream devices with latest firmware. The same server hosts also BETA firmware when available.

Follow below steps to successfully upgrade your device:

1. Access web interface of your device and go to **Maintenance → Upgrade and Provisioning**
2. Make sure to select "**Always Check for New Firmware**" for "**Firmware Upgrade and Provisioning**"

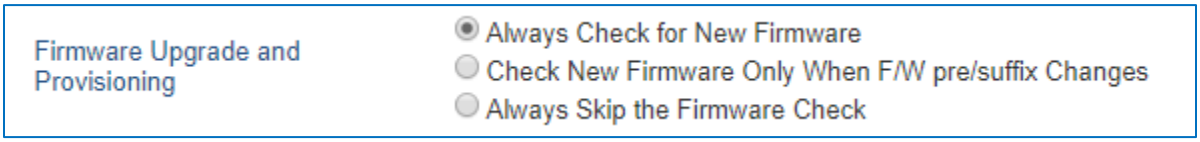

Figure 1: Option "Firmware Upgrade and Provisioning"

3. Go to "Firmware" section,
   - Select "**HTTP"** for "Firmware Upgrade via"
   - Enter "***firmware.grandstream.com***" under "**Firmware Server Path**".

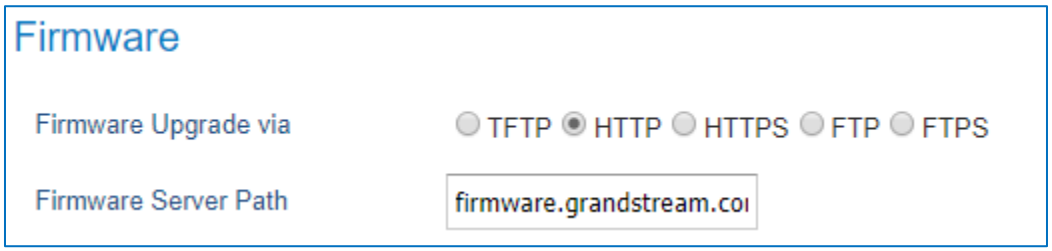

Figure 2: Firmware Web GUI section

4. Click on "**Save and Apply"** button to apply the new settings.
5. **Reboot** the device and wait until the upgrade process is completed.

Notes:

- Internet Access is mandatory in order to be able to upgrade using Grandstream HTTP server.
- To upgrade to BETA firmware (if available), use "***firmware.grandstream.com/BETA***" in step 4.

Scenario 2: Upgrade using a Local Server

Customers can use their own HTTP/HTTPS, FTP/FTPS or TFTP server to upgrade Grandstream devices.

To achieve this, first download firmware files for the appropriate device model from http://www.grandstream.com/support/firmware. Unzip downloaded package and put extracted files in the root directory of your server.

Notes:

- Devices and your server need to be in same LAN.
- If using remote server, make sure to open/redirect ports in your router, so devices can download firmware files from it.

Reminder:
HTTP (TCP) default port is 80, HTTPS (TCP) default port is 443 and TFTP (UDP) default port is 69.

Local Upgrade via HTTP Server

Please refer to the below steps for a local upgrade using **HTTP File Server** tool.

Installing HTTP Server and Uploading Firmware File(s)

1. Launch the install wizard of the tool once it's fully downloaded.
   - Link: http://www.rejetto.com/hfs/download
2. Click on **Run** to launch.

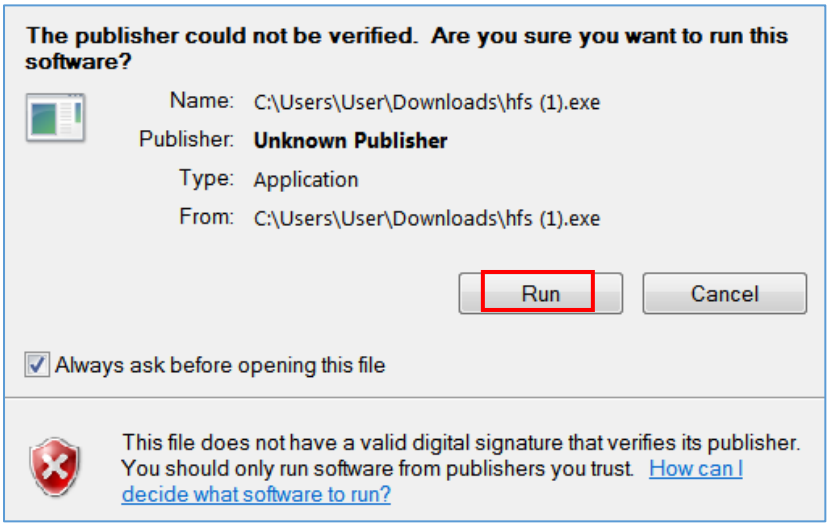

Figure 3: Starting the HTTP server

3. Once HFS start, browse to locate and select the firmware files from your local directories
   - Under **Menu** → **Add files**.

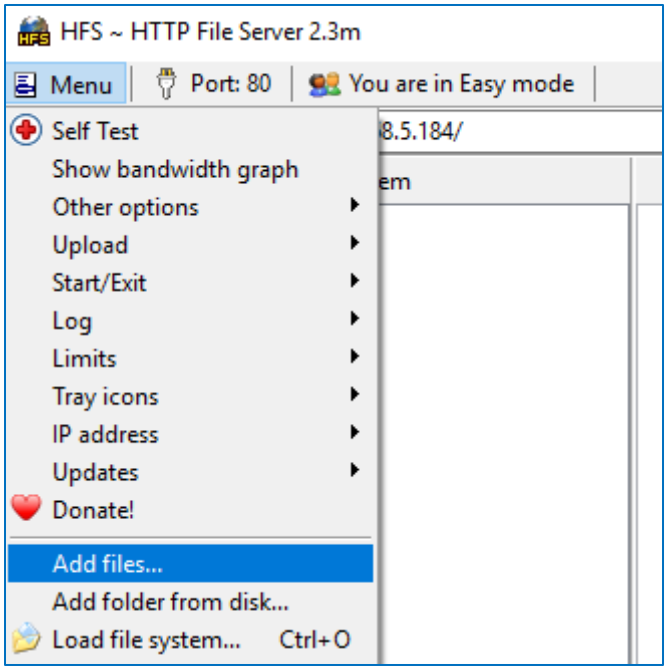

Figure 4: Selecting the firmware file to upload on the HTTP server

4. Select the file(s) and click **Open** to upload the file(s) to your HTTP server.

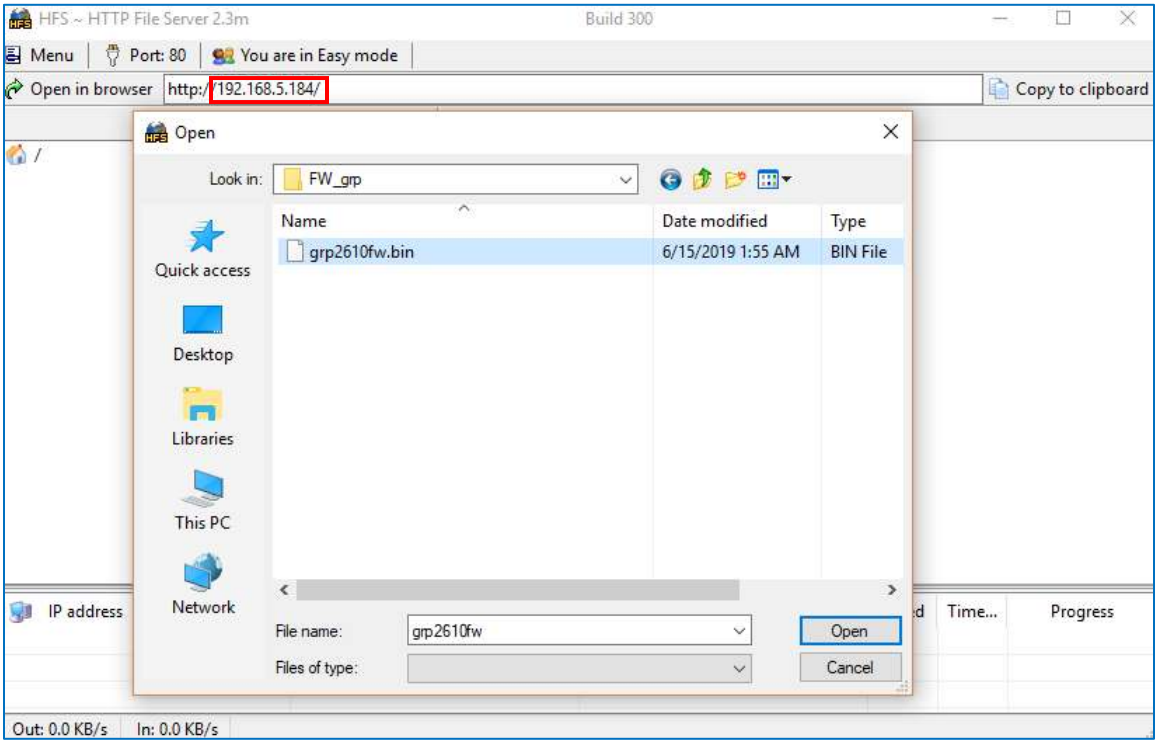

Figure 5: Uploading the firmware file to the HTTP Server

5. Once uploaded to the HTTP server, the firmware file should be available on the link: "*http://192.168.5.184/grp2610fw.bin*" Next to **Open in browser.** As shown on the screenshot:
   - **192.168.5.184** is the IP address of the computer running the local HTTP server

Configuring Grandstream devices for local HTTP upgrade

Configure Grandstream devices to upgrade the firmware via HTTP by doing the following:

1. Access the Web GUI and navigate to "**Upgrade and Provisioning**" page.
2. Set "Firmware Upgrade and Provisioning" to "**Always Check for New Firmware**"
3. Go to "Firmware" section,
   - Select "**HTTP"** for "Firmware Upgrade via"
   - Enter the path (IP address) of your HTTP server containing the firmware file under "Firmware Server Path".
4. Press "**Save and Apply**" at the bottom of the page to apply the new settings
5. Reboot the device and wait until the upgrade process is completed.

Notes:

- In our example, we have configured the firmware server path as: "192.168.5.184".
- Make sure to not include leading http:// in HTTP Firmware server path.
- You can verify the upgrade progress on the HFS Server as shown blow:

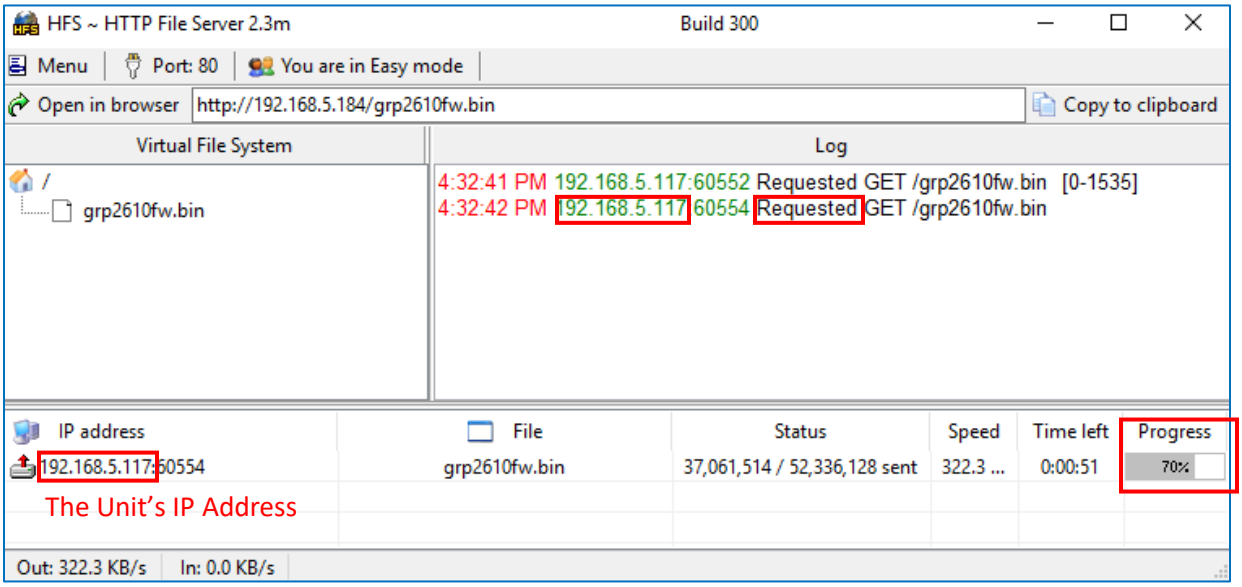

Figure 6: Firmware upgrade progress

- Once completed, a Fully downloaded log will be registered

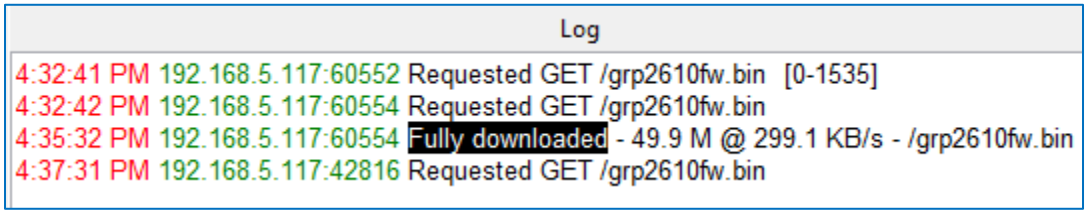

Figure 7: Firmware File Fully Downloaded

Local Upgrade via HTTPS Server

Please refer to the below steps for a local upgrade using XAMPP (with built in HTTPS server)
Download link: https://www.apachefriends.org/download.html

Installing HTTPS Server

1. Download appropriate version depending on your platform.

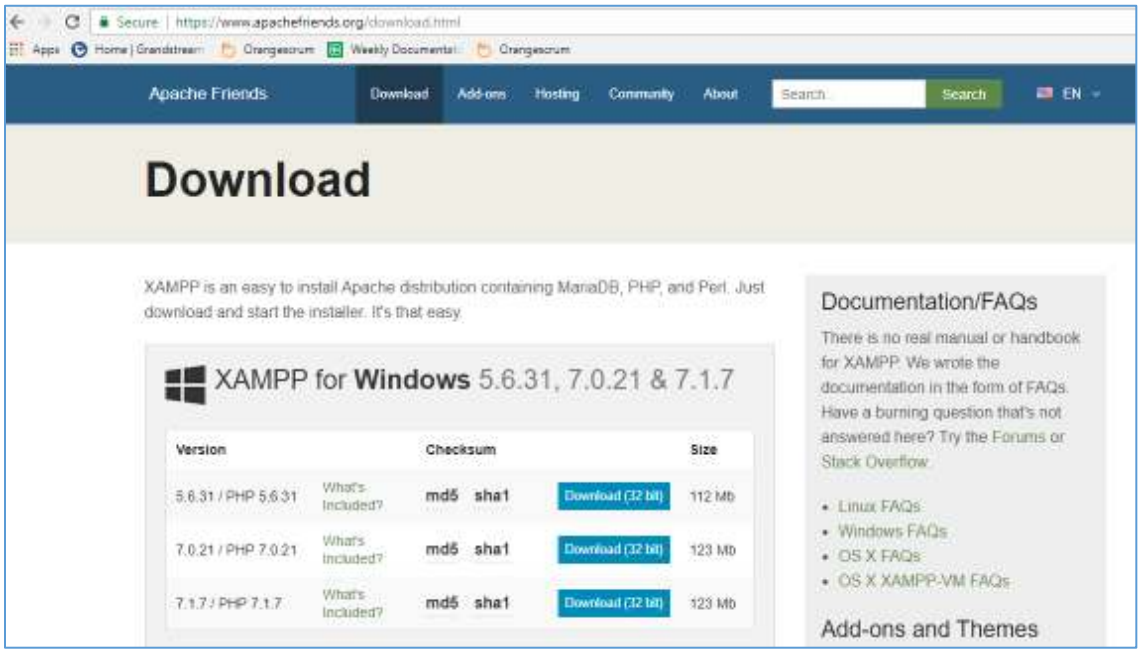

Figure 8: Download XAMPP for windows

2. Launch the install wizard once the file is fully downloaded and follow the installation steps:

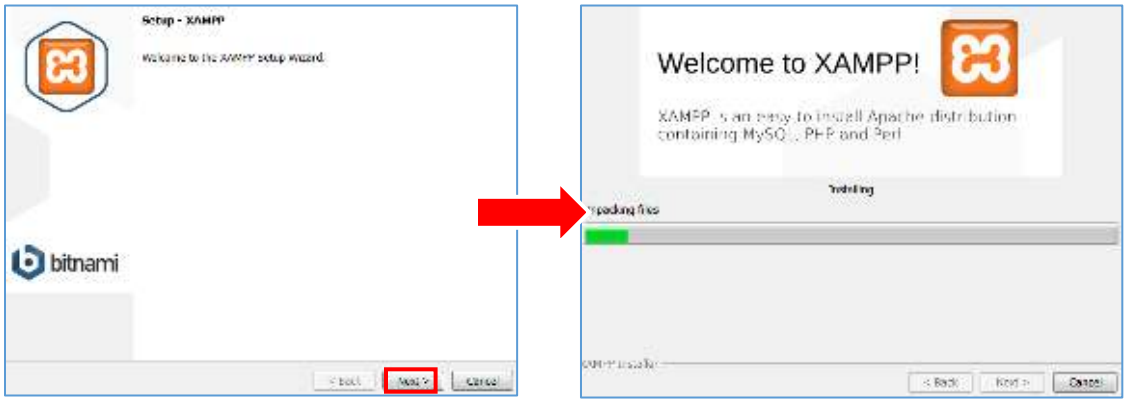

Figure 9: XAMPP Installation

3. Launch the XAMPP server. The following interface will be available:

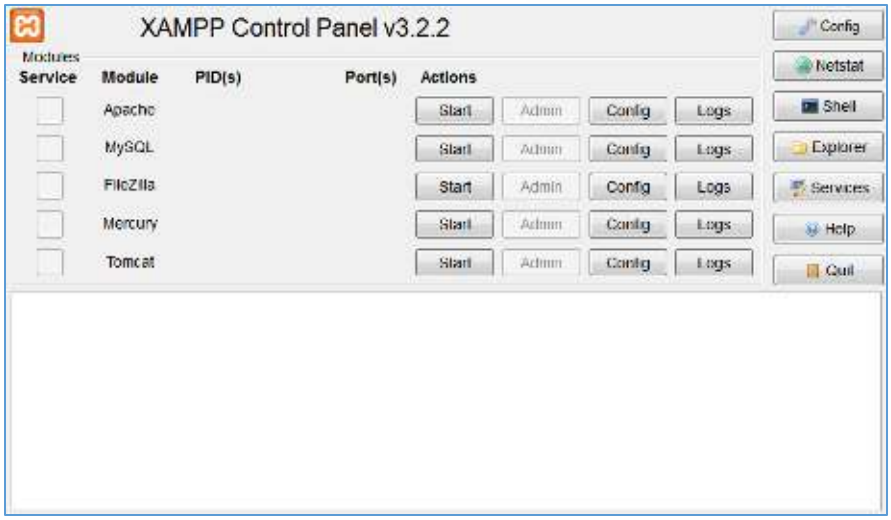

Figure 10: XAMPP Control Panel

Uploading firmware file(s) to XAMPP HTTPS Server

1. Start **Apache** module in order to use the HTTPS server.

Figure 11: Apache Module Started

2. Access the XAMPP root directory on your computer and put the firmware files on the following path: "***C:\xampp\htdocs\xampp***"

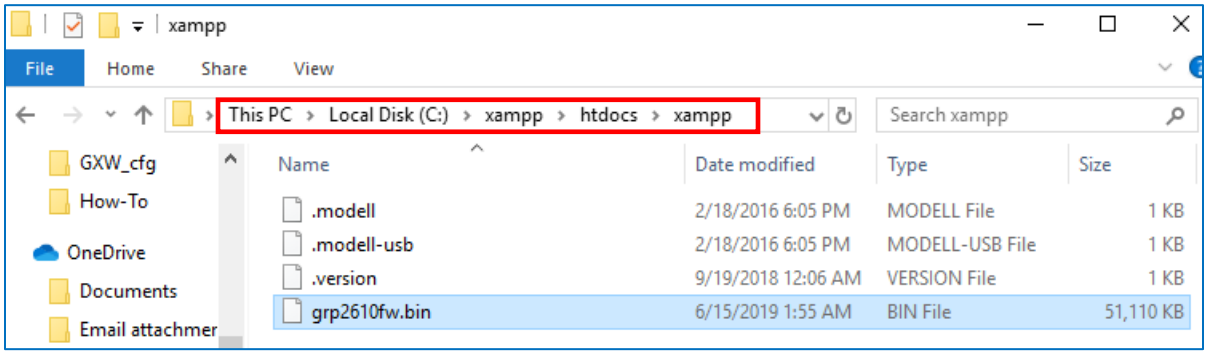

Figure 12: XAMPP Directory

3. To list all available firmware files on the root directory, access the local link address "https://127.0.0.1/xampp/" from the computer running HTTPS server.

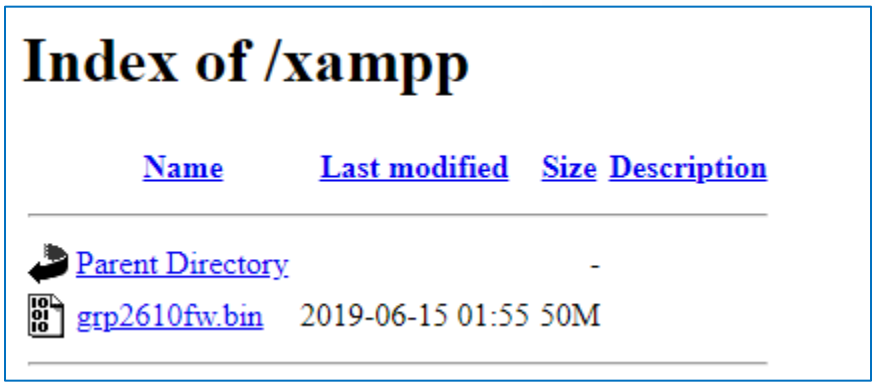

Figure 13: Index of XAMPP Files

Note: XAMPP has a built-in SSL certificates for HTTPS access. Changing the certificates, is possible by a simple copy/paste of the generated certificates on the following folder***: "C:\xampp\apache\conf "***. The folder contains 3 sub directories: ssl.crt, ssl.csr and ssl.key.

Configuring Grandstream devices for a local HTTPS upgrade

Configure Grandstream devices to upgrade the firmware via HTTPS by doing the following:

1. Access the Web GUI and navigate to "**Upgrade and Provisioning**" page.
2. Set "**Firmware Upgrade and Provisioning**" to "**Always Check for New Firmware**"
3. Go to "**Firmware**" section,
   - Select "**HTTPS"** for "**Firmware Upgrade via**"
   - Enter the HTTPS server URL containing the firmware file in "**Firmware Server Path**" field.

   Example: (**x.x.x.x/xampp**) where x.x.x.x is the IP address of computer running XAMPP.
4. Press "**Save and Apply**" at the bottom of the page to apply the new settings
5. **Reboot** the device and wait until the firmware upgrade process is completed.

The following screenshot illustrates the steps mentioned above.

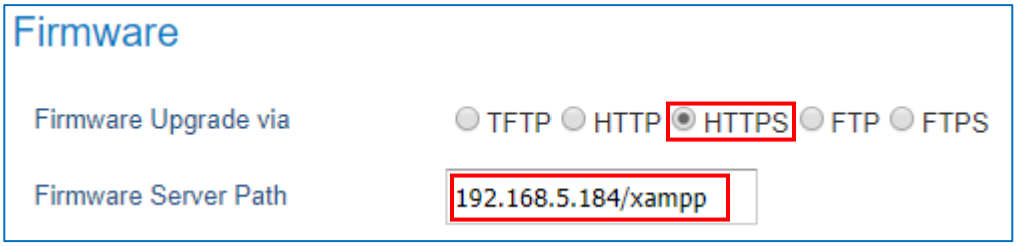

Figure 14: Example of Configuring the Upgrade via HTTPS on GRP26XX

Local Upgrade via TFTP Server

To upgrade locally using TFTP protocol, users can download and install a free TFTP server as described in below steps.

Installing the TFTP Server

A free windows version TFTP server is available for download from following link: http://tftpd32.jounin.net/

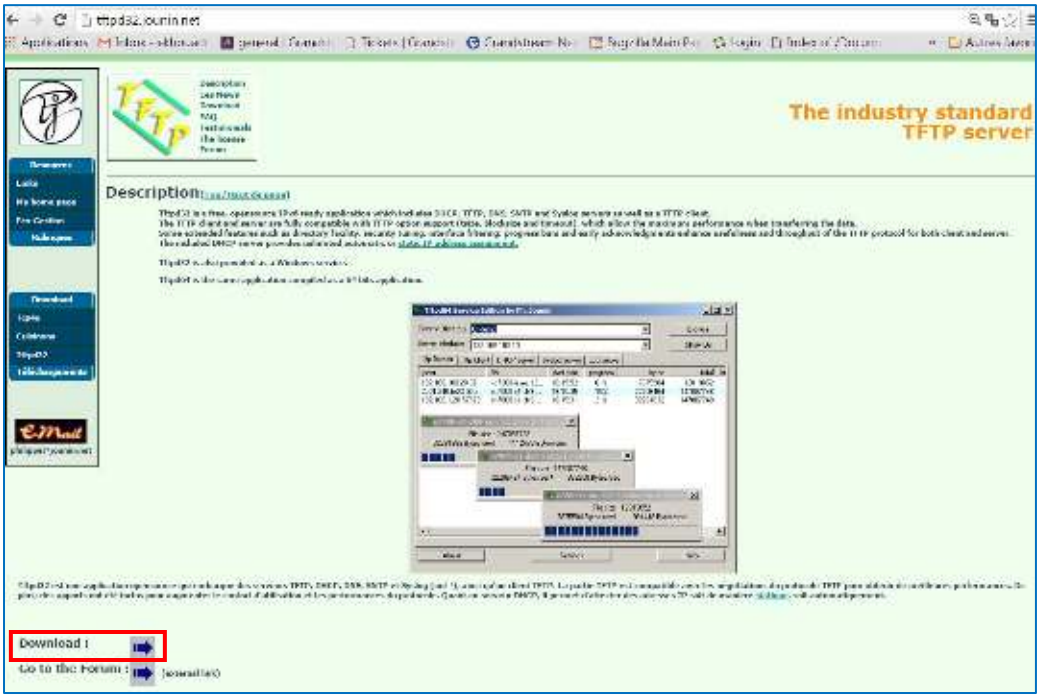

Figure 15: Downloading the TFTP server

1. Select which version is appropriate for your computer, and start downloading it.

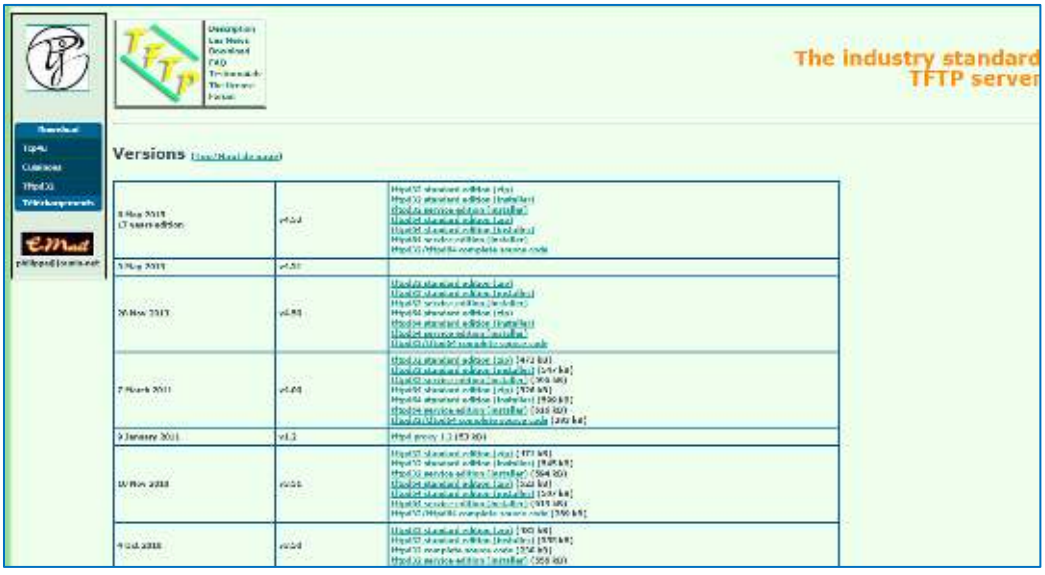

Figure 16: Selecting Install Version

2. Launch the TFTP server install wizard.

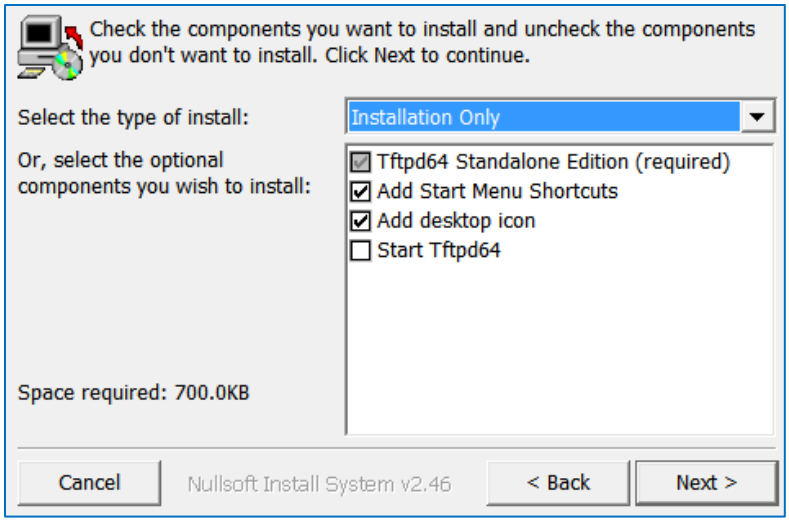

Figure 17: TFTP Server Installation

3. Once the TFTP server is installed, Open TFTPD64. The following interface will be displayed:

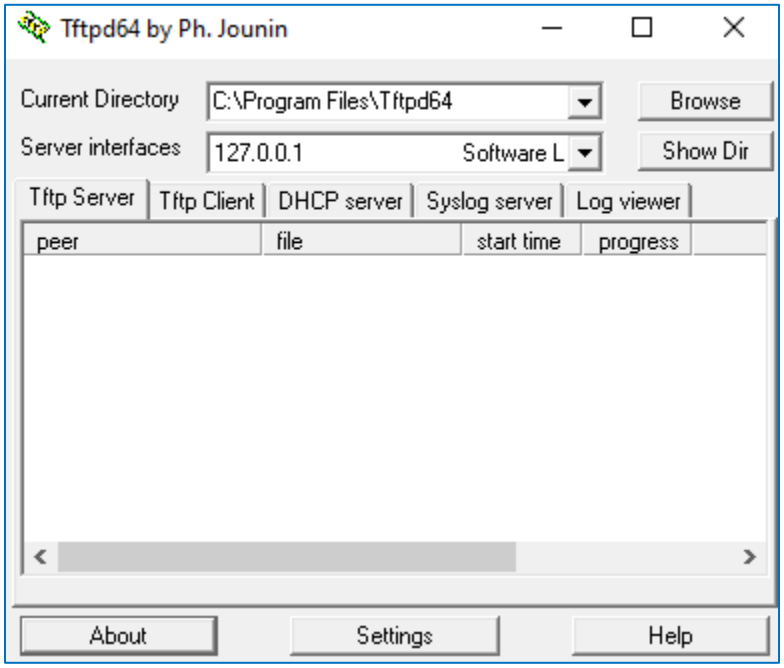

Figure 18: TFTP Server Interface

Uploading the firmware file

1. Make sure that the TFTP service is selected and started under **Settings → Global**
   - Select **"TFTP Server"** then click button **OK** to confirm your configuration.

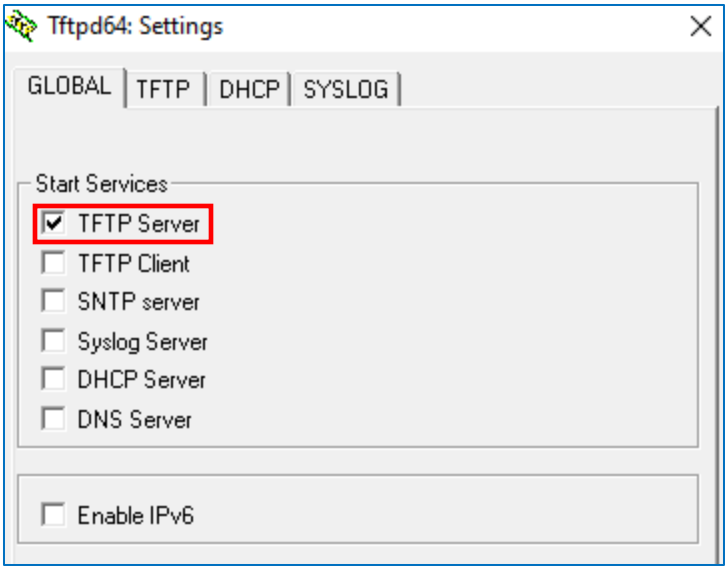

Figure 19: Selecting TFTP Server Services

2. **Browse** to locate and select the required firmware file from your local system.

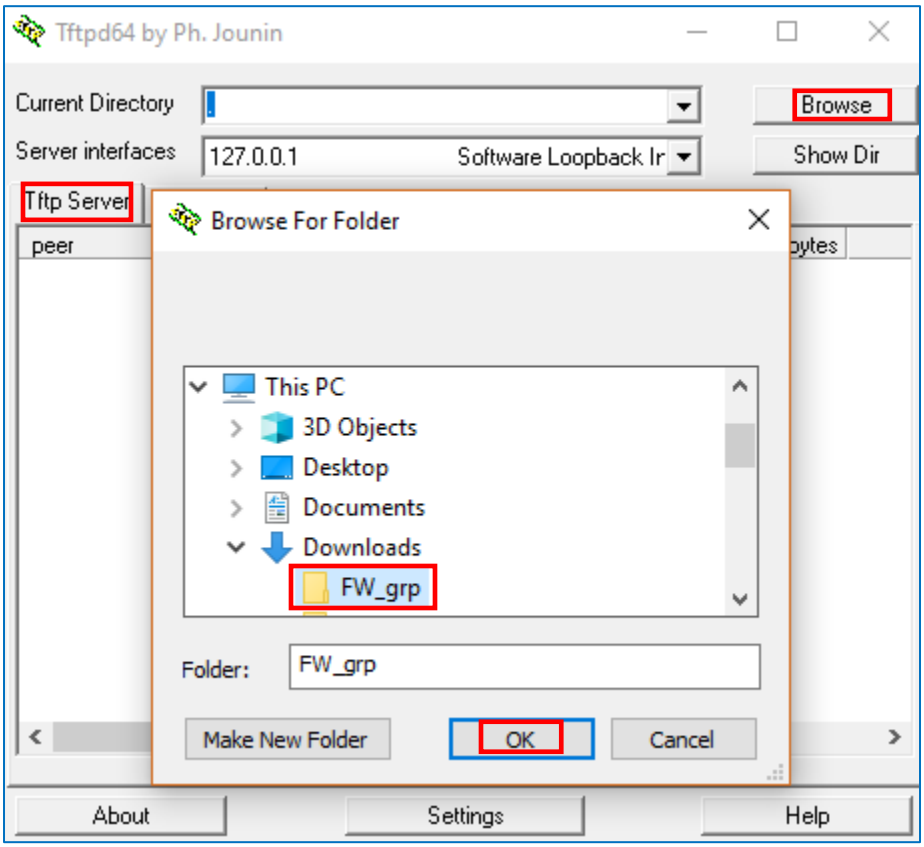

Figure 20: Selecting Local Directory containing Firmware File

3. Press **Show Dir** to see if the firmware file was successfully linked to the TFTP server.

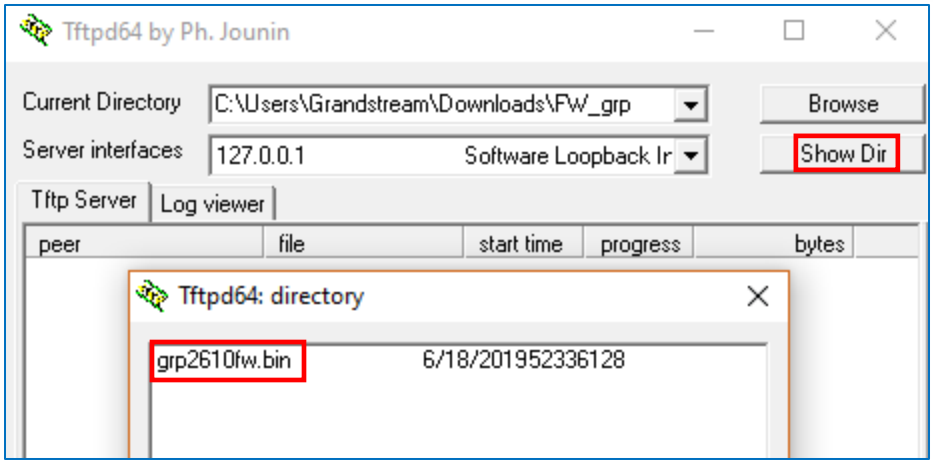

Figure 21: Firmware File Upload Verification

4. Select the interface of the computer running the TFTP server on **Server Interfaces**.

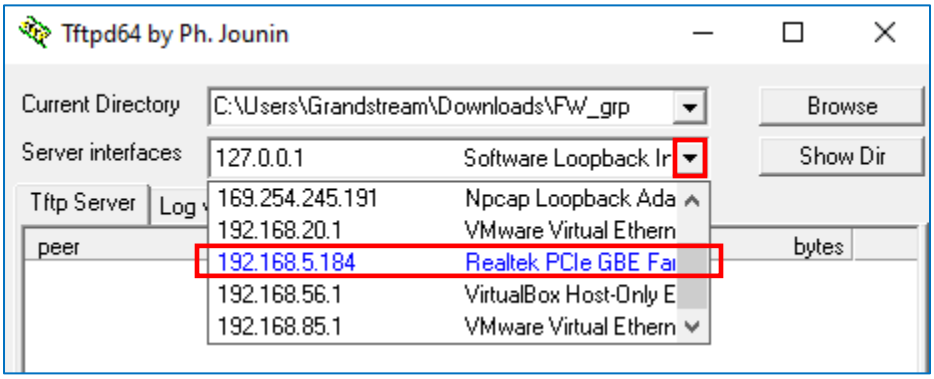

Figure 22: TFTP Server Configuration

Configuring Grandstream devices for local TFTP upgrade

Configure Grandstream devices to upgrade the firmware via HTTPS by doing the following:

1. Access the Web GUI and navigate to "**Upgrade and Provisioning**" page.
2. Set "**Firmware Upgrade and Provisioning**" to "**Always Check for New Firmware**"
3. Go to "**Firmware**" section,
   - Select "**TFTP"** for "**Firmware Upgrade via**"
   - Enter the path of your TFTP server containing the firmware file under "**Firmware Server Path**"
4. Press "**Save and Apply**" at the bottom of the page to apply the new settings
5. **Reboot** the phone and wait until the upgrade process is completed.

ADVANCED OPTIONS

Automatic Upgrade

Automatic Upgrade allows to periodically check if a newer firmware is available to download and upgrade the device. This option will help to keep the devices up-to-date. It can be enabled from **web GUI → Maintenance → Upgrade and provisioning** page.

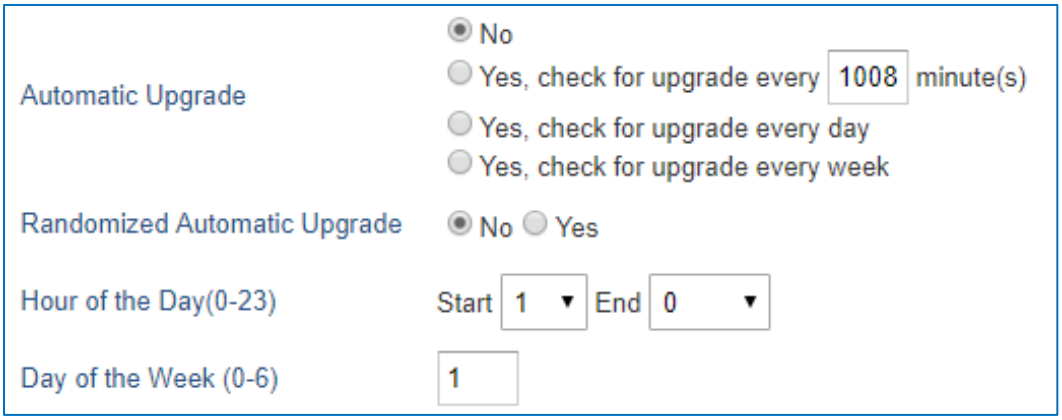

Figure 23: Example of Configuring Automatic Upgrade on GRP26XX

The automatic upgrade can be configured based on following parameters:

- Every [Time interval] in minute(s)
- Every day ("Hour of the Day" should be configured)
- Every week ("Hour of the Day" and "Day of the Week" should be configured, 0 is Sunday)

The device will check the firmware file availability in the specified time interval. If found, it will be downloaded and the upgrade process will be initiated automatically.

Firmware File Prefix and Postfix

Firmware prefix and postfix are two options which can be configured by users to lock the firmware update, then only the firmware with the matching prefix and/or postfix will be downloaded and flashed into phone.

Firmware file prefix and postfix can be configured from **Web GUI → Maintenance → Upgrade and provisioning**.

Figure 24: Screenshot of Firmware file Prefix and Postfix fields

Use Case Example:

Using firmware prefix and postfix, users store different firmware versions in same folder and only upgrade to specific version.

- If **Firmware File Prefix** is set to *1.0.0.31* on a GRP20XX series phone, for example, requested firmware file will be *1.0.0.31grp2610fw.bin*

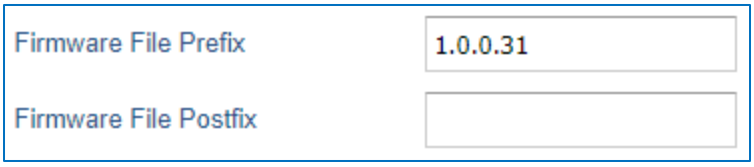

Figure 25: Configuring the Firmware File Prefix

- If **Firmware File Postfix** is set to *1.0.0.16* on a GRP20XX series phone, for example, requested firmware file will be *grp2610fw1.0.0.16.bin*

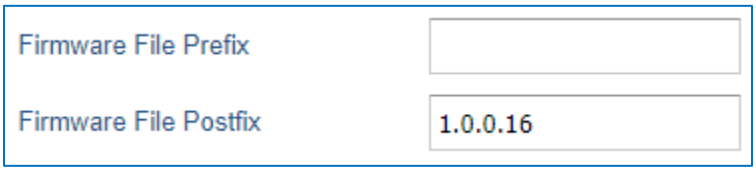

Figure 26: Configuring the Firmware File Postfix

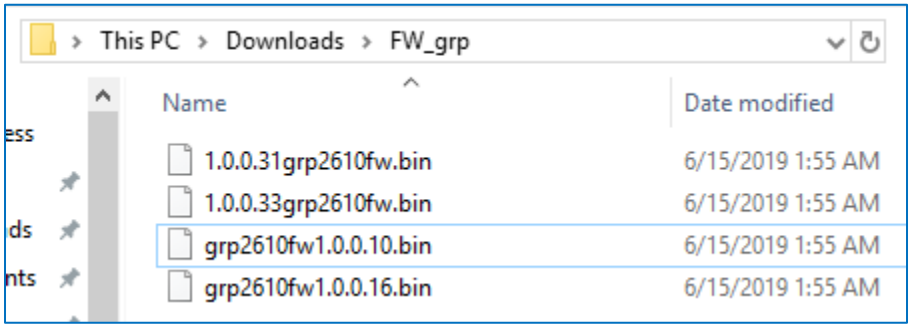

Figure 27: Firmware Files with Prefix/Postfix on local directory

HTTP/HTTPS User Name and Password

HTTP/HTTPS User Name and Password need to be configured if HTTP/HTTPS server requires authentication to access and download firmware files.

To begin firmware upgrade process, the phone sends an initial request to download firmware files from the server, the request will be challenged by the server to provide valid credentials, the phone sends same request including configured HTTP/HTTPS User Name and Password, if accepted, firmware upgrade process can start.

If **Always Authenticate Before Challenge** is set to "Yes", the phone includes configured credentials in initial request to download firmware files before being challenged by the server. The default setting is "No".

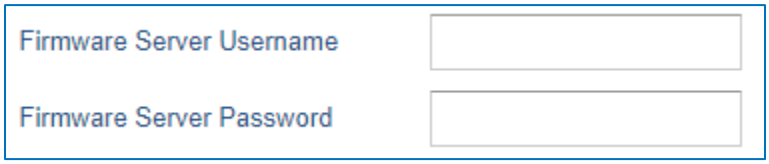

Figure 28: Screenshot of HTTP / HTTPS Username and Password Fields