Grandstream Networks, Inc.

Firmware Upgrade Guide

Table of Content

Firmware Upgrade Guide

Table of Figures

Firmware Upgrade Guide

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_GXP16xx_1.0.3.28.zip* and *Release_Note_GXP16xx_1.0.3.28.pdf* are specific to GXP16XX Small Business IP Phones series.

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 Grandstream devices firmware version and covers following scenarios:

- **Scenario 1:** Upgrade using Grandstream Public HTTP Server.
- **Scenario 2:** Upgrade using local HTTP/HTTPS/TFTP 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 settings page**

2. Make sure to select "**Always Check for New Firmware**".

3. Under "Firmware", Select Upgrade **via HTTP**.

4. Enter "**firmware.grandstream.com**" under **Firmware Server Path**.

5. Press **Save and Apply** button to apply the new settings.

6. **Reboot** the device and wait until the upgrade process is completed.

Notes:
- To upgrade using Grandstream HTTP server, the device needs to be connected to Internet.
- To upgrade to BETA firmware (if available), use "firmware.grandstream.com/BETA" in step 4.

Scenario 2: Upgrade using Local HTTP/ HTTPS/TFTP Server

Customers can use their own HTTP, HTTPS 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 needs 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.

Firmware Upgrade Guide

Local Upgrade via HTTP Server

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

Installing HTTP Server and Uploading Firmware File(s)

Please refer to following steps in order to download / install the HTTP server and upload the firmware:

1. Launch the install of the tool once it's fully downloaded from the following link:

   " http://www.rejetto.com/hfs/download "

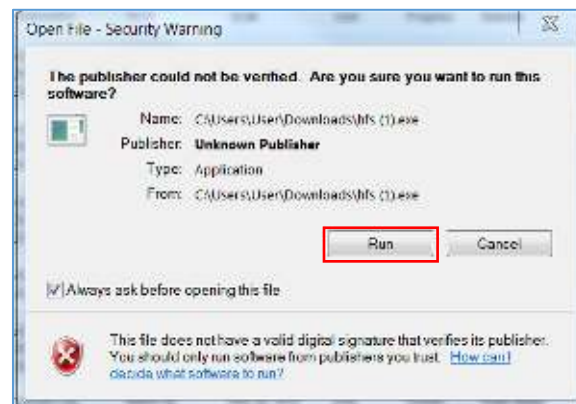2. Click on **Run** to launch the HTTP server.

Figure 1: Starting the HTTP server

3. Start the HFS server, browse to locate and select the required firmware files from your local directories under **Menu** options → **Add files**.
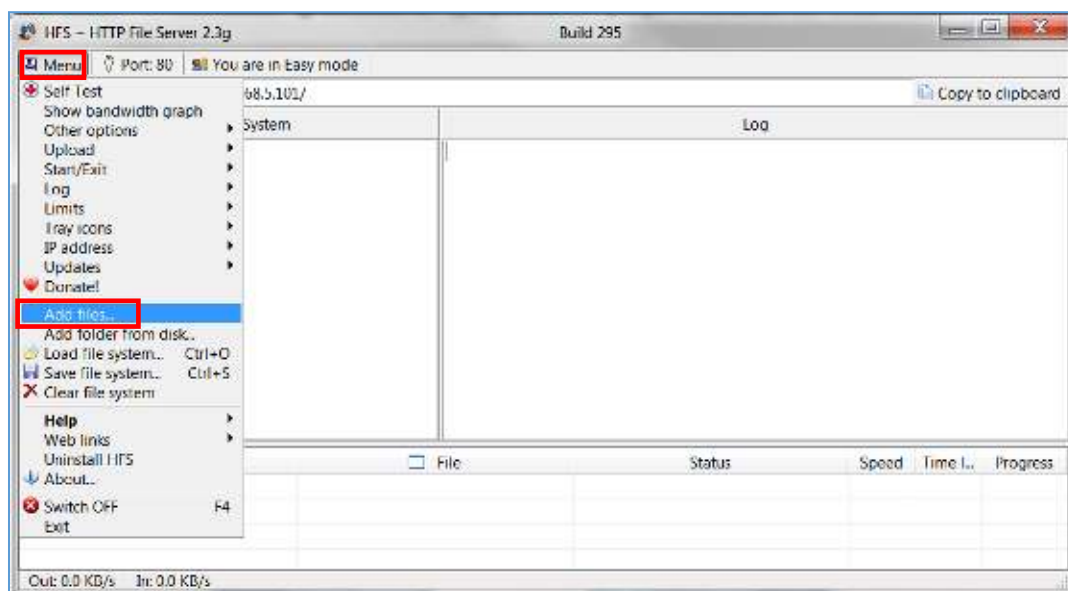

Figure 2: Selecting the firmware file to upload on the HTTP server

4. Choose from your local directory where the firmware files are downloaded and click **Open** to upload the file(s) to your HTTP server.
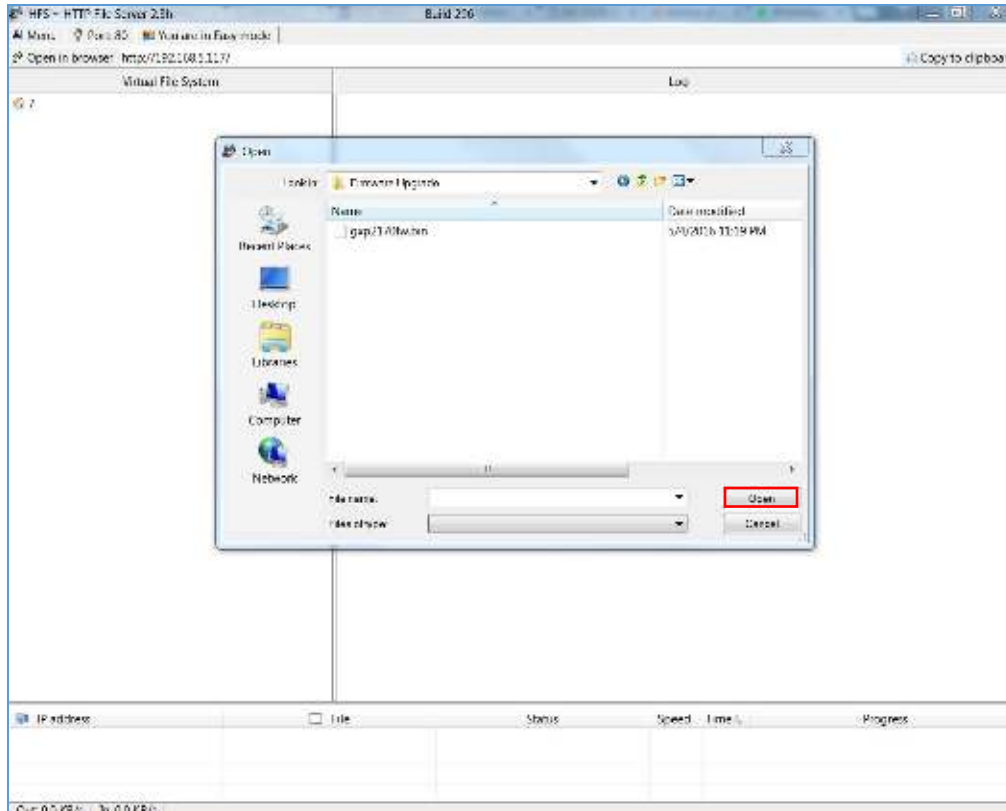

Firmware Upgrade Guide

Figure 3: Uploading the firmware file to the HTTP Server

5. Once uploaded to the HTTP server, the firmware file will be available. In our example, on the following link: "192.168.5.101/gxp2170fw.bin" as shown on the screenshot below (where 192.168.5.101 is the IP address of the computer running the local HTTP server).
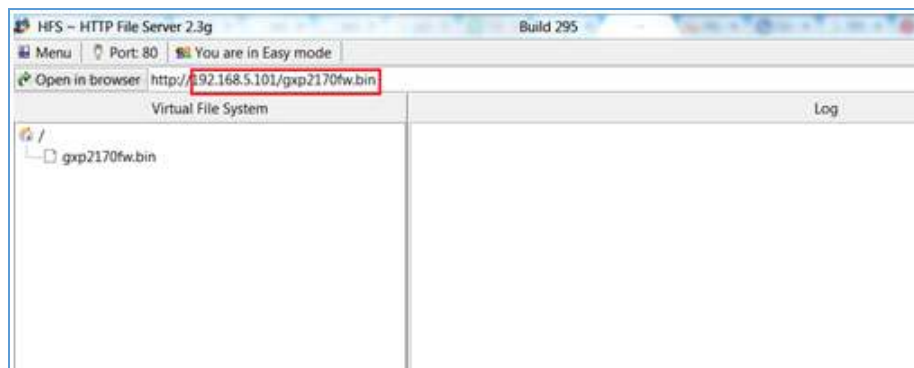

Figure 4: Firmware server path hosting the firmware file

Configuring Grandstream devices for local HTTP upgrade

Please refer to following steps to configure Grandstream devices to upgrade the firmware:

1. Access the web GUI of your device and navigate to "**Upgrade and Provisioning**" settings.

2. Make sure to select "**Always Check for New Firmware**".

Firmware Upgrade Guide

3. Select **Upgrade via HTTP**

4. Enter the path of your HTTP server containing the firmware file under Firmware Server Path.

   Notes:
   - In our example, we have configured the firmware server path as: "192.168.5.101".
   - Make sure to not include leading **http://** in HTTP Firmware server path.

5. Press **Save and Apply** at the bottom of the page to apply the new settings

6. **Reboot** the device and wait until the upgrade process is completed.

You can also verify the status of the upgrade progress on the HFS Server as displayed on the following screenshots:
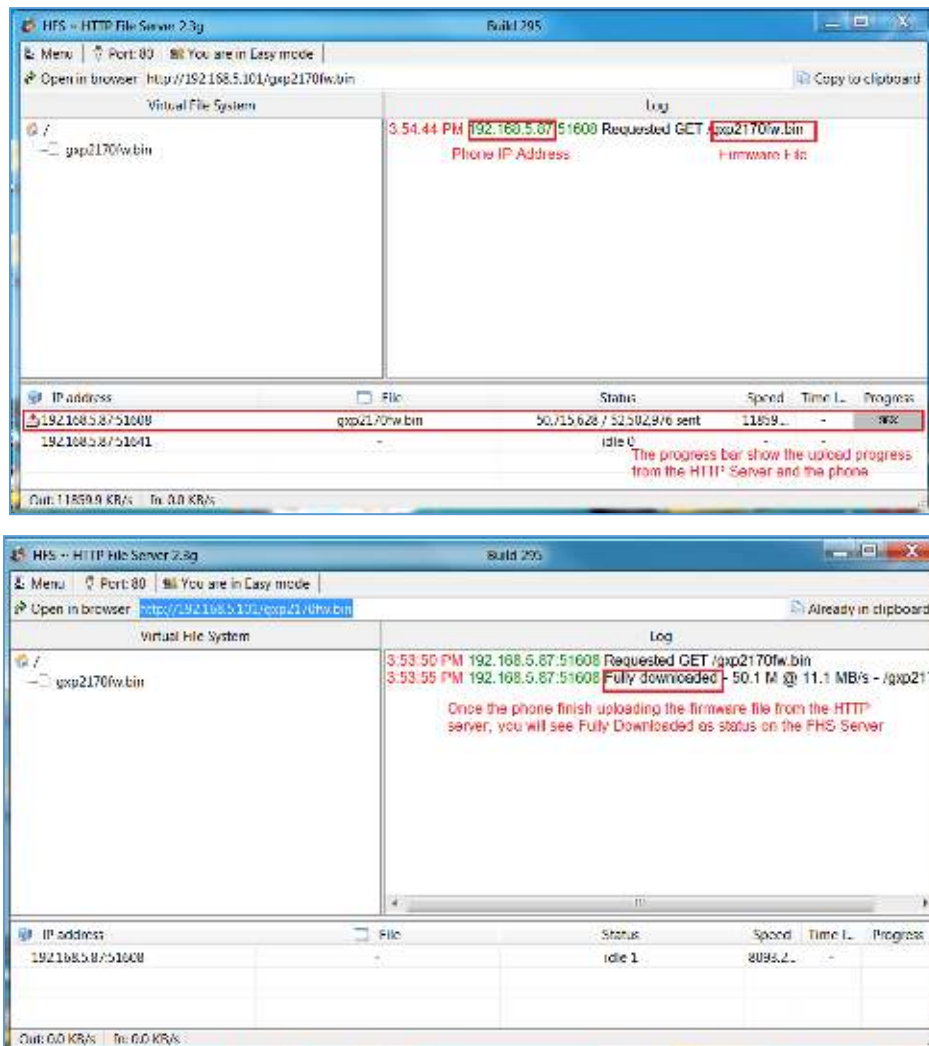

Figure 5: Status of firmware upgrade progress

Local Upgrade via HTTPS Server

Please refer to steps below for the local upgrade using **HTTPS**.

XAMPP with built in HTTPS server is available in this link (https://www.apachefriends.org/download.html) and can be used.

Firmware Upgrade Guide

Installing HTTPS Server

1. Download appropriate version depending on your platform.

Figure 6: Download XAMPP for windows

2. Launch the install of the XAMPP server once it's fully downloaded and follow the installation steps by clicking on **Next** button.
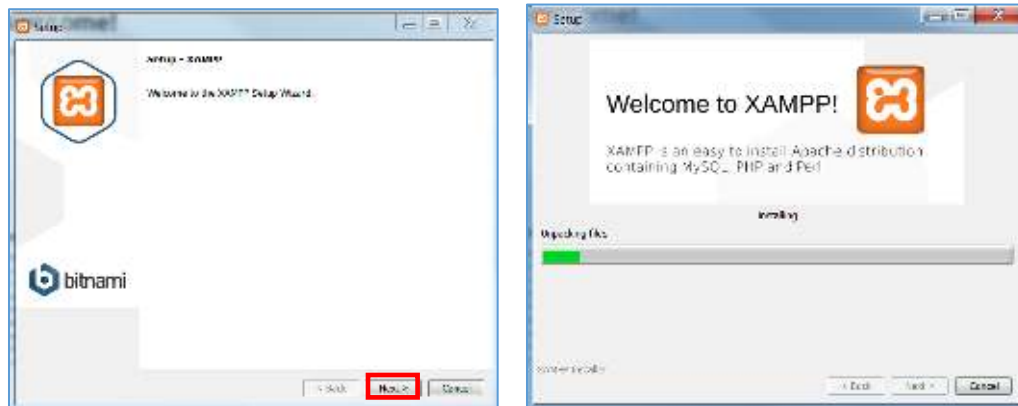

Figure 7: XAMPP Installation Steps

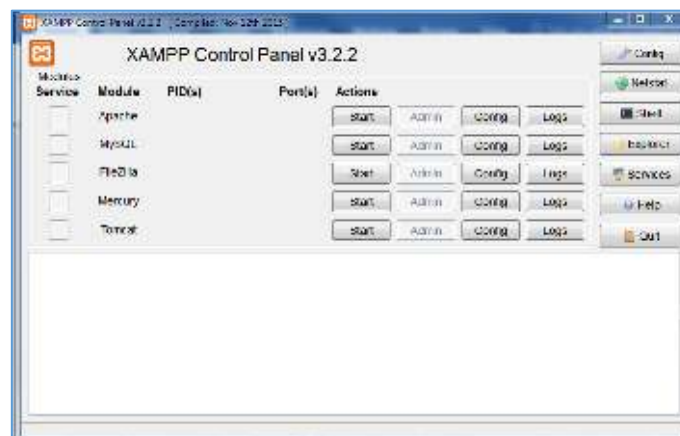3. Launch the XAMPP server. Following interface will be available.

Figure 8: XAMPP Control Panel

Firmware Upgrade Guide

Uploading firmware file(s) to XAMPP HTTPS Server

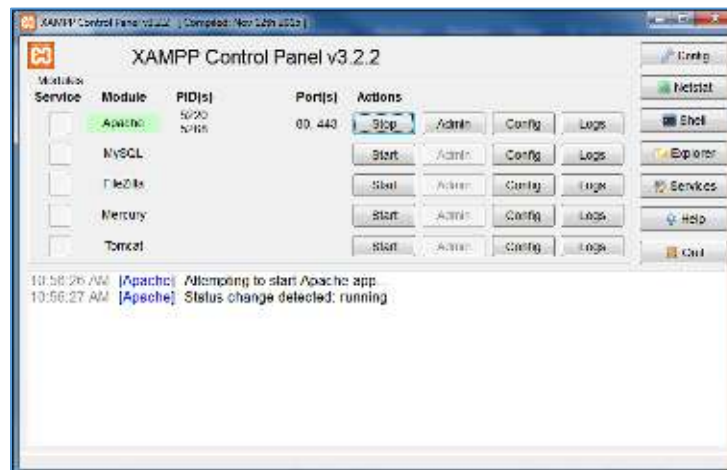1. Start **Apache** module in order to use the HTTPS server.

Figure 9: Apache Module Started

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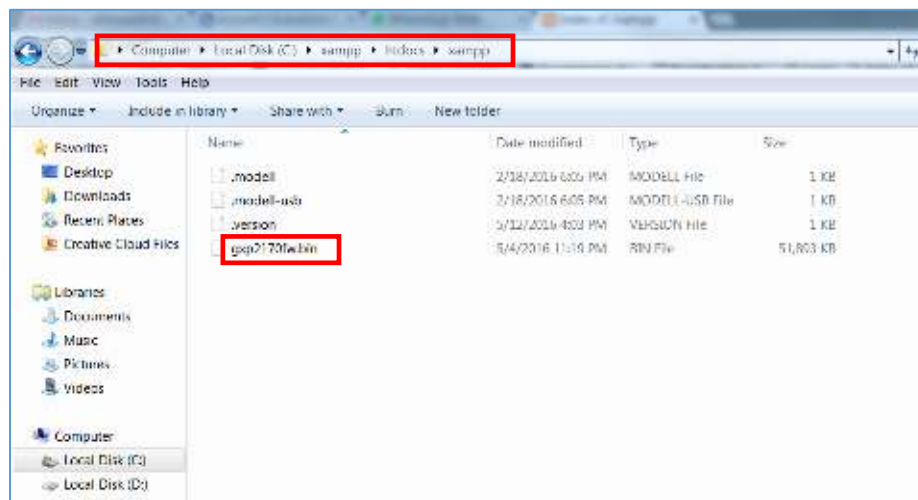

Figure 10: XAMPP Directory

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

Figure 11: Index of XAMPP Files

Note: XAMPP has a built-in SSL certificates for HTTPS access, if users need to change the certificates, this can be done by copy/paste generated certificates on the following folder: **"C:\xampp\apache\conf "**. This folder contains 3 sub directories (ssl.crt, ssl.csr, ssl.key) where to put SSL certificates.

Configuring Grandstream devices for a local HTTPS upgrade

Please refer to following steps to configure Grandstream devices to upgrade the firmware:

1. Access the web GUI of your device and navigate to "**Upgrade and Provisioning**" settings:
2. Make sure to select "**Always Check for New Firmware**".
3. Select **Upgrade via HTTPS**.
4. Enter 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.
5. Press "**Save and Apply**" at the bottom of the page to apply the new settings
6. **Reboot** the device and wait until firmware upgrade process is completed.

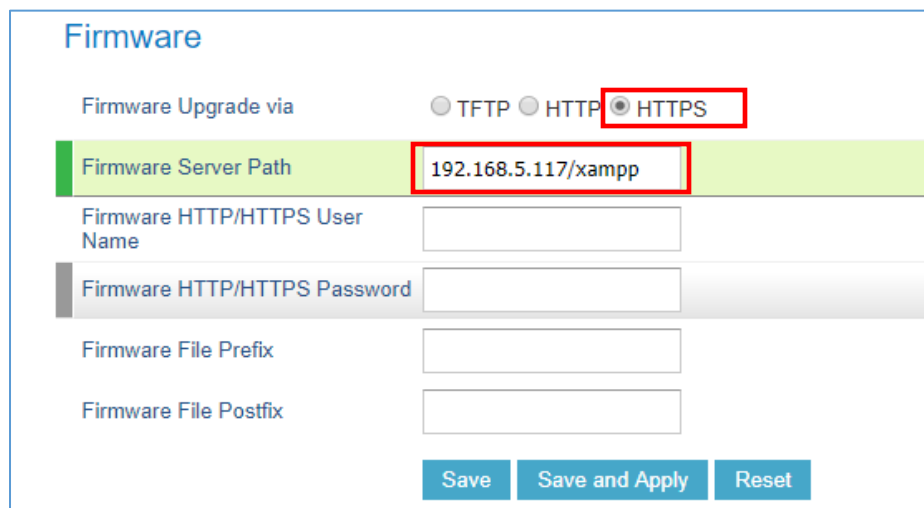The following screenshot illustrates the steps mentioned above.

Figure 12: Example of Configuring the Upgrade via HTTPS on GXP2170

Firmware Upgrade Guide

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

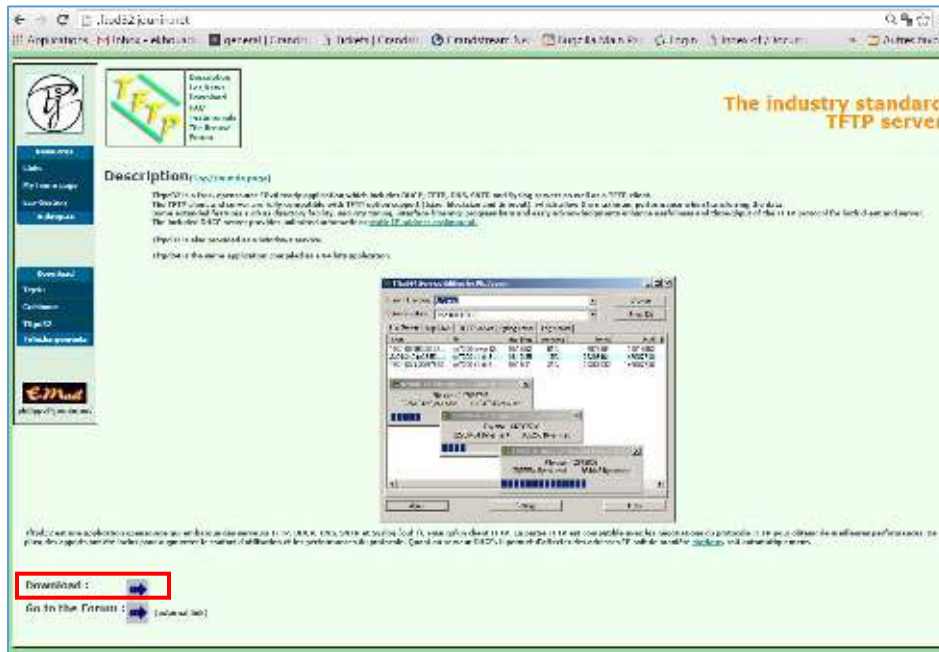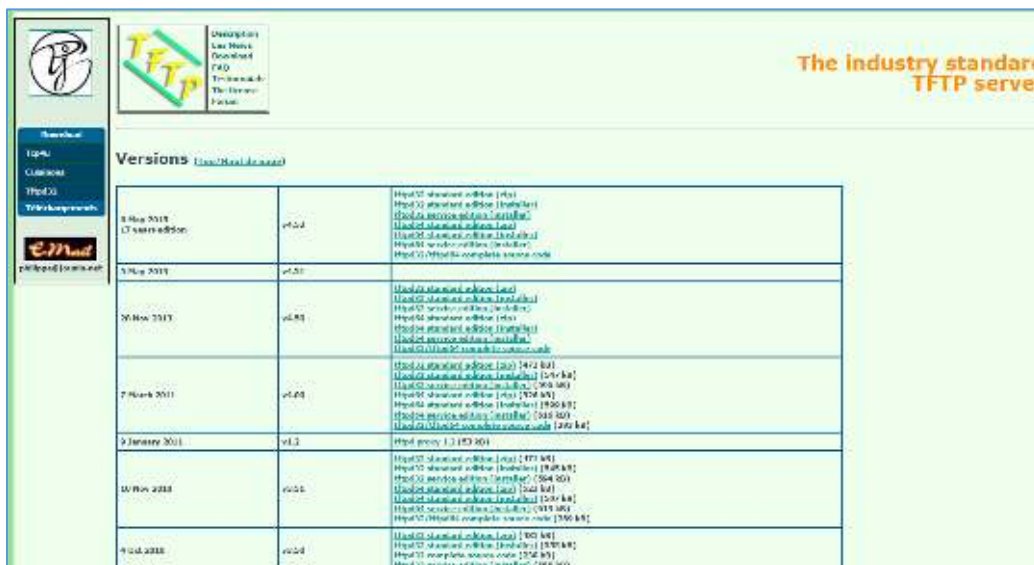A free windows version TFTP server is available for download from following link: http://tftpd32.jounin.net/

Figure 13: Downloading the TFTP server

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

Figure 14: Selecting Install Version

Firmware Upgrade Guide

2. Launch the TFTP server install and click on "next" buttons to continue the installation.
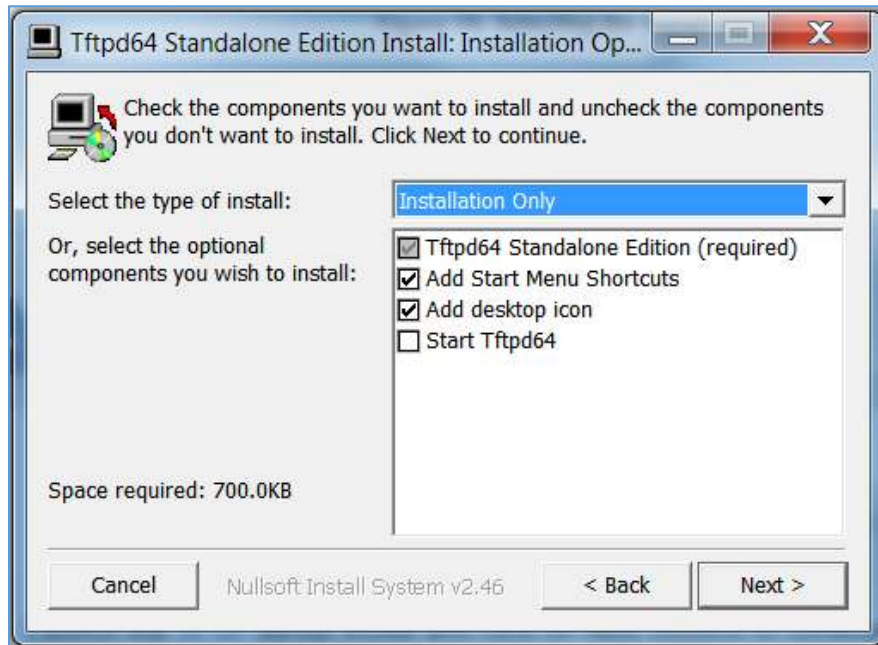

Figure 15: TFTP Server Installation

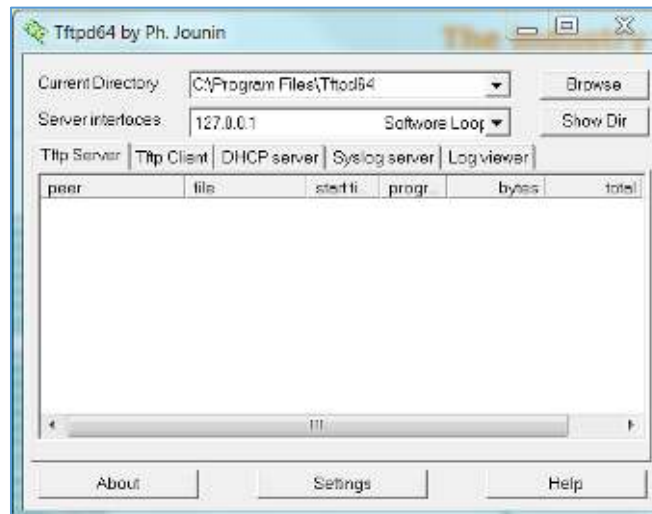3. Once the TFTP server is installed, the following interface will be displayed.

Figure 16: TFTP Server Interface

Uploading the firmware file

1. Make sure that the TFTP services are selected and started under **Settings → Global** and click button **OK** to confirm your configuration.
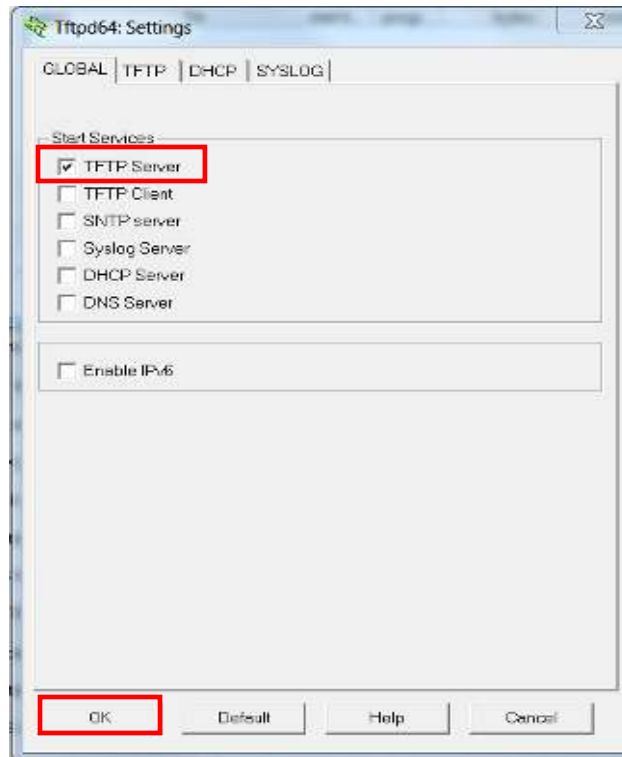
Firmware Upgrade Guide

Figure 17: Selecting TFTP Server Services

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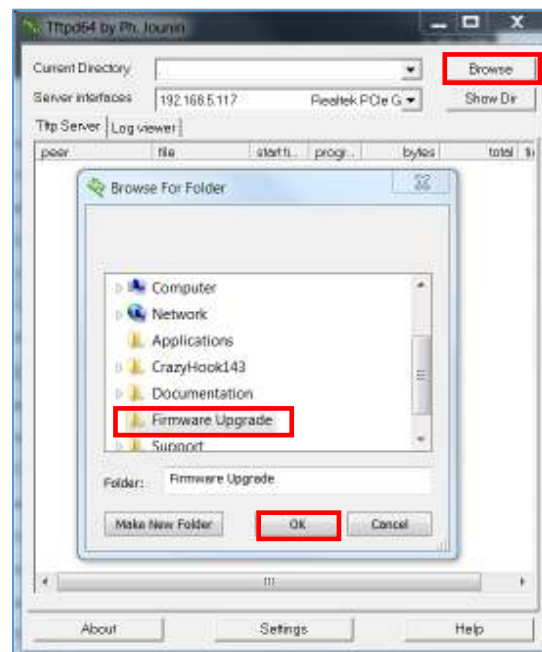

Figure 18: Selecting Local Directory containing Firmware File

3. Press **Show Dir** to see if the firmware file is uploaded on the TFTP server.
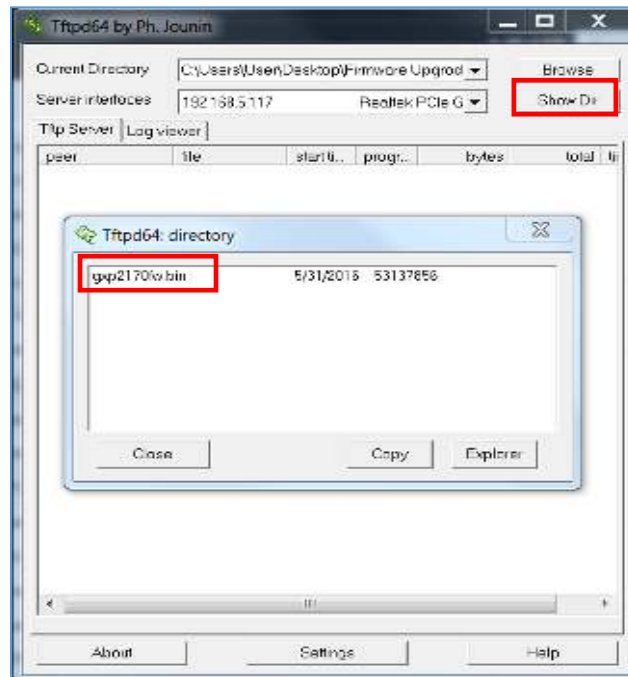

Figure 19: Firmware File Upload Verification

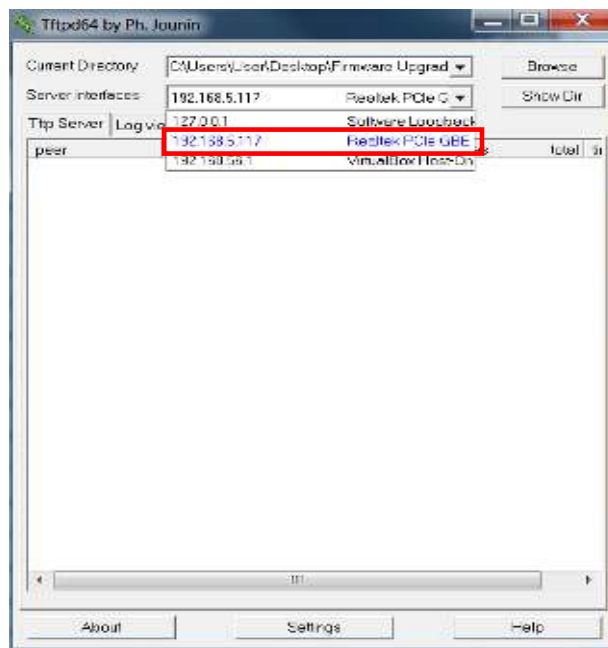4. Select the interface of the computer running the TFTP server on **Server Interfaces**.

Figure 20: TFTP Server Configuration

Configuring Grandstream devices for local TFTP upgrade

Now you need to configure your Grandstream devices for upgrading via your TFTP server, for this you need to follow the steps below:

1- Access the web GUI of your device and navigate to "**Upgrade and Provisioning**" settings:

2- Make sure to select "**Always Check for New Firmware**"

3- Select Upgrade via **TFTP**

4- Enter the path of your TFTP server containing the firmware file under "Firmware Server Path"

5- Press "**Save and Apply**" at the bottom of the page to apply the new settings

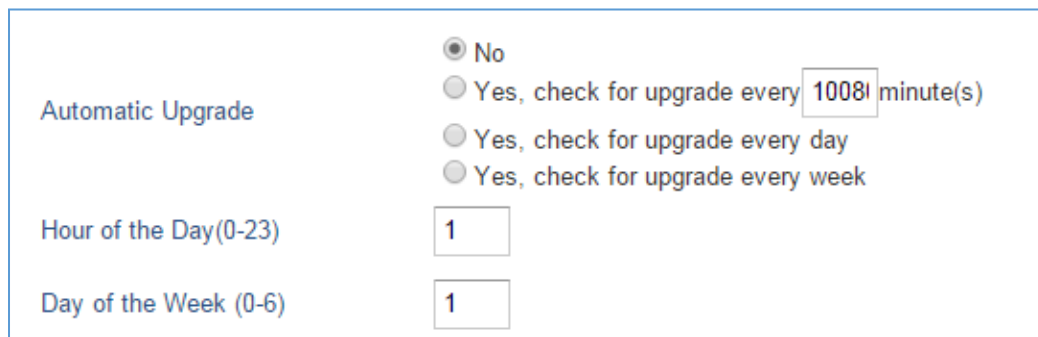6- **Reboot** the phone and until the upgrade process is completed.

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.

Automatic Upgrade can be enabled from web configuration interface → **Upgrade and provisioning** settings.

Figure 21: Example of Configuring Automatic Upgrade on GXP21xx

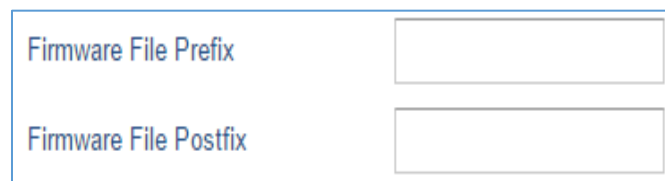The automatic upgrade can be configured based on following options:

- Every 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)

If the firmware is available, it will be downloaded and the device will be upgraded 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 22: 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 upgrade to specific version.

- If **Firmware File Prefix** is set to *1.0.3.14* on GXP1600 series phone, for example, requested firmware file will be *1.0.3.14gxp1600fw.bin*

Firmware File Prefix	1.0.3.14
Firmware File Postfix	

Figure 23: Configuring the Firmware File Prefix

- If **Firmware File Postfix** is set to *1.0.2.22* on GXP1600 series phone, for example, requested firmware file will be *gxp1600fw.bin1.0.2.22*

Firmware File Prefix	
Firmware File Postfix	1.0.2.22

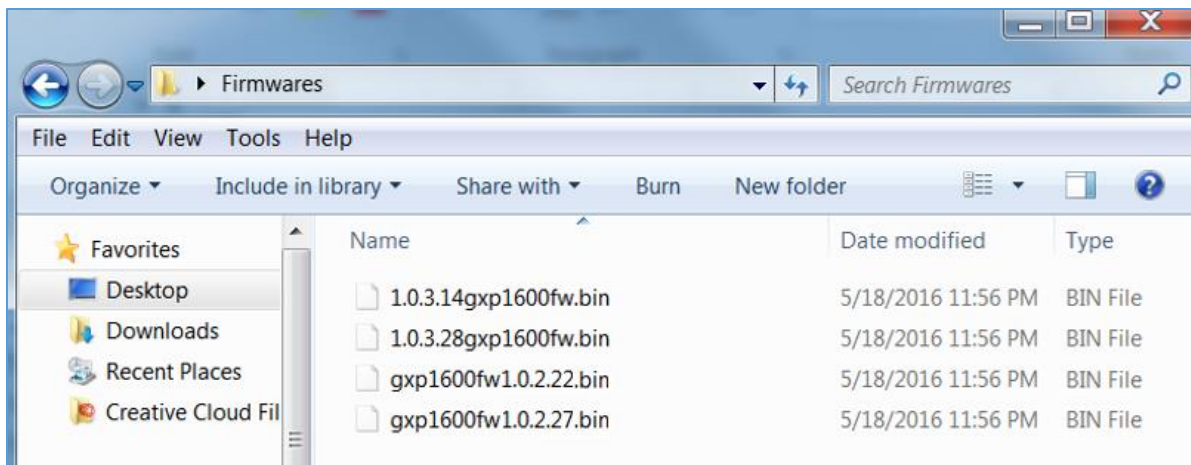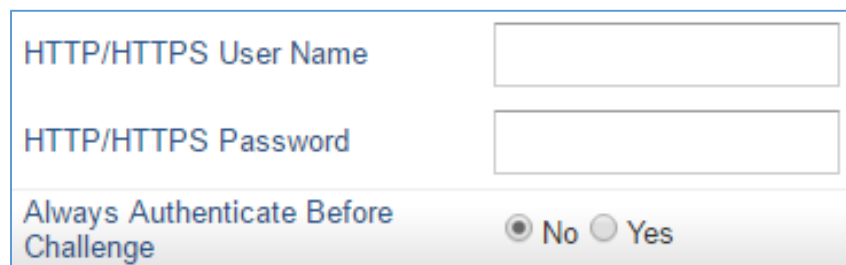**Figure 24: Configuring the Firmware File Postfix**

Figure 25: Firmware Files with Prefix/Postfix Values

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 26: Screenshot of HTTP / HTTPS Username and Password Fields