Grandstream Networks, Inc.

Firmware Upgrade Guide

Overview

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 device up-to-date by upgrading their firmware versions regularly.

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

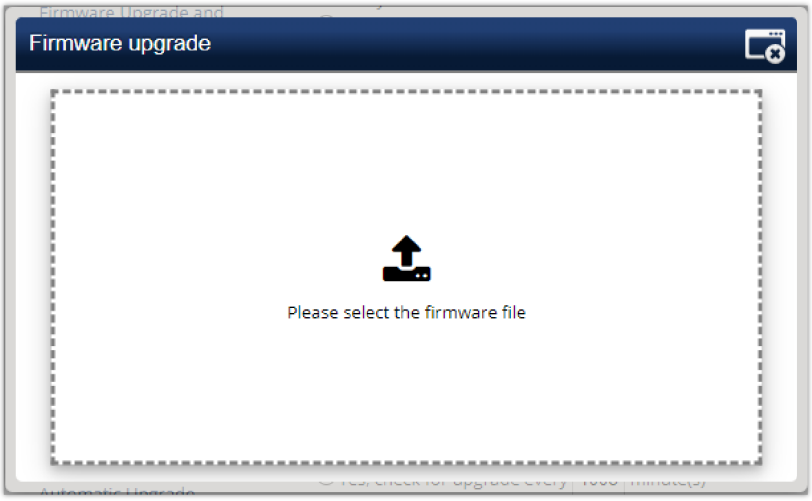
- **Scenario 1:** Upgrade using the device's web UI to upload the firmware file.
- **Scenario 2:** Upgrade using Grandstream Public HTTP Server.
- **Scenario 3:** Upgrade using local HTTP/HTTPS/TFTP/FTP/FTPS Server.

Scenario 1: Upgrade using the device's web UI to upload the firmware fil

Users can directly download new firmware files found on the official Grandstream firmware page, the page can be accessed via the link: https://www.grandstream.com/support/firmware

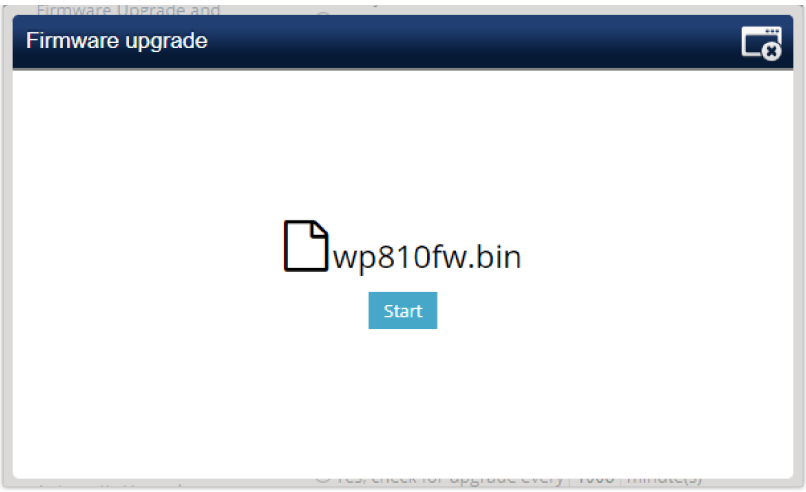
After the firmware file is downloaded, it can be uploaded directly to the Device's web UI under the Upgrade and provisioning section, depend on the specific model, the WEB UI layout might differ, but the concept of uploading the file on the web GUI is the same, we will take an examp on how to upload a new firmware on the Wi-Fi Phone WP810:

1. Access the WEB UI of the WP810
2. Go to **Maintenance => Upgrade and Provisioning => Upgrade Firmware**
3. Click on Start to upload the firmware file in .bin format.
4. Either drag the firmware file to the firmware upgrade pop-up or click on it to upload the firmware file.



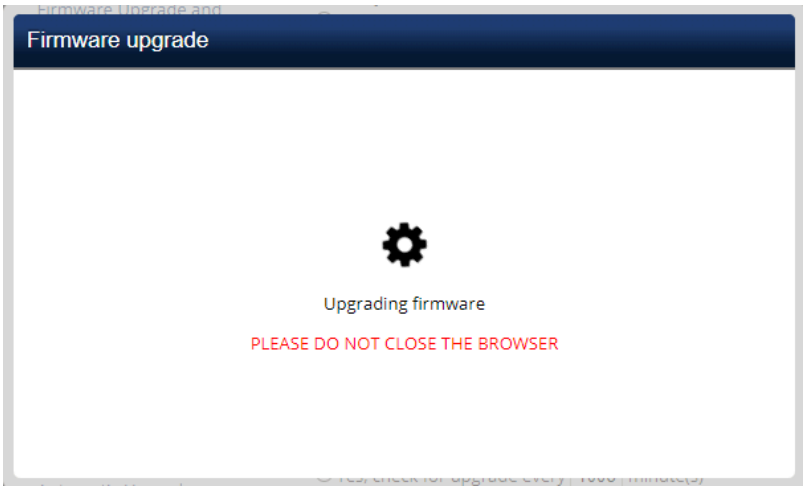
Example of Manual Firmware Upgrade for WP810

5. After the firmware file is uploaded, click again on Start to start the firmware upgrade process.



Starting Manual Firmware Upgrade for WP810

6. Once you click Start , a confirmation pop-up will be displayed on the WP810 LCD, click on "Yes" to confirm, after this the firmware will uploading with the following message displayed on the Web UI



Manual Upgrade In Progress for WP810

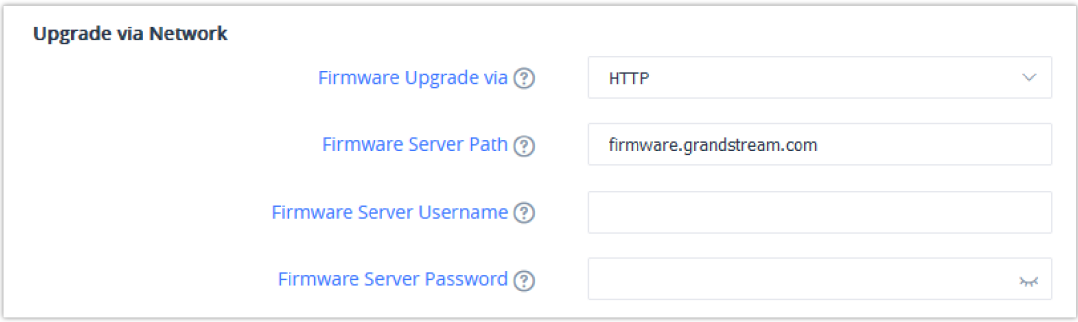
After the firmware is successfully uploaded the device will restart with the new firmware.

Scenario 2: 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 the web interface of your device and go to the **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 3: Upgrade using Local HTTP/ HTTPS/TFTP/FTP/FTPS 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.

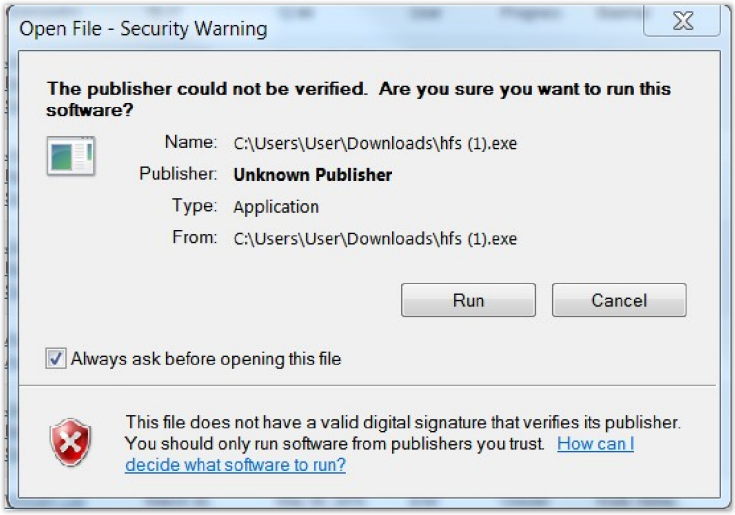
Local Upgrade via HTTP Server

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

Installing HTTP Server and Uploading Firmware File(s)

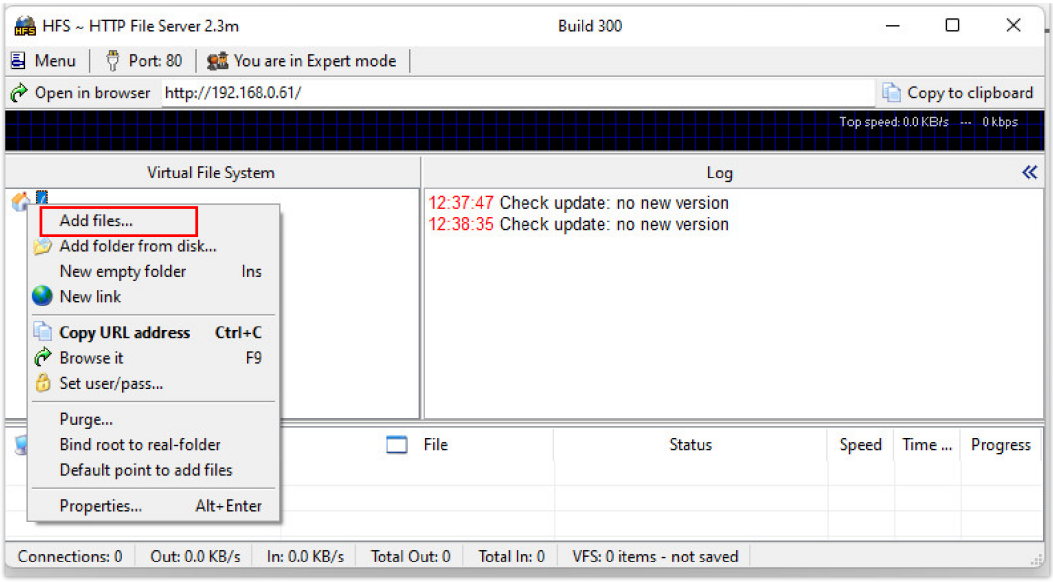
Please refer to following steps in order to download / install the HTTP server and upload the firmware:

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.



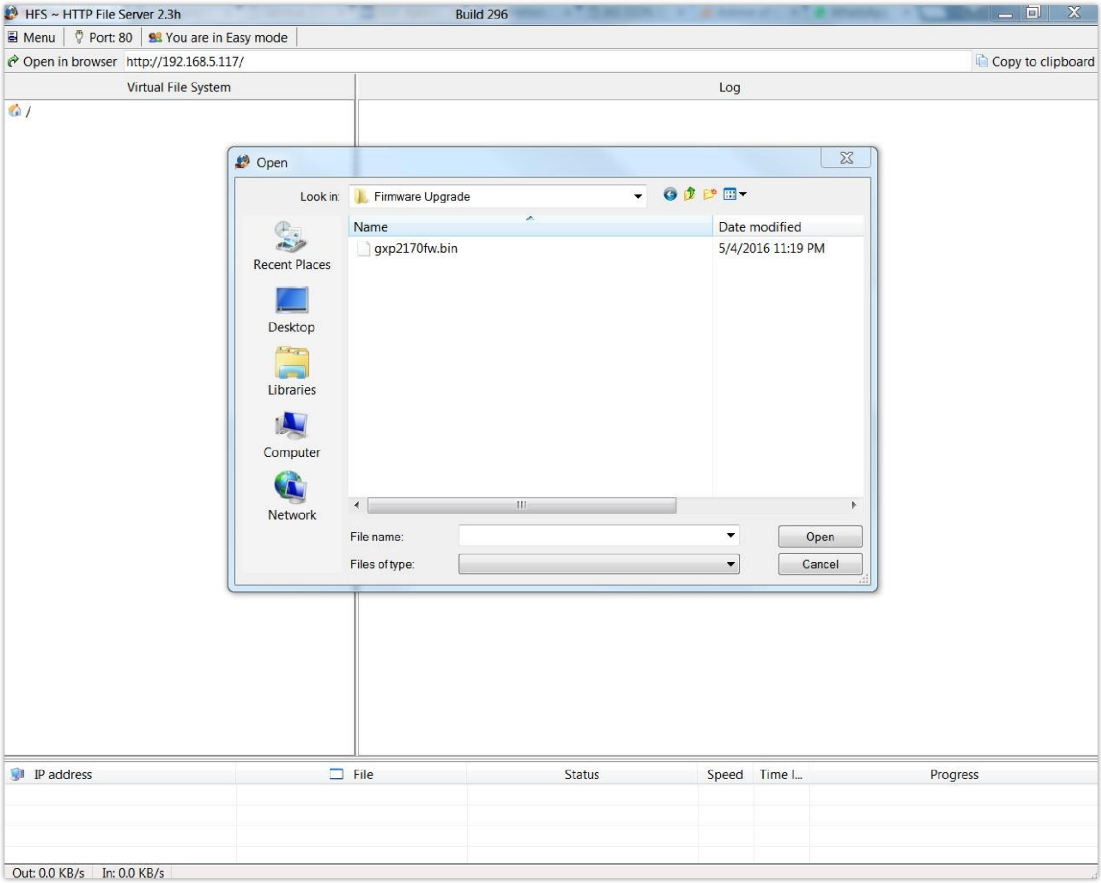
Starting the HTTP server

3. Start the HFS server, browse to locate and select the required firmware files from your local directories by right-clicking on the root direct and selecting **Add files.**



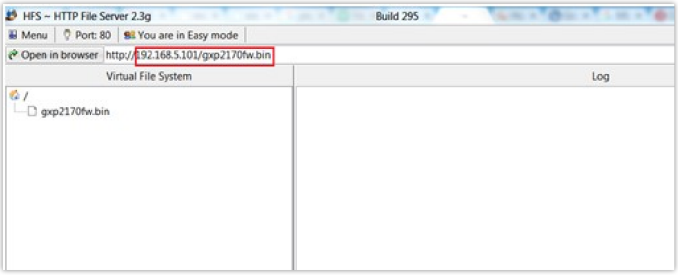
Selecting the firmware file to upload on the HTTP server

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



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 shown on the screenshot below (where 192.168.5.101 is the IP address of the computer running the local HTTP server).



IP Address of the local HTTP Server

Configuring Grandstream devices for local HTTP upgrade

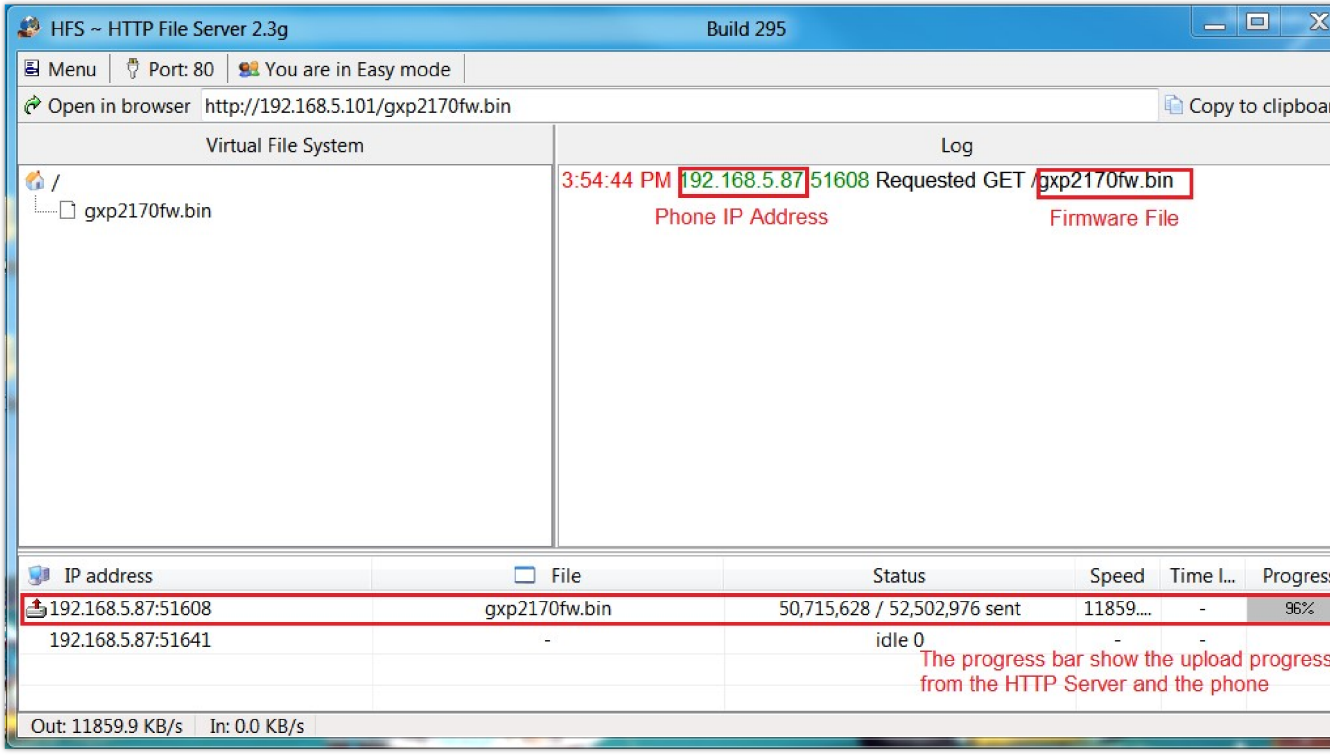
Please refer to following steps to configure Grandstream devices to upgrade the firmware:

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**".
3. Select **Upgrade via HTTP**
4. Enter the path of your HTTP server containing the firmware file under Firmware Server Path.

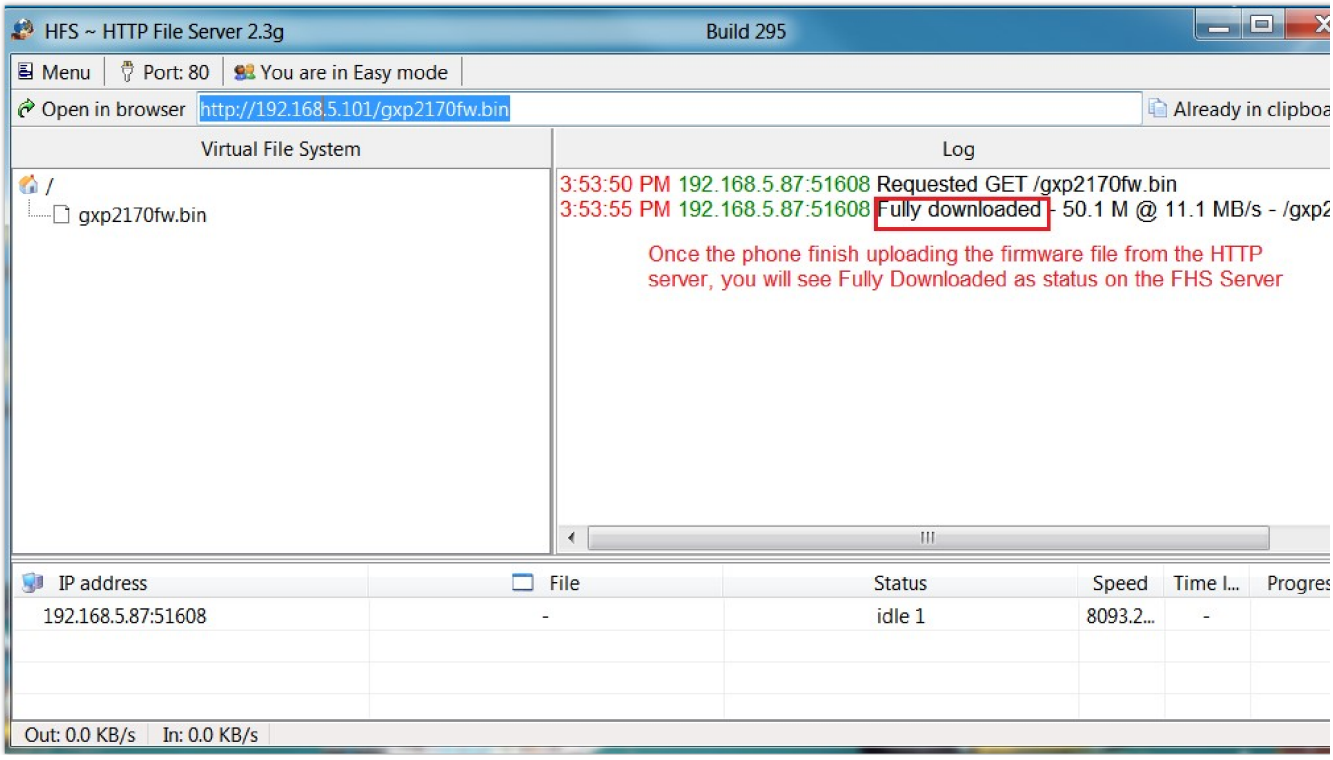
Notes:

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



Firmware upgrade progress



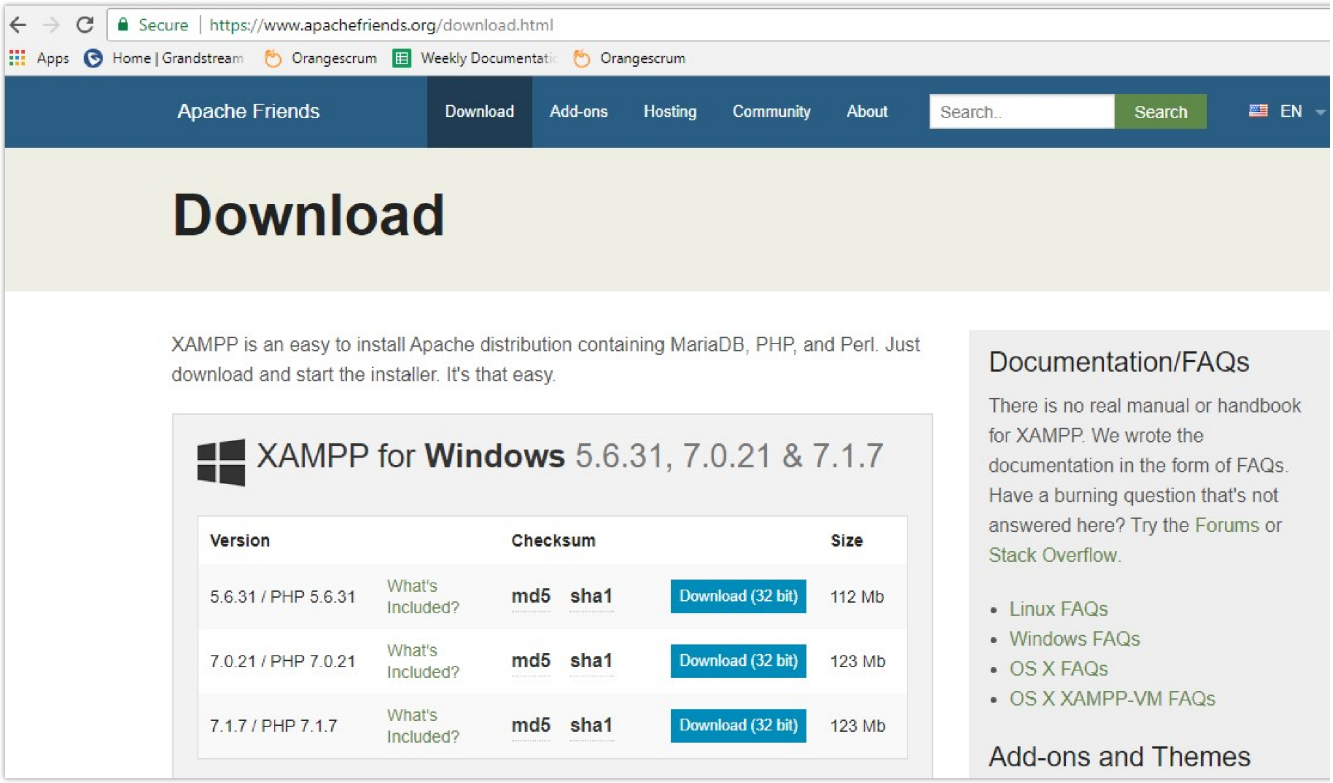
Local Upgrade via HTTPS Server

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.

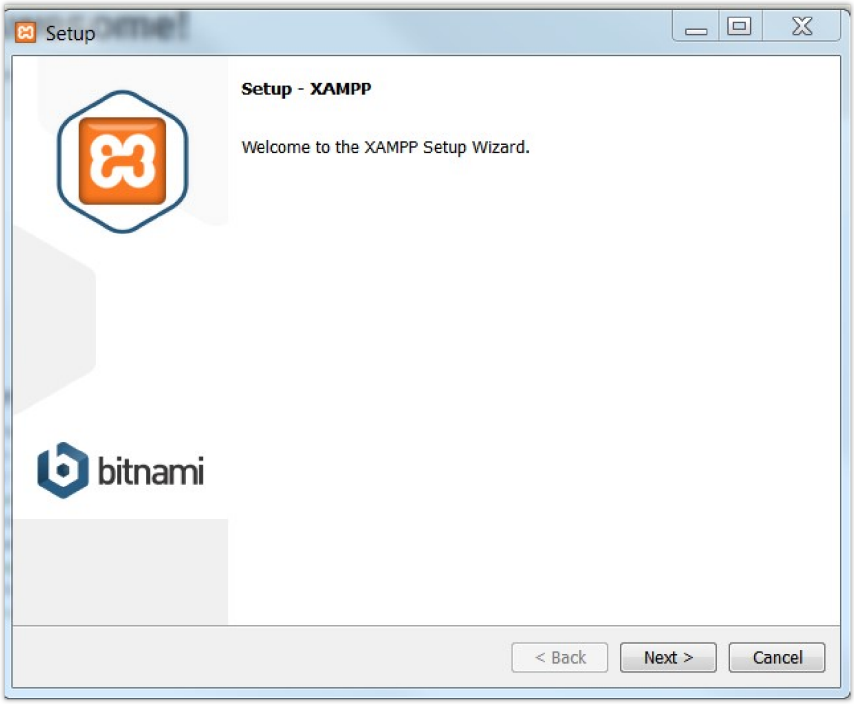
Installing HTTPS Server

1. Download appropriate version depending on your platform.



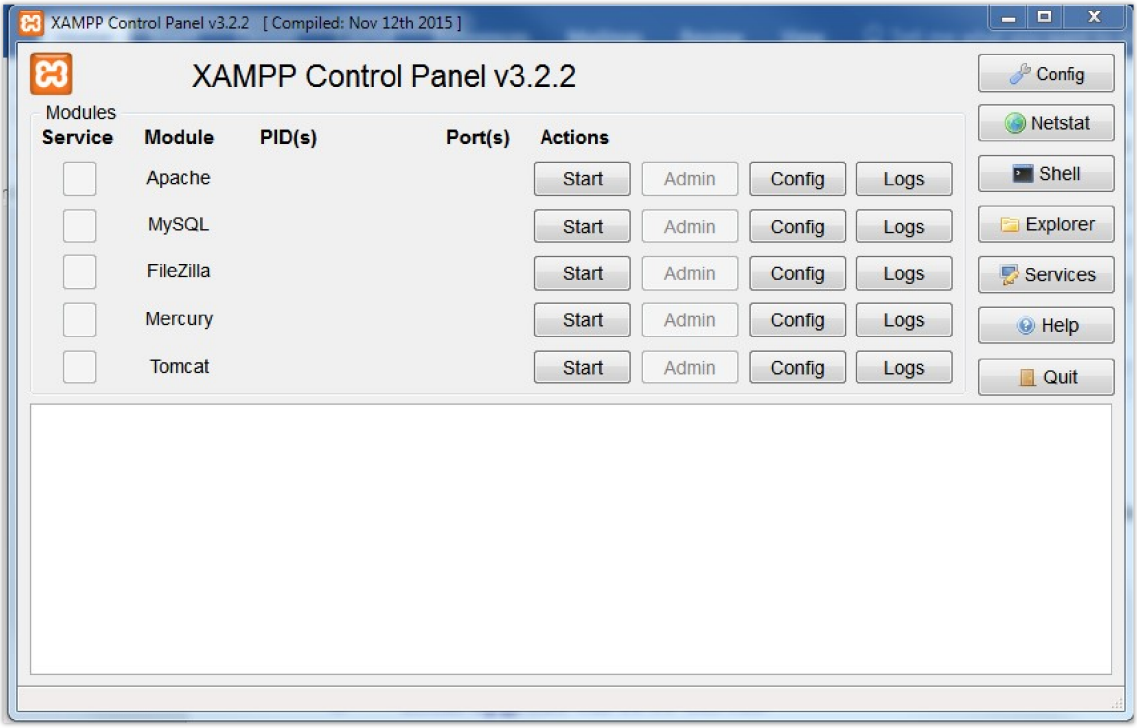
Download XAMPP for windows

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



XAMPP Installation

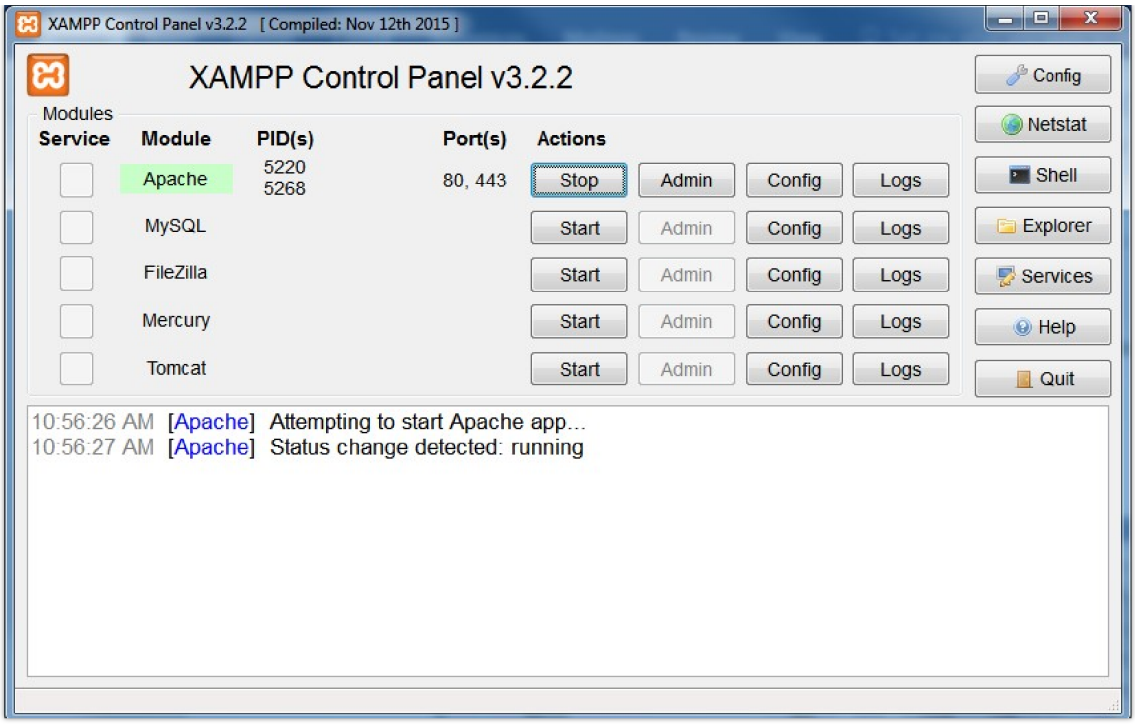
3. Launch the XAMPP server. Following interface will be available.



XAMPP Control Panel

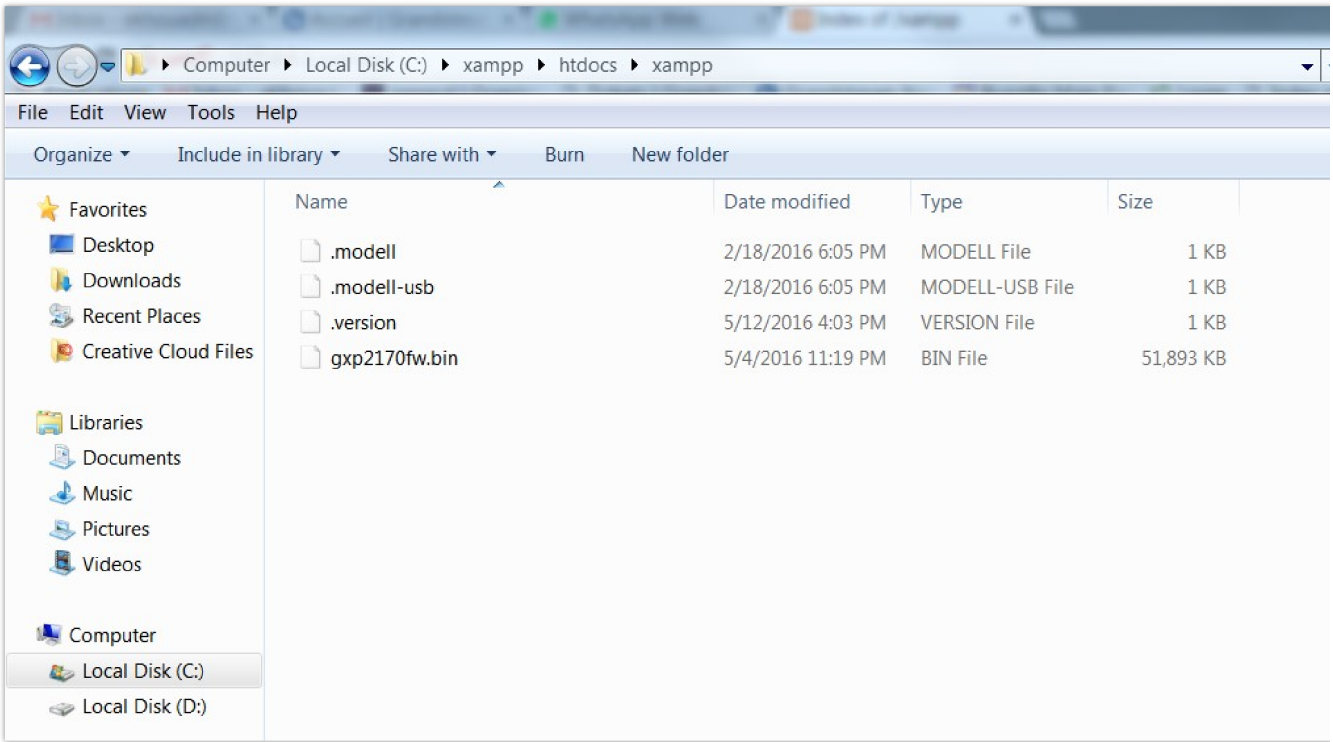
Uploading firmware file(s) to XAMPP HTTPS Server

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



Apache Module Started

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



XAMPP Directory

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

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 generat 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

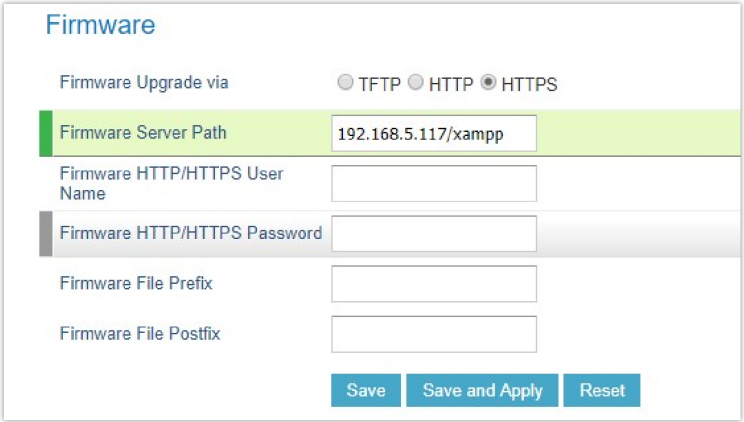
Please refer to following steps to configure Grandstream devices to upgrade the firmware:

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.



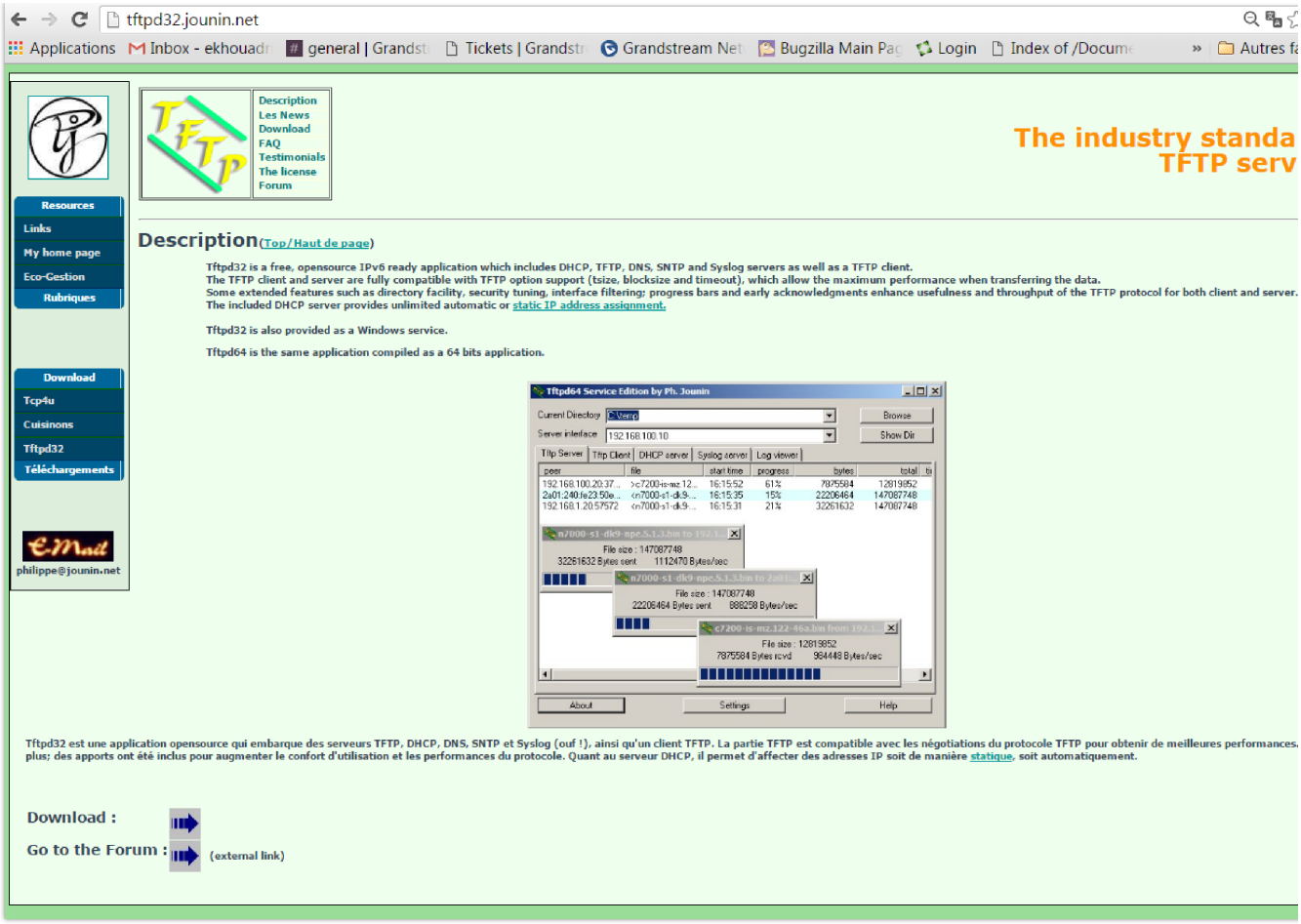
Example of Configuring the Upgrade via HTTPS

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.

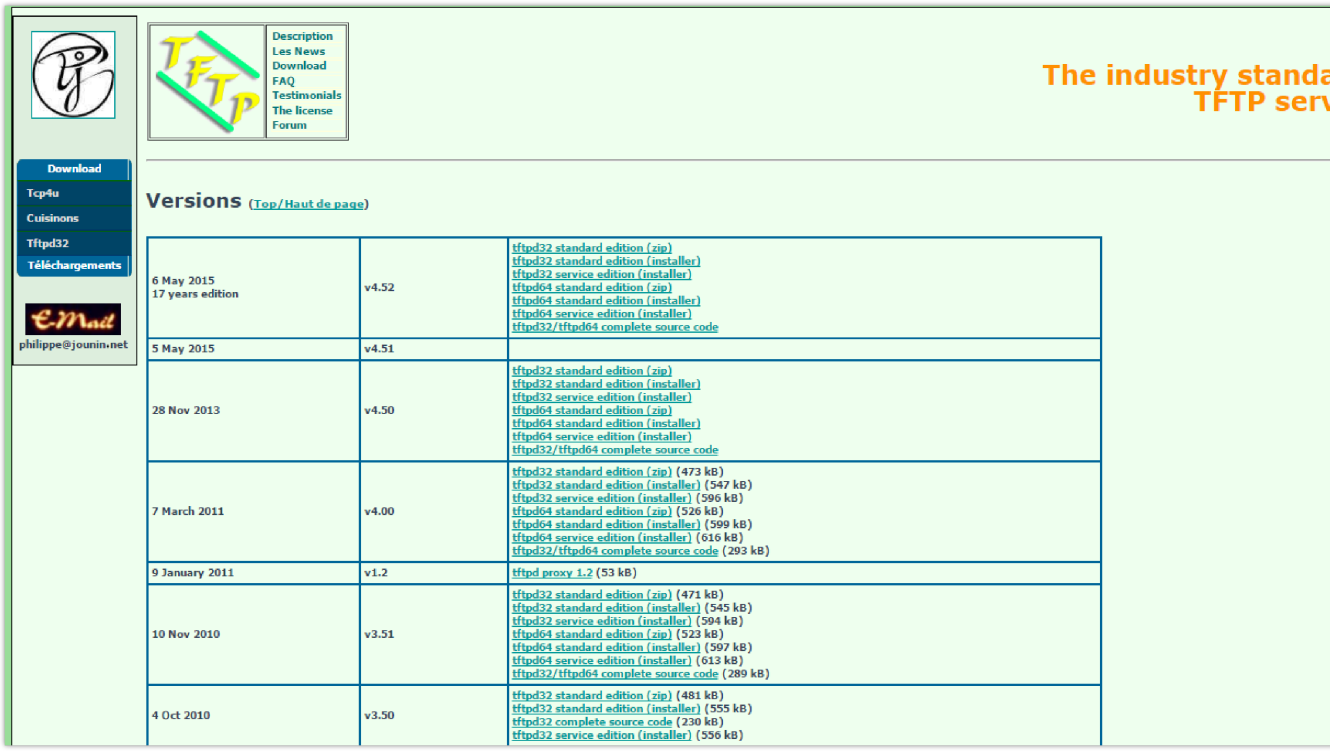
Installing the TFTP Server

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



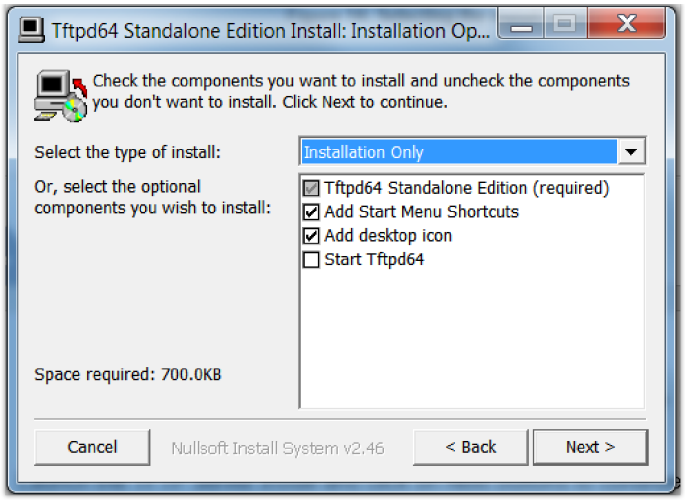
Downloading the TFTP server

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



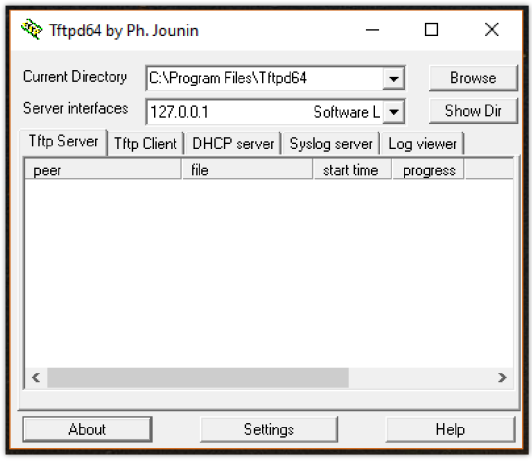
Selecting Install Version

2. Launch the TFTP server install wizard.



TFTP Server Installation

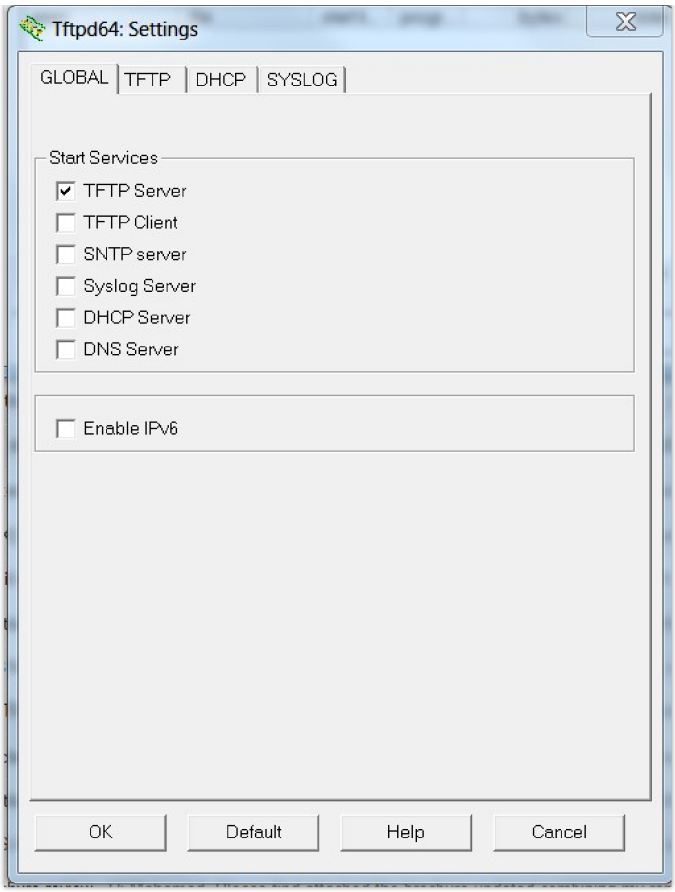
3. Once the TFTP server is installed, Open TFTPD64. The following interface will be displayed:



TFTP Server Interface

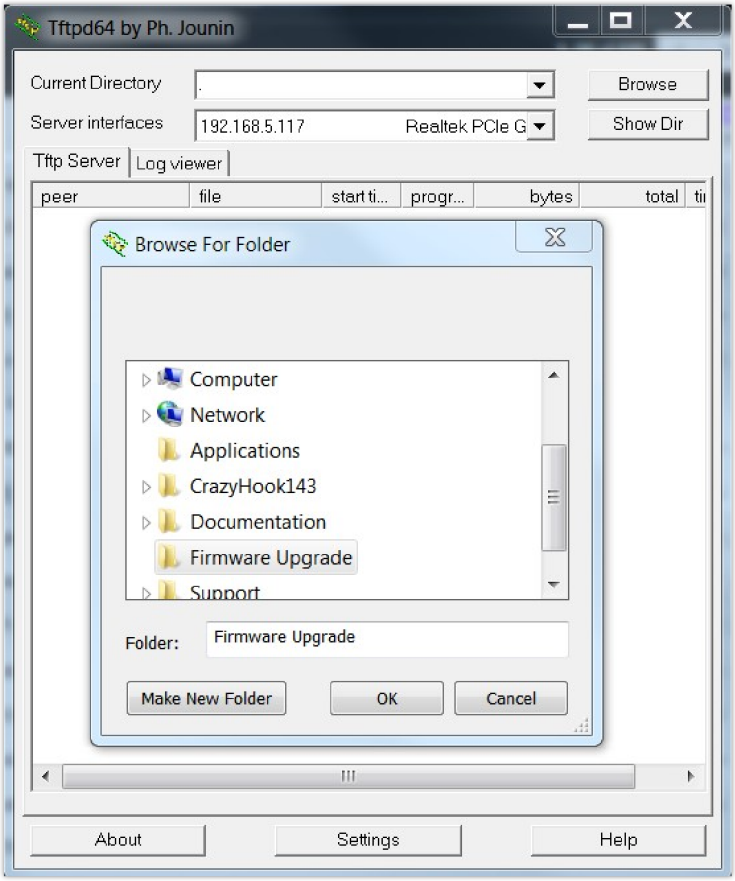
Uploading the firmware file

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



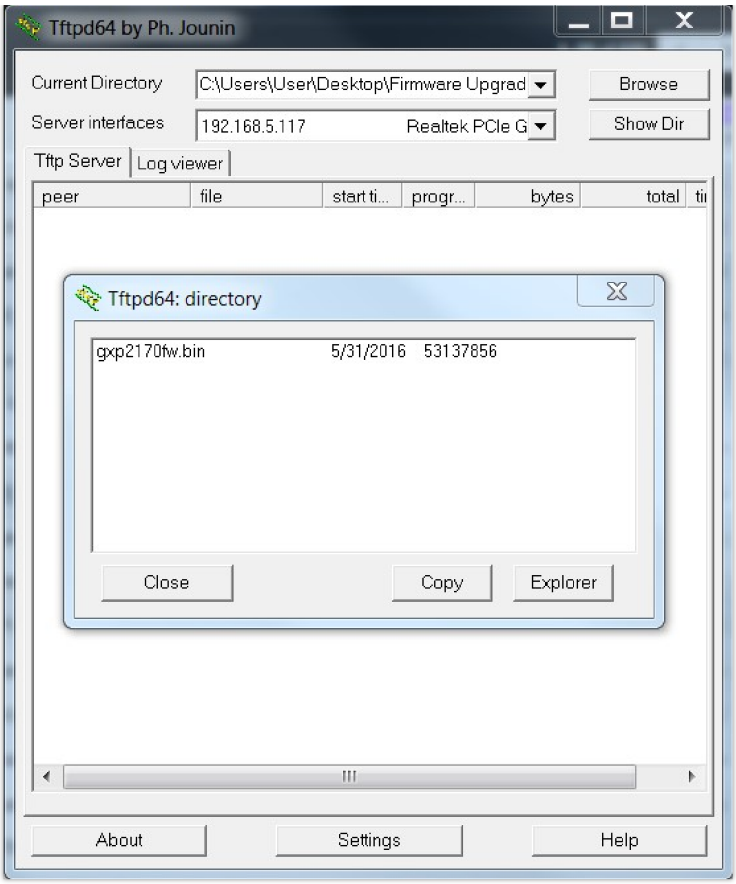
Selecting TFTP Server Services

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



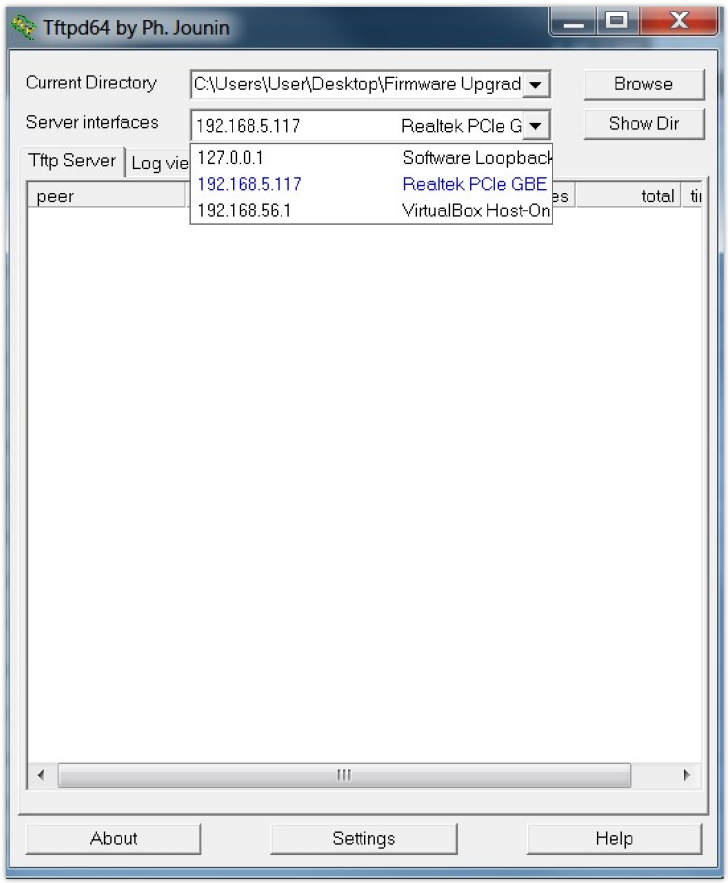
Selecting Local Directory containing Firmware File

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



Firmware File Upload Verification

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



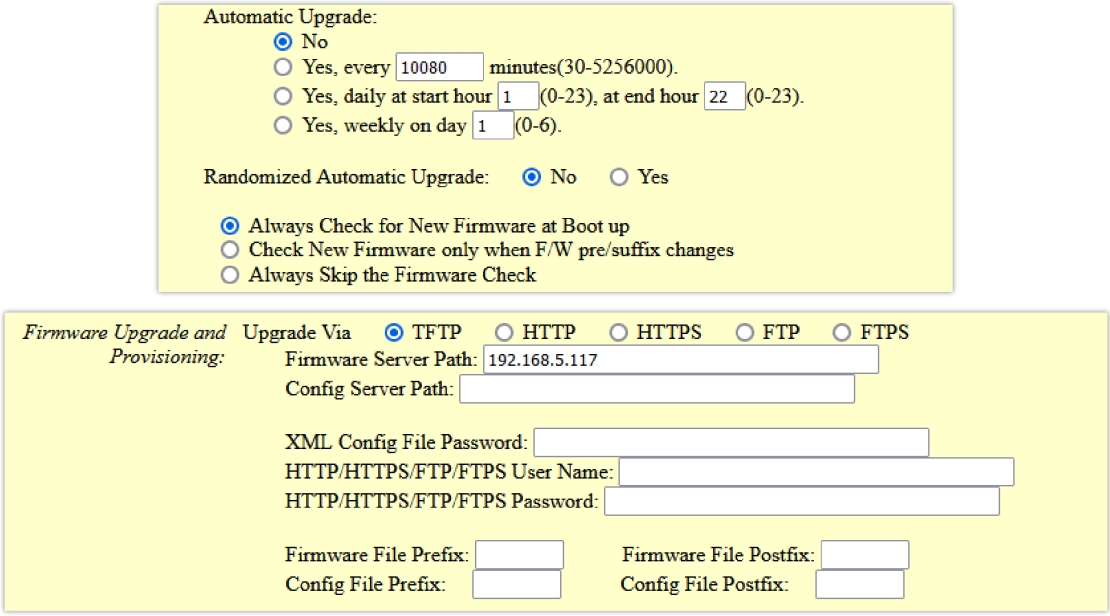
TFTP Server Configuration

Configuring Grandstream devices for local TFTP upgrade

To configure your Grandstream devices for upgrading via your TFTP server, please 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.



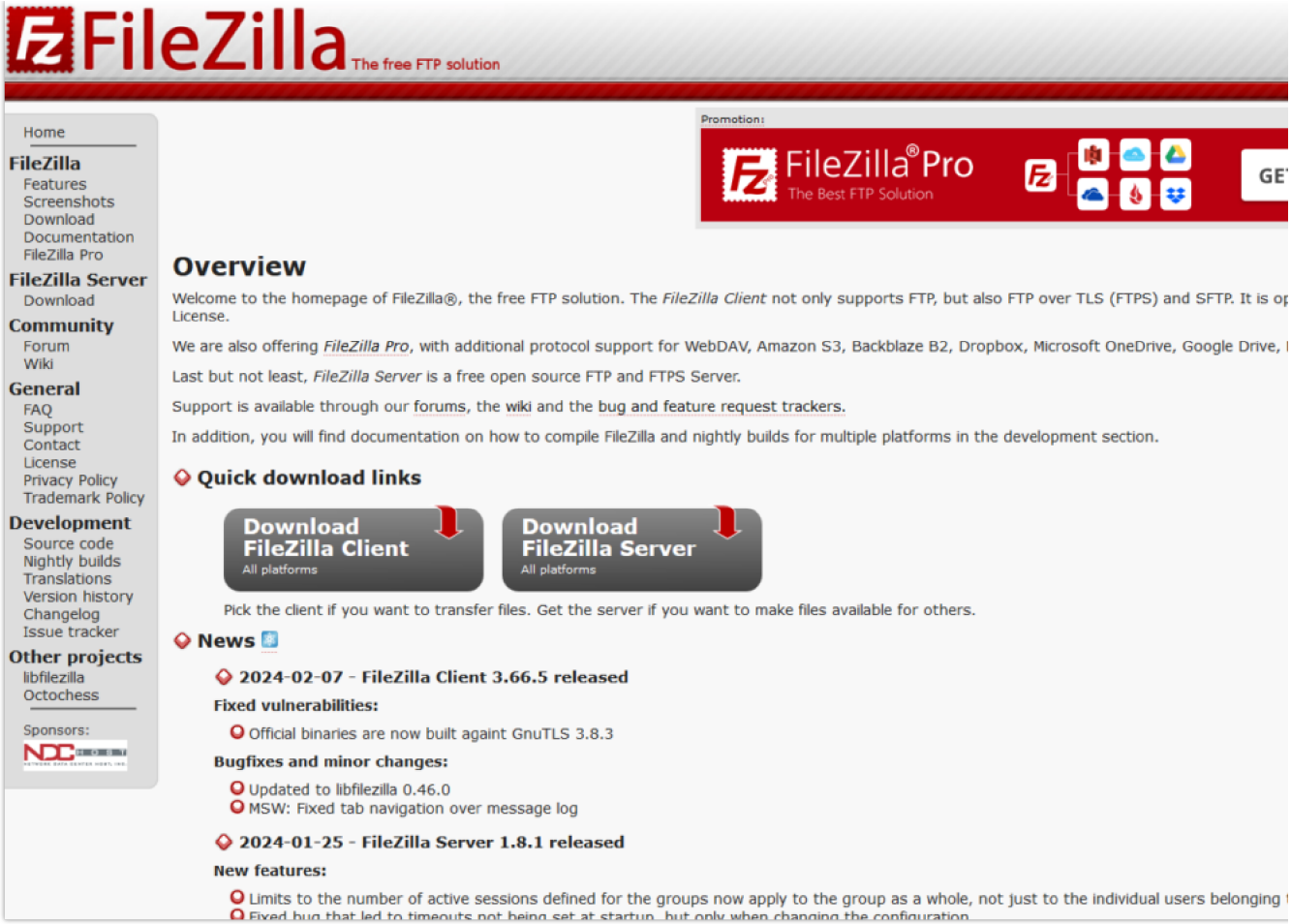
Example of Configuring the Upgrade via TFTP on HT8xx

Local Upgrade via FTP/FTPS Server

The following section contains the steps to upgrade using a local FTP/FTPS server.

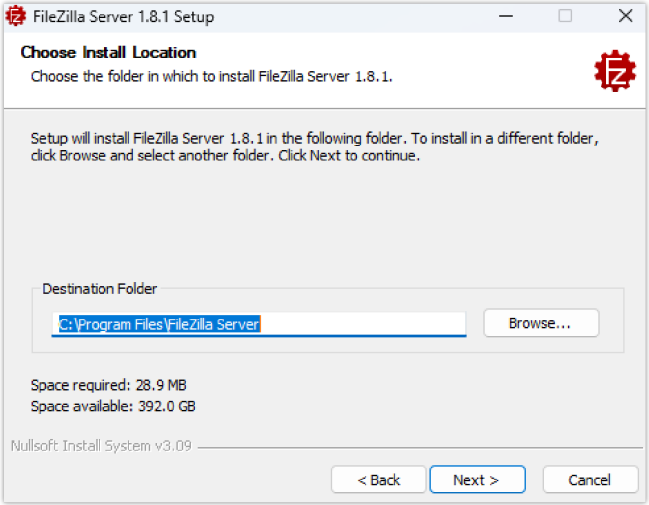
Installing the FTP/FTPS Server

Users can download a free FTP server for windows using this link : http://filezilla-project.org



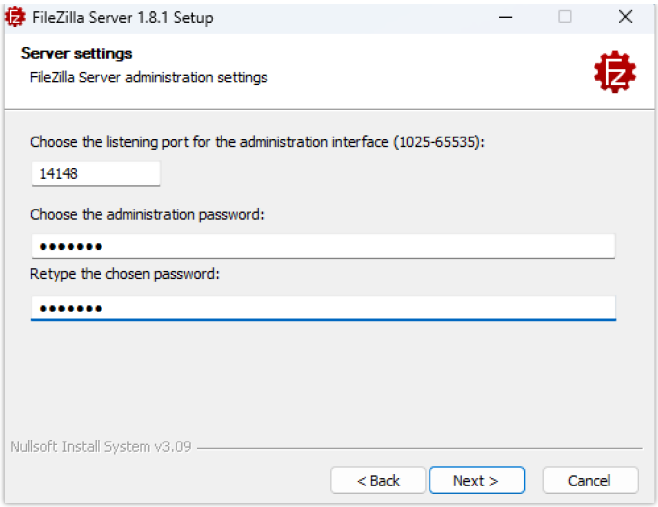
FTP/FTPS Server Download Page

1. Choose the option "**Download FileZilla Server**" and launch the Install wizard;



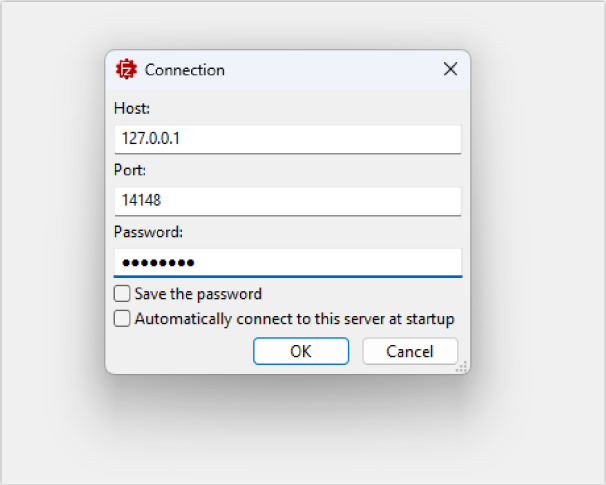
FTP/FTPS Server Install Wizard

2. During the installation process, you will be prompted to enter the **listening port for the administration interface** as well as a **password** *(We chose the default port number "14148").*



FTP/FTPS Server Admin Settings

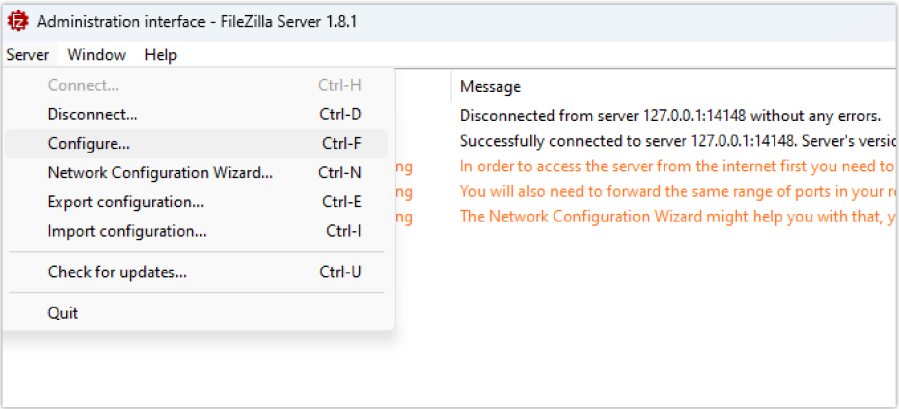
3. Once the installation is finished, you can open the FTP/FTPS server and connect using your **admin port** and **password**.



FTP/FTPS Server Connection Page

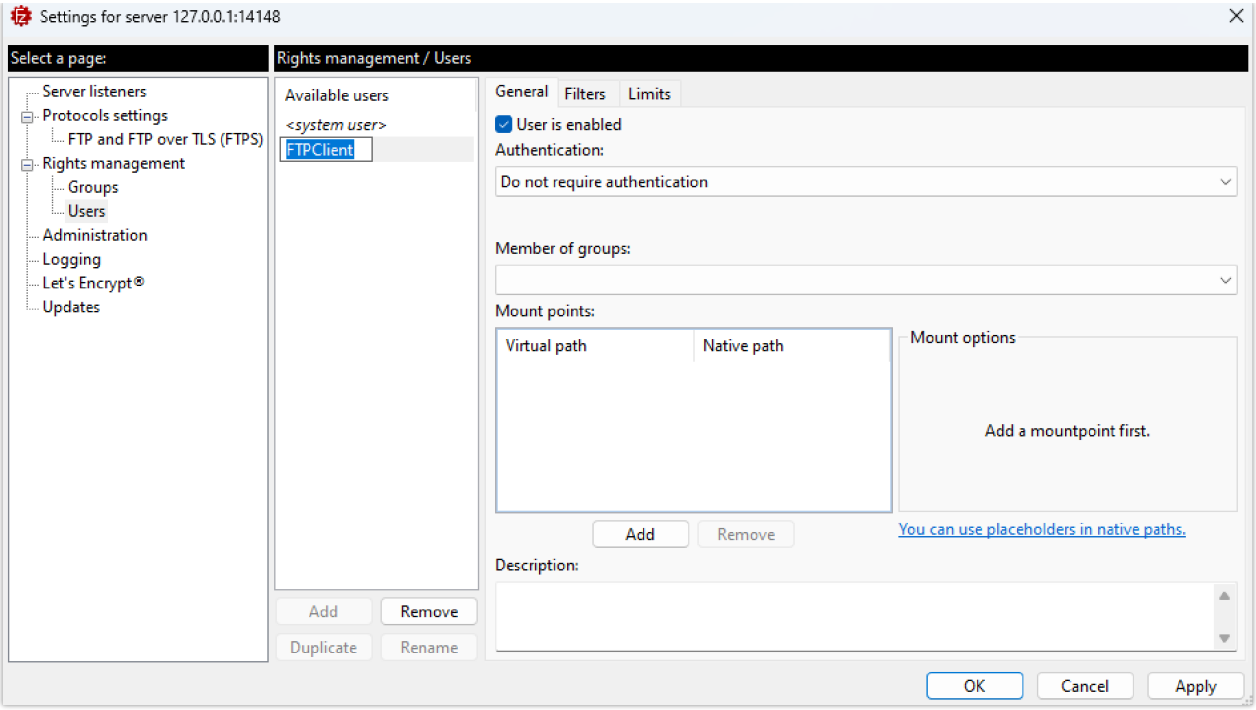
Configuring the FTP Server

1. To configure the FTP server, in the "**Server**" drop-down menu, select "**Configure**".



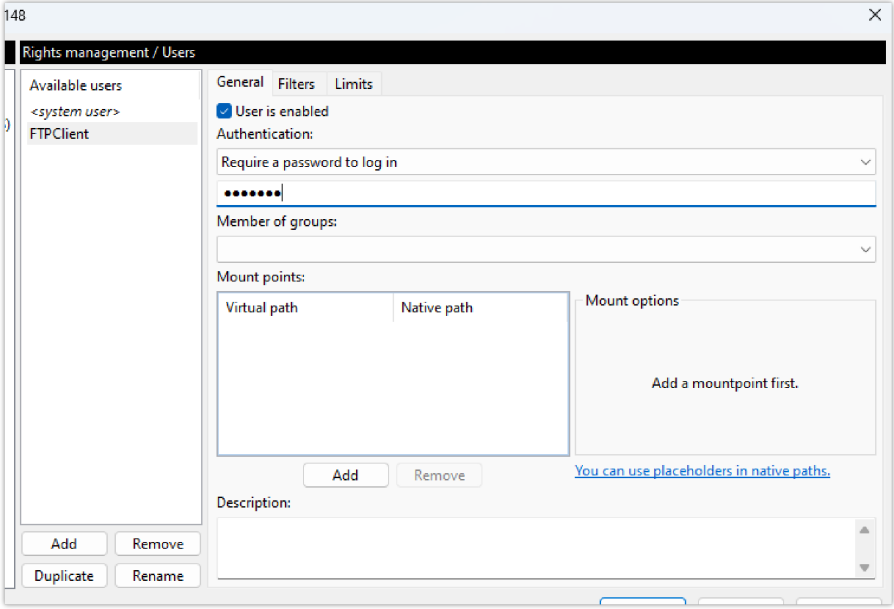
FTP Server Configuration Option

2. Select the Users page and click the "**Add**" button under "**Available users**" *(In this scenario we're naming our user "FTPClient").*



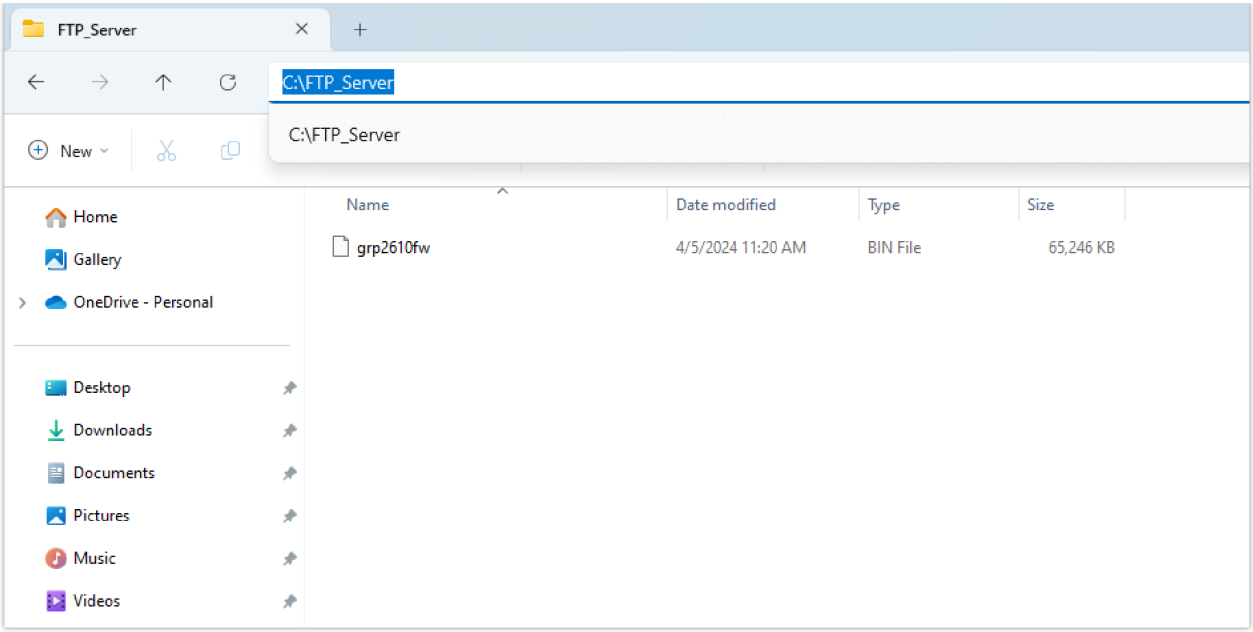
Example of adding FTP user

3. For authentication, choose the option "**Require a password to log in**" and enter the user's password.



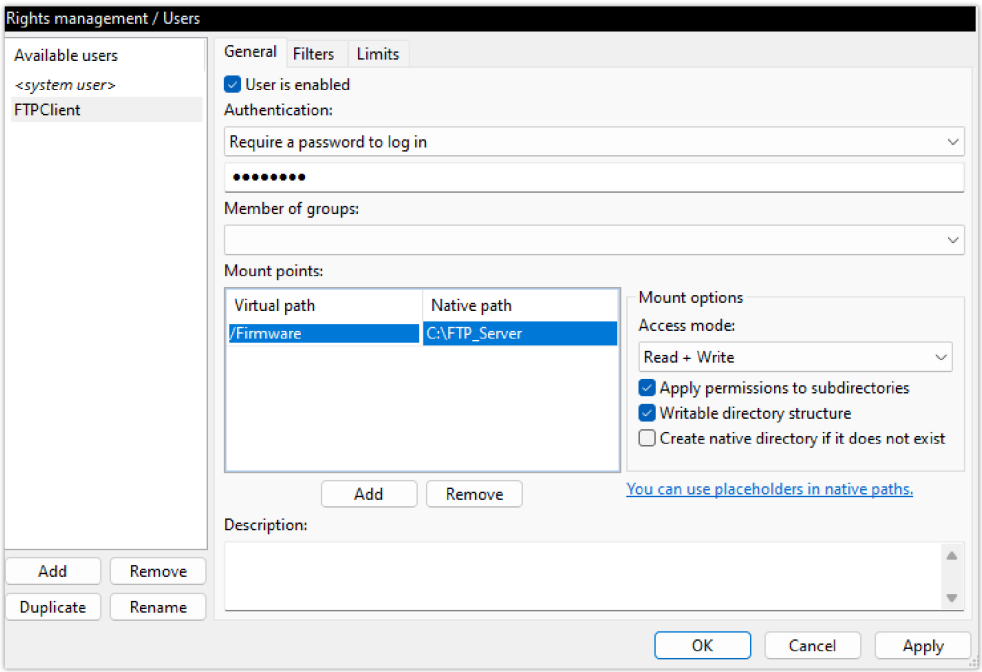
FTP user authentication

4. On the computer running the FTP Sever, create a **Folder** containing the firmware files and copy the **folder path**.



Copying the Folder Path for FTP user

5. In the settings of the FTP user created, add the copied folder path under "**Native Path**" and provide a name in "**Virtual path**".
6. To configure the user's rights, choose one of the options in the "**Access mode**" drop-down menu. *(For this example we selected "**Read + Write**").*

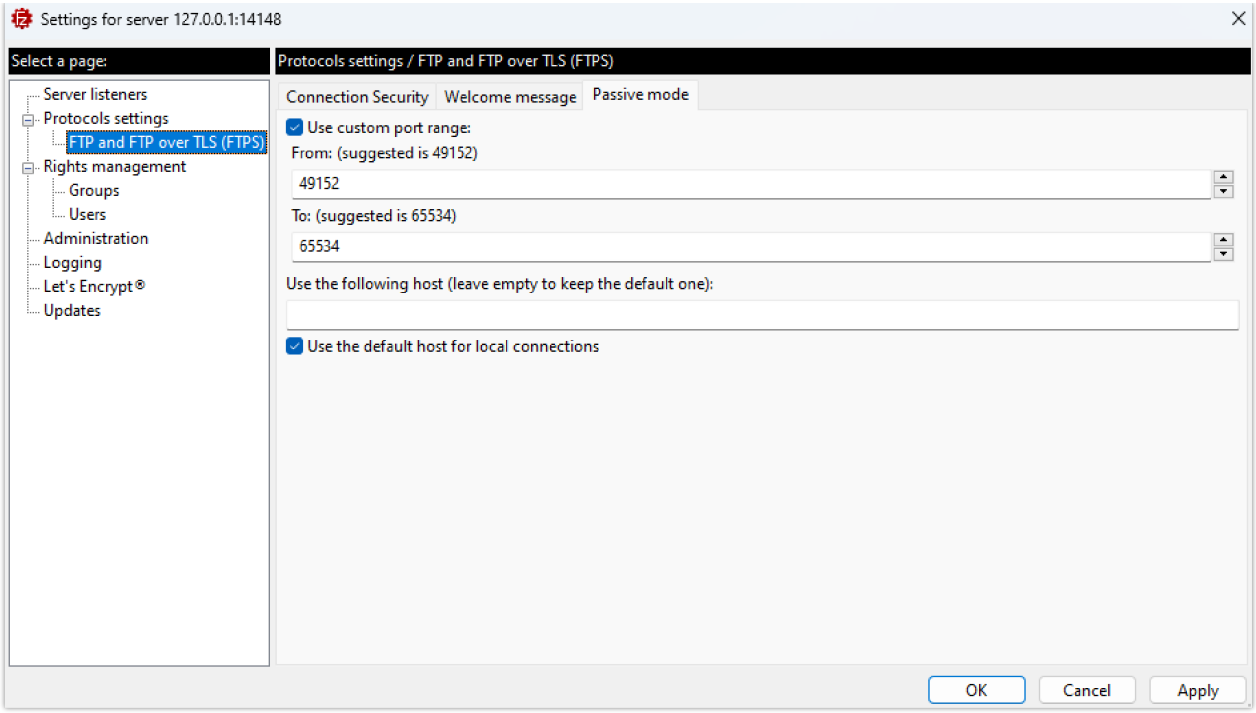


Adding Mount points for FTP user

Important :

The **Virtual path** name should begin with a forward slash character "**/**" *(In this example we chose "/Firmware").*

7. In order to enable FTP Passive Mode, select the page **"FTP and FTP over TLS (FTPS)**" and click on the "**Passive Mode**" tab.
8. Check the option to "**Use custom port range**" and enter the suggested port range.

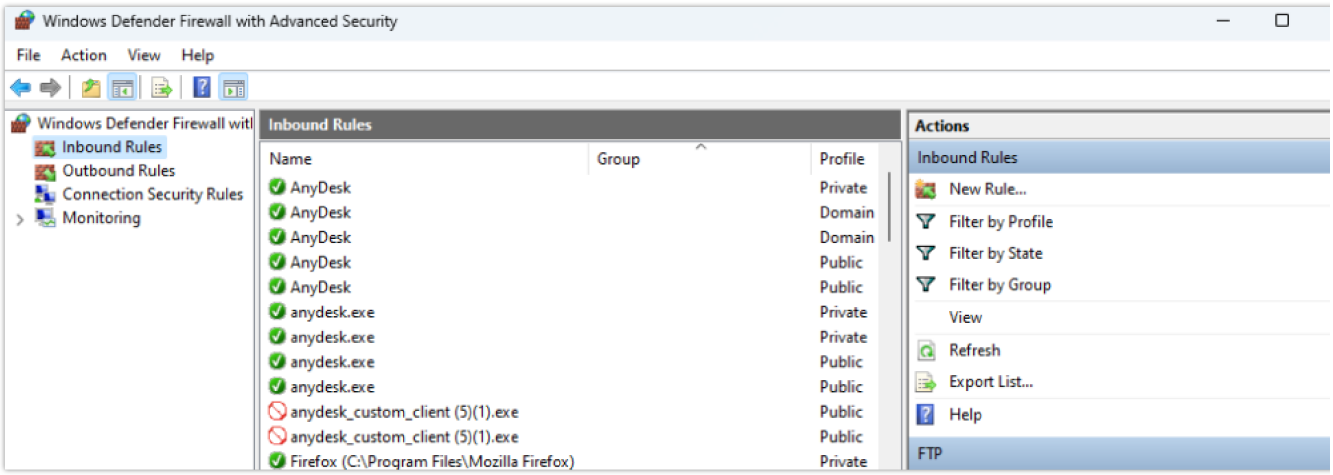


FTP Passive Mode

FTP Passive Mode :

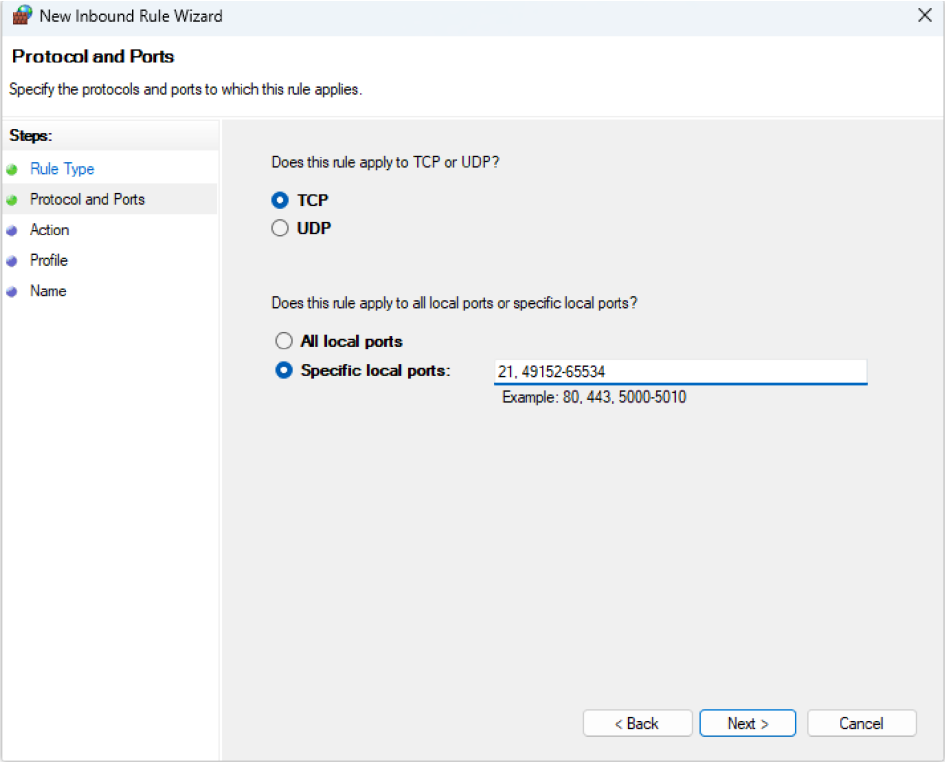
FTP passive mode is a configuration option in FTP (File Transfer Protocol) where the data connection is established by the client rather than the server. This mode is particularly useful in local FTP server configurations where the server is behind a firewall or NAT (Network Address Translation) device.

9. Now that we have created a user and defined the port range for FTP Passive Mode, the next step is to **open FTP port** (TCP port 21) as we the **FTP Passive Mode port range** (TCP ports 49152-65534) on the **firewall**. *(In this case, we're using Windows Defender Firewall)*.
10. Open **Windows Defender Firewall with Advanced Security** and create a "**New Rule**" under "**Inboud Rules**".



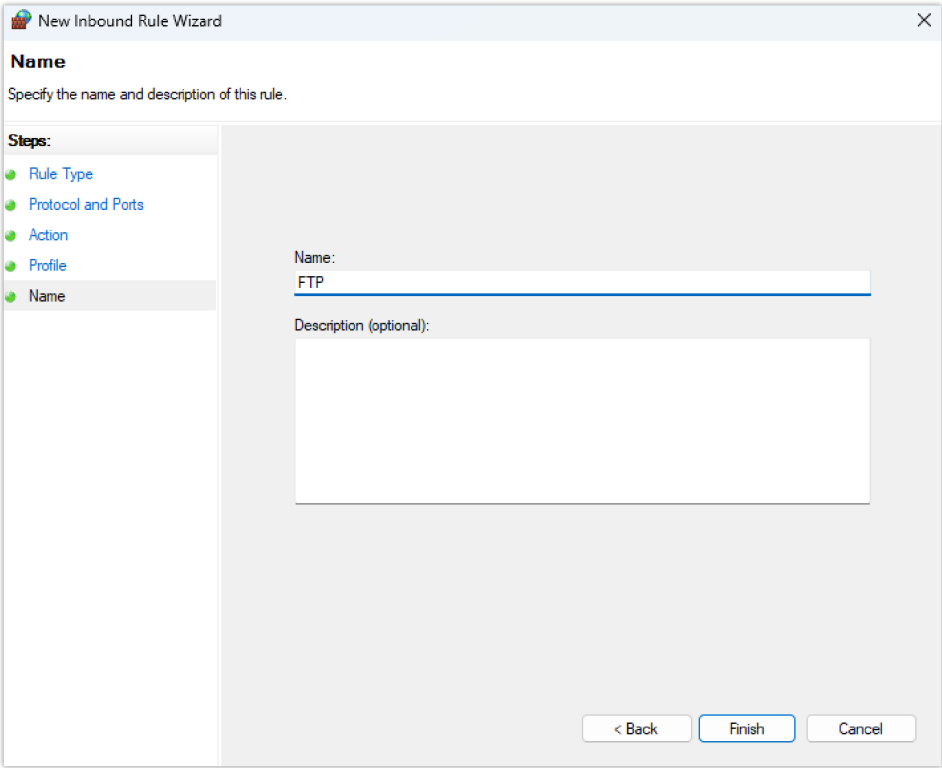
Windows Defender Firewall with Advanced Security (Inbound Rules)

11. Choose "**Port**" as a "**Rule Type**" and "**21**, **49152-65534**" in "**Protocols and Ports**".



Protocols and Ports for the New Inbound Rule

12. Check the option "**Allow connection**" in "**Action**" and leave the "**Profile**" settings as default.
13. The last step in creating this Inbound Rule is providing a "**Name**" and clicking on the **Finish** button.

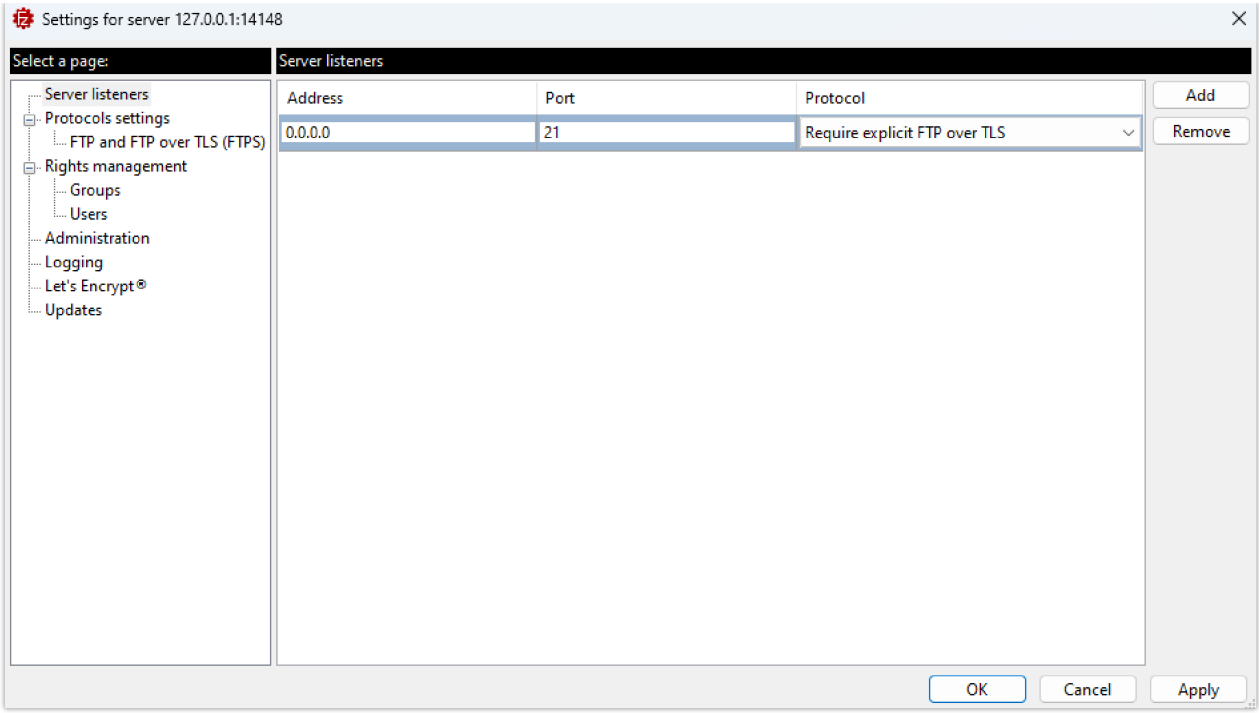


New Inbound Rule Name

Configuring the FTPS Server

In order to configure the FTPS server, users will have to follow the same instructions in the section [Configuring the FTP Server] and add the following steps :

1. Select "**Configure**" from the "**Server**" Menu.
2. On the "**Server listeners**" page, after removing all the entries by clicking on the "**Remove**" button, enter "**0.0.0.0**" under Address, "**21**" in port and "**Require explicit FTP over TLS**" for Protocol.

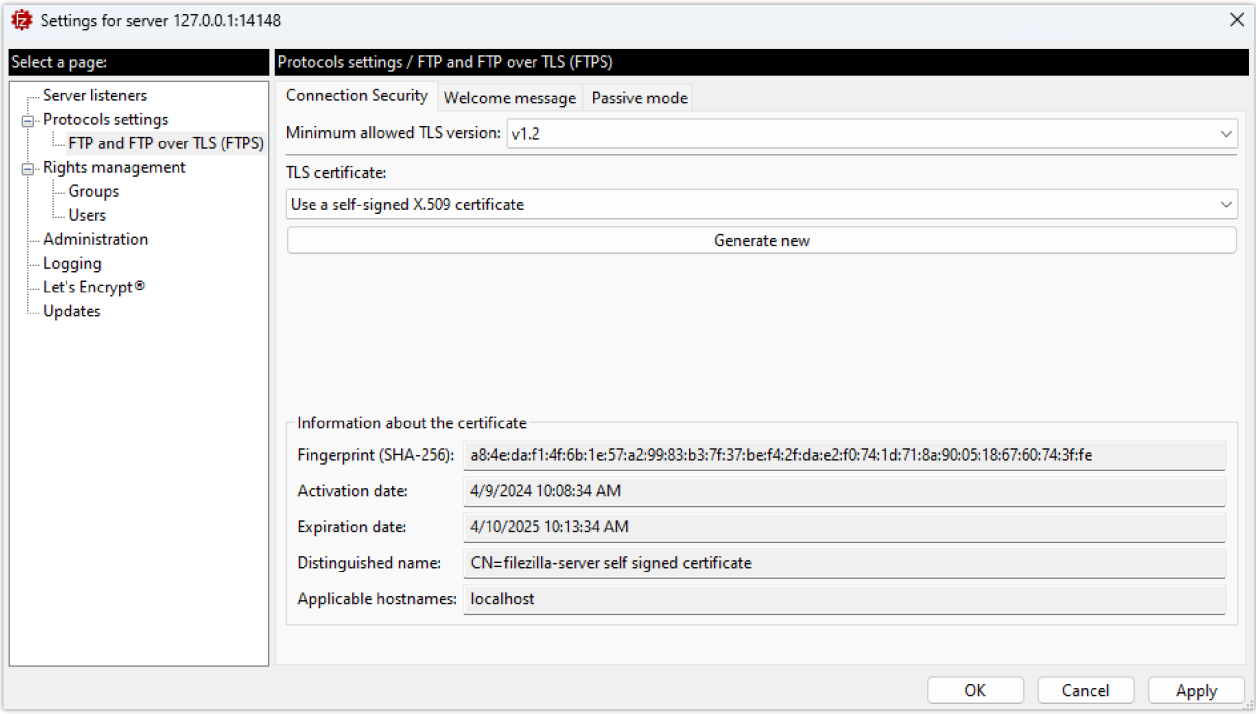


Explicit FTP over TLS configuration

Explicit FTP over TLS :

In Explicit FTP over TLS, the client initially connects to the server's standard port 21 without encryption. After the client sends a "AUTH TLS" command, the server responds by negotiating a secure TLS connection. This approach allows for both secure and non-secure FTP connections on the same port.

By default, Filezilla uses a self-signed X.509 TLS certificate. We can choose the minimum allowed TLS version by going to the "**FTP and FTP ov TLS (FTPS)**" page from the server's configuration settings.



TLS Certificate

Configuring Grandstream devices for local FTP/FTPS upgrade

Please follow the steps below to configure Grandstream devices to upgrade their firmware via FTP:

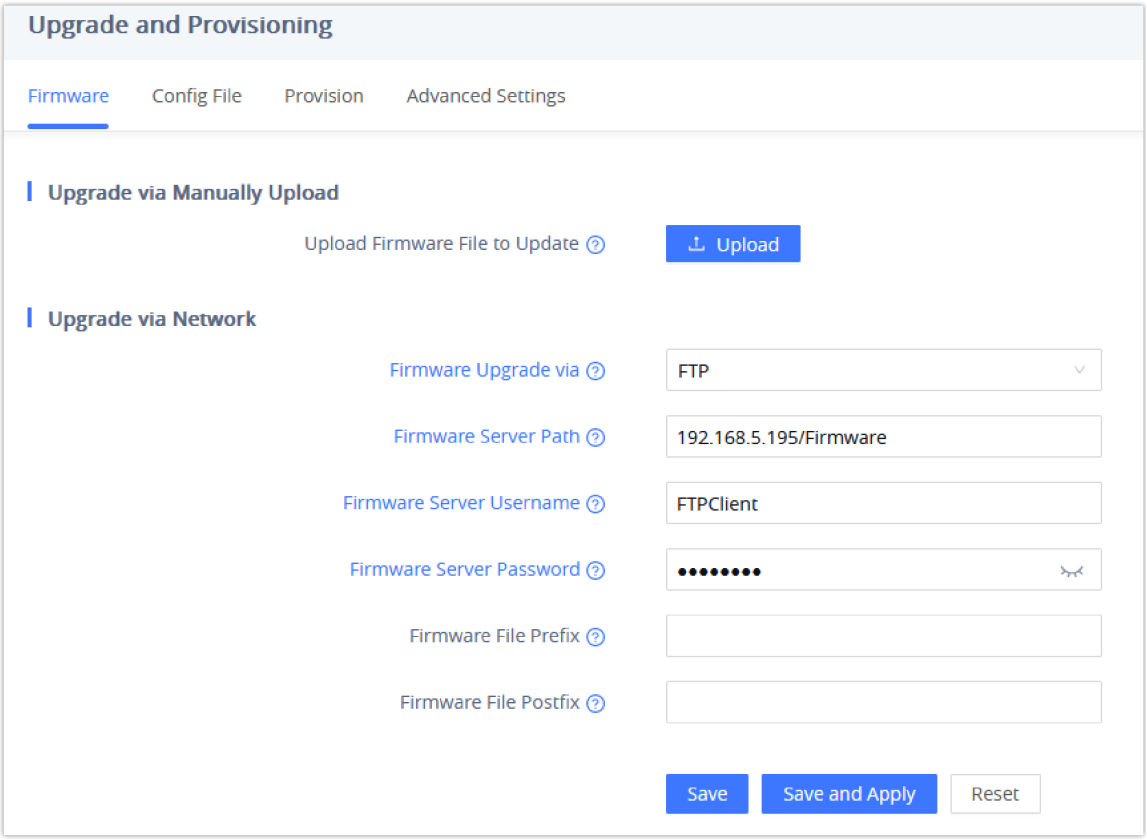
1. Access the Web GUI and navigate to "**Upgrade and Provisioning**" page.
2. In the "**Provision**" section, Set "**Firmware Upgrade and Provisioning**" to "**Always Check for New Firmware**".
3. Go to the "**Firmware**" section,
4. Select "**FTP"** or "**FTPS**" for "**Firmware Upgrade via**".

5. Enter the path of the FTP/FTPS server containing the firmware file under "**Firmware Server Path**".

FTP Server Path

The "Firmware Server Path" should follow this format : **x.x.x.xVirtual Path** Where **x.x.x.x** is the IP Address of the computer running the FTP Server and the **Virtual Path** is the one defined for the FTP User. In this example, the IP address is 192.168.5.195 and the Virtual Path for the user we created (FTPClient) is "/Firmware". In this case, the "Firmware Server Path" is : **192.168.5.195/Firmware**

6. Fill in the "**Firmware Server Username**" and the "**Firmware Server Password**" fields with the credentials of the FTP/FTPS user created.



Example of configuring the Upgrade via FTP on GRP1x

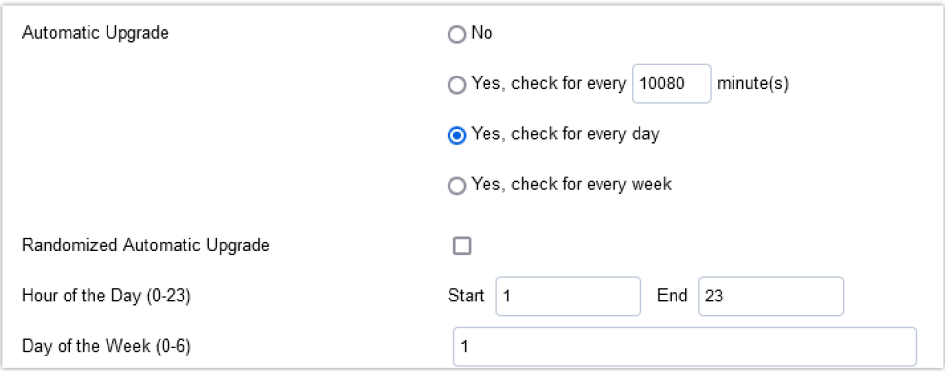
7. Press "**Save and Apply**" at the bottom of the page to apply the new settings.
8. **Reboot** the device and wait until the firmware upgrade process is completed.

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.



Example of Configuring Automatic Upgrade on GSC3610

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 downloadec 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.

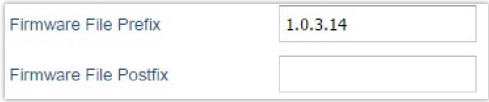
Firmware file prefix and postfix can be configured from **web GUI →Maintenance → Upgrade and provisioning**.

Screenshot of Firmware file Prefix and Postfix fields for GSC3610

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*



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*

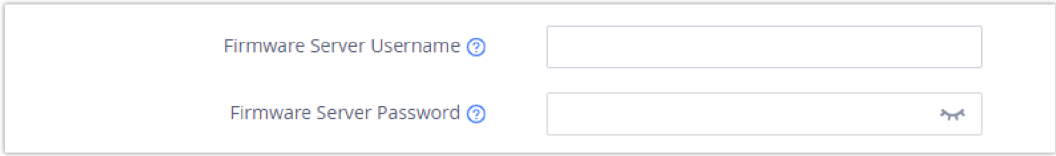
Configuring the Firmware File Postfix

Firmware Server Username and Password

A username and password need to be configured if the firmware server requires authentication to access and download firmware files.

To begin the 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 firmware server Username 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 fil before being challenged by the server. The default setting is "No".



Screenshot of Firmware Server Username and Password Fields for GRP261x

Upgrade via Firmware Server Supported Devices

Category	Models	Firmware Upgrade via HTTP	Firmware Upgrade via HTTPS	Firmware Upgrade via TFTP	Firmware Upgrade via FTP	Firmware Upgrade via FTPS

IP Voice Telephony	**GRP Series IP Phones**					
	GRP260x	✓	✓	✓	✓	✓
	GRP261x	✓	✓	✓	✓	✓
	GRP262x	✓	✓	✓	✓	✓
	GRP263x	✓	✓	✓	✓	✓
	GRP2650	✓	✓	✓	✓	✓
	GRP2670	✓	✓	✓	✓	✓
	GXP Series IP Phones					
	GXP16xx	✓	✓	✓	✓	✓
	GXP17xx	✓	✓	✓	✗	✗
	GXP21xx	✓	✓	✓	✓	✓
	GHP Series Hotel Phones					
	GHP61x	✓	✓	✓	✓	✓
	GHP62x	✓	✓	✓	✓	✓
	GHP63x	✓	✓	✓	✓	✓
	DECT Cordless					
	DP75x	✓	✓	✓	✓	✓
	DP760	✓	✓	✓	✓	✓
	Wi-Fi Cordless IP Phones					
	WP810	✓	✓	✓	✓	✓
	WP820	✓	✓	✓	✗	✗
	WP822	✓	✓	✓	✓	✓
	WP825	✓	✓	✓	✓	✓
IP Video Telephony	**GXV Series of IP Video Phones**					
	GXV33xx	✓	✓	✓	✗	✗
	GXV34xx	✓	✓	✓	✗	✗

Gateways & ATAs	**Analog VoIP Gateways**					
	GXW4104/4108	✓	✗	✓	✗	✗
	GXW42xx v1	✓	✓	✓	✗	✗
	GXW42xx v2	✓	✓	✓	✓	✓
	GXW45xx	✓	✓	✓	✗	✗
	Analog Telephone Adapters					
	HT841/HT881	✓	✓	✓	✓	✓
	HT8xx	✓	✓	✓	✓	✓
Business Conferencing	**Audio Conferencing**					
	GAC2500	✓	✓	✓	✗	✗
	GAC2570	✓	✓	✓	✗	✗
	Video Conferencing					
	GVC3212	✓	✓	✓	✗	✗
	GVC3220	✓	✓	✓	✗	✗
Facility Management	**Control Stations**					
	GSC3570	✓	✓	✓	✓	✓
	IP Video Surveillance					
	GSC3610	✓	✓	✓	✗	✗
	SIP Intercoms & Paging					
	GSC350x	✓	✓	✓	✗	✗
	GSC351x	✓	✓	✓	✗	✗
	Facility Access Systems					
	GDS370x	✓	✓	✓	✗	✗
	GDS371x	✓	✓	✓	✗	✗