Grandstream Networks, Inc.

GRP26xx - 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_GRP260x_1.0.1.50.zip* and *Release_Note_GRP260x_1.0.1.50.pdf* are specific to GRP260X Carrier Grade IP Phones.

Grandstream recommends reading 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.
- **Scenario 3:** Upgrade through Manual Upload .
- **Advanced options.**

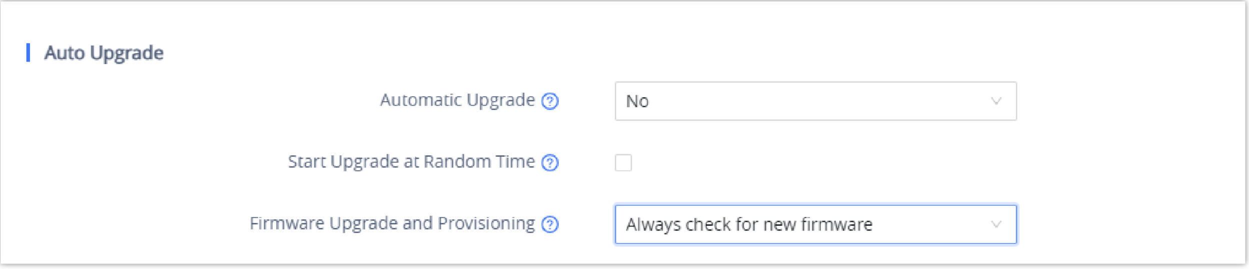
GRP26xx series include GRP260x and GRP261x series as well as GRP2624, GRP2634, GRP2636, GRP2650 and GRP2670.

Scenario 1: Upgrade using Grandstream Public 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 also hosts 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** and go to "**Provision**" tab.
2. Make sure to select "Always Check for New Firmware" for "Firmware Upgrade and Provisioning".



Auto Upgrade

Automatic Upgrade: No

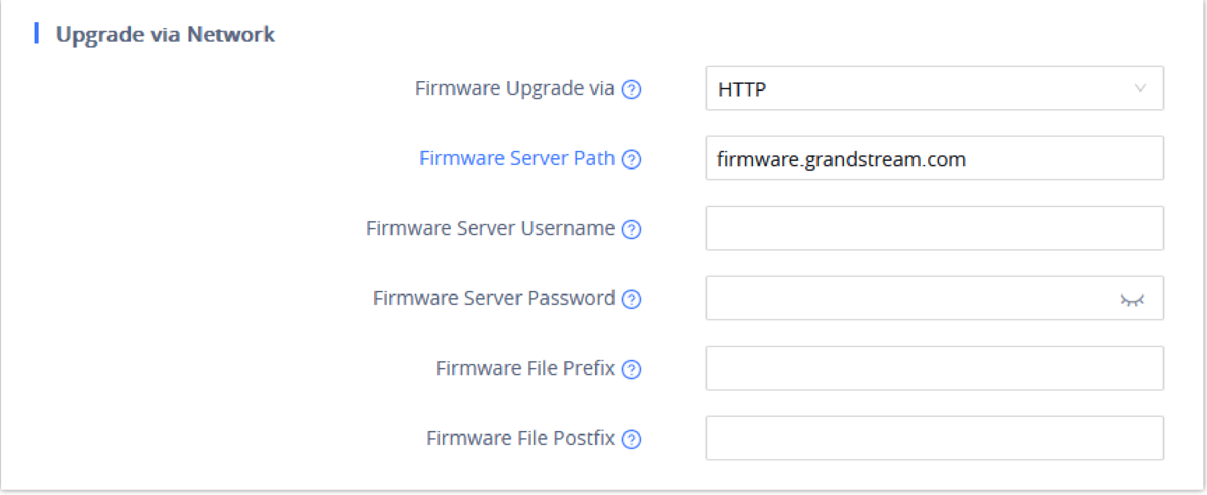
Start Upgrade at Random Time: □

Firmware Upgrade and Provisioning: Always check for new firmware

Option "Firmware Upgrade and Provisioning" – GRP26xx

3. Go to "**Firmware**" Tab and under **"Upgrade via Network"**,

- Select "**HTTP"** for "Firmware Upgrade via"
- Enter "***firmware.grandstream.com***" under "**Firmware Server Path**".


Upgrade via Network

Firmware Upgrade via: HTTP

Firmware Server Path: firmware.grandstream.com

Firmware Server Username:

Firmware Server Password:

Firmware File Prefix:

Firmware File Postfix:

Firmware Web GUI section for GRP26xx

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

- Internet Access is mandatory for the 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.

- 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

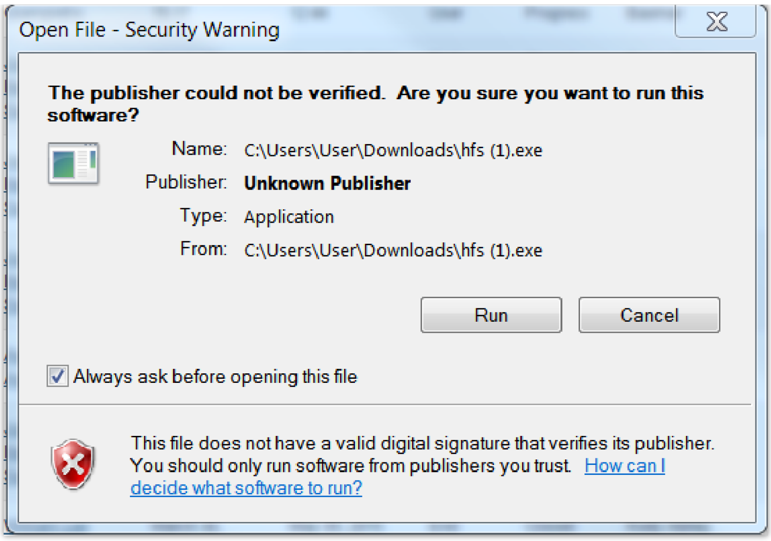
Please refer to the below steps for a local upgrade using **HTTP File Server** tool.

Installing HTTP Server and Uploading Firmware Files

1. Launch the install wizard of the tool once it is fully downloaded.

- Link: http://www.rejetto.com/hfs/download

2. Click on **Run** to launch.


Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: C:\Users\User\Downloads\hfs (1).exe

Publisher: **Unknown Publisher**

Type: Application

From: C:\Users\User\Downloads\hfs (1).exe

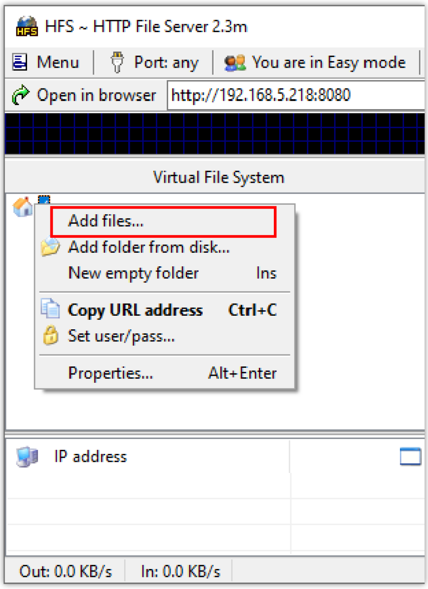
☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

Starting the HTTP server

3. Once HFS starts, browse and select the firmware files from your local directories.

- To add file to the HTTP File Server, please right-click on the VFS url and then choose **Add Files** in as shown in the screenshot below.


HFS ~ HTTP File Server 2.3m

Port: any

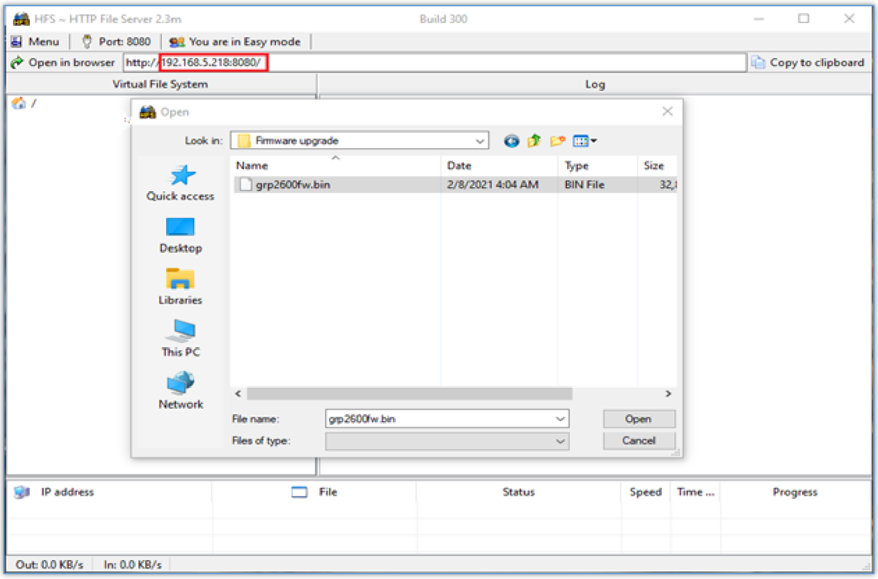
You are in Easy mode

Open in browser http://192.168.5.218:8080

Out: 0.0 KB/s In: 0.0 KB/s

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.


HFS ~ HTTP File Server 2.3m Build 300

Port: 8080

You are in Easy mode

Open in browser http://192.168.5.218:8080/

Look in: Firmware upgrade

Name	Date	Type	Size
grp2600fw.bin	2/8/2021 4:04 AM	BIN File	32,!

File name: grp2600fw.bin

Files of type:

Out: 0.0 KB/s In: 0.0 KB/s

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://192.168.5.218/grp2600fw.bin*" Next to **Open in browser.** As shown on the screenshot:

- **192.168.5.218** 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:

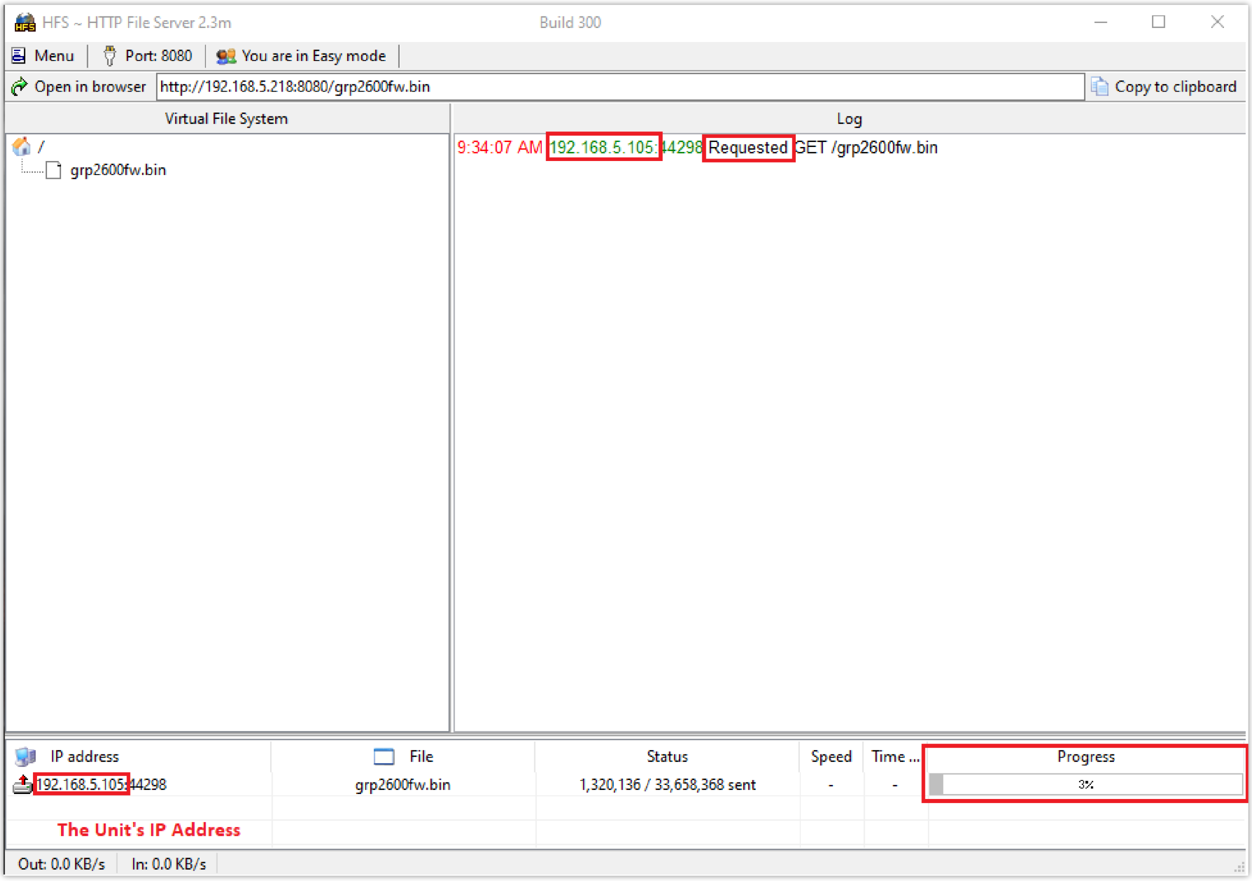
1. Access the Web GUI and navigate to "**Upgrade and Provisioning**" page.
2. Set "Firmware Upgrade and Provisioning" to "**Always Check for New Firmware**"
3. Go to "Firmware" section,

- 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: "192.168.5.218".
- Make sure to not include leading http:// in HTTP Firmware server path.
- You can verify the upgrade progress on the HFS Server as shown below:



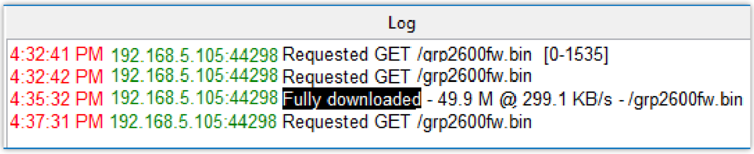
http://192.168.5.218:8080/grp2600fw.bin

```
9:34:07 AM 192.168.5.105:44298 Requested GET /grp2600fw.bin
```

IP address	File	Status	Speed	Time ...	Progress
192.168.5.105:44298	grp2600fw.bin	1,320,136 / 33,658,368 sent	-	-	3%

Firmware upgrade progress

- Once completed, a Fully downloaded log will be registered.



Log

```
4:32:41 PM 192.168.5.105:44298 Requested GET /grp2600fw.bin  [0-1535]
4:32:42 PM 192.168.5.105:44298 Requested GET /grp2600fw.bin
4:35:32 PM 192.168.5.105:44298 Fully downloaded - 49.9 M @ 299.1 KB/s - /grp2600fw.bin
4:37:31 PM 192.168.5.105:44298 Requested GET /grp2600fw.bin
```

Firmware File Fully Downloaded

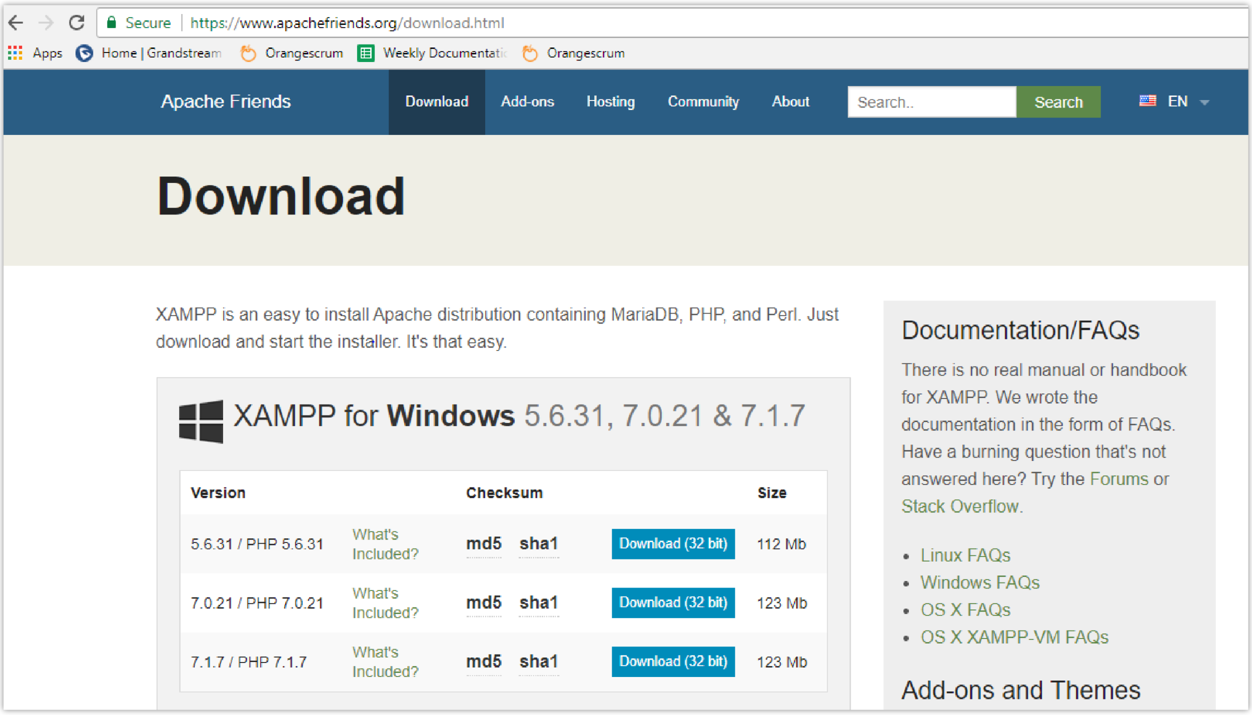
Local Upgrade via HTTPS Server

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.



Download

XAMPP is an easy to install Apache distribution containing MariaDB, PHP, and Perl. Just download and start the installer. It's that easy.

XAMPP for **Windows** 5.6.31, 7.0.21 & 7.1.7

Version		Checksum		Size
5.6.31 / PHP 5.6.31	What's Included?	md5 sha1	Download (32 bit)	112 Mb
7.0.21 / PHP 7.0.21	What's Included?	md5 sha1	Download (32 bit)	123 Mb
7.1.7 / PHP 7.1.7	What's Included?	md5 sha1	Download (32 bit)	123 Mb

Documentation/FAQs

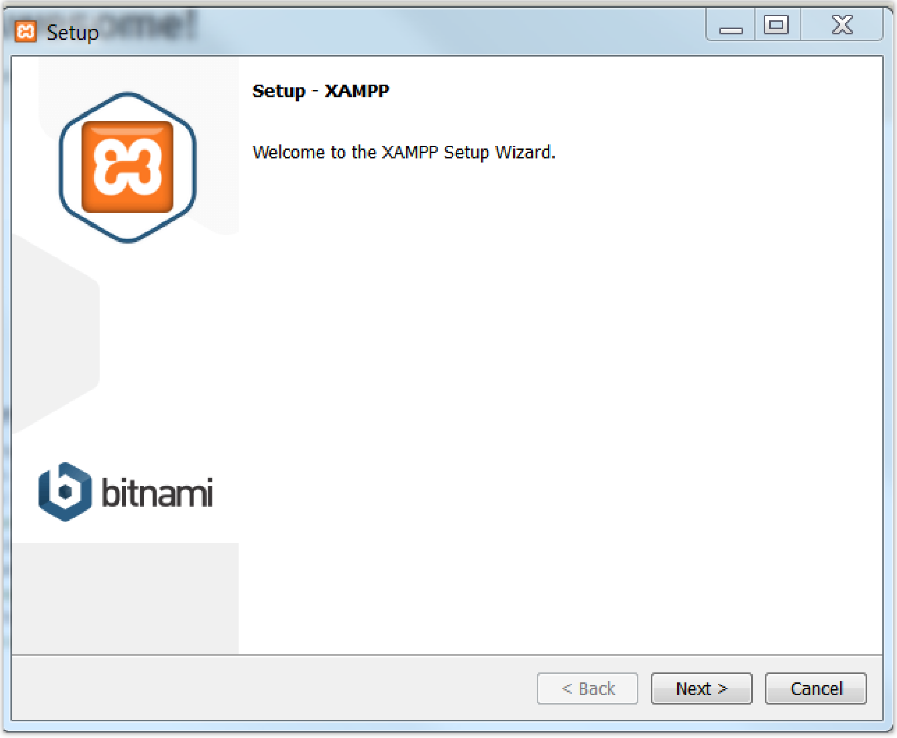
There is no real manual or handbook for XAMPP. We wrote the documentation in the form of FAQs. Have a burning question that's not answered here? Try the Forums or Stack Overflow.

- Linux FAQs
- Windows FAQs
- OS X FAQs
- OS X XAMPP-VM FAQs

Add-ons and Themes

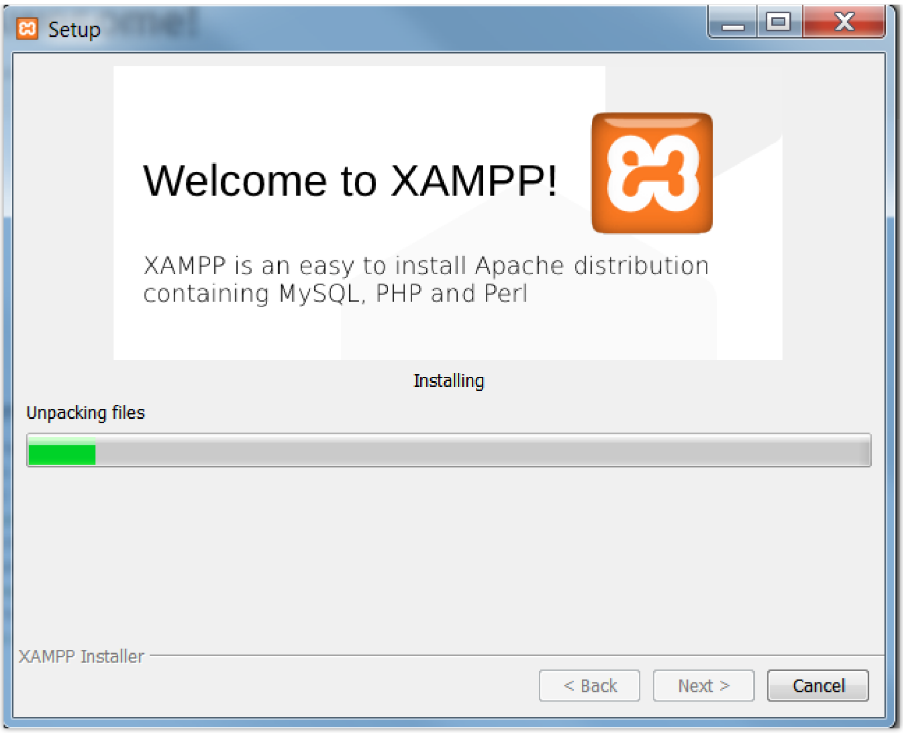
Download XAMPP for windows

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



Setup - XAMPP

Welcome to the XAMPP Setup Wizard.



Welcome to XAMPP!

XAMPP is an easy to install Apache distribution containing MySQL, PHP and Perl

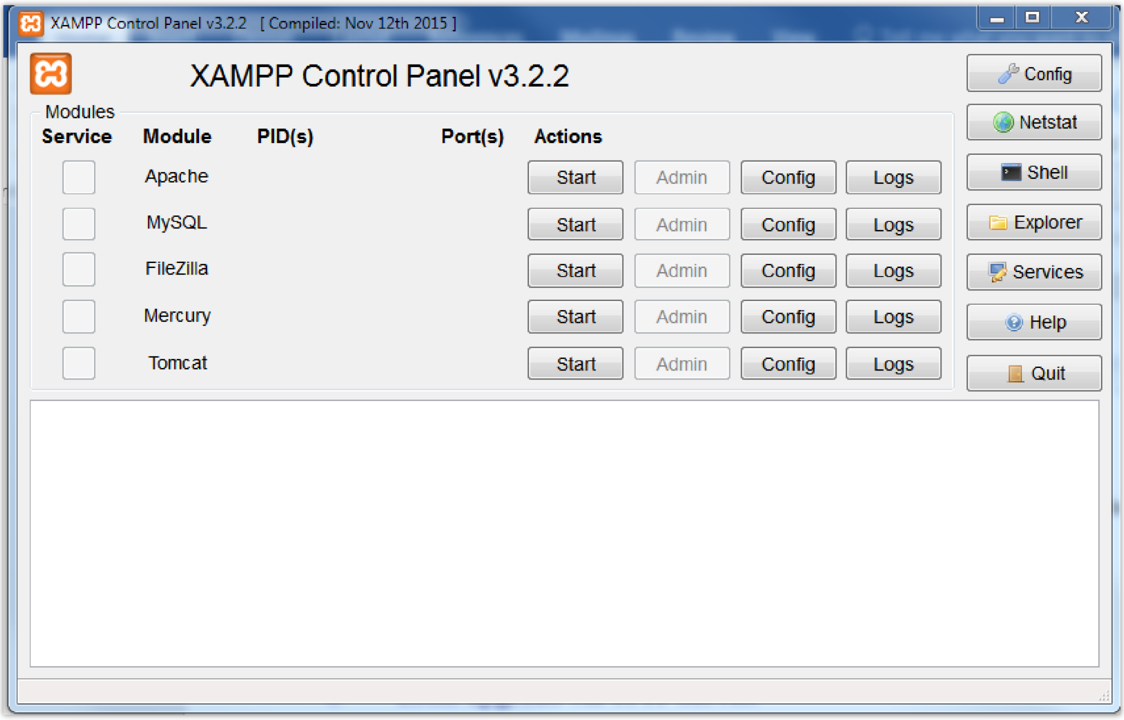
Installing

Unpacking files

XAMPP Installer

XAMPP Installation

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



XAMPP Control Panel v3.2.2

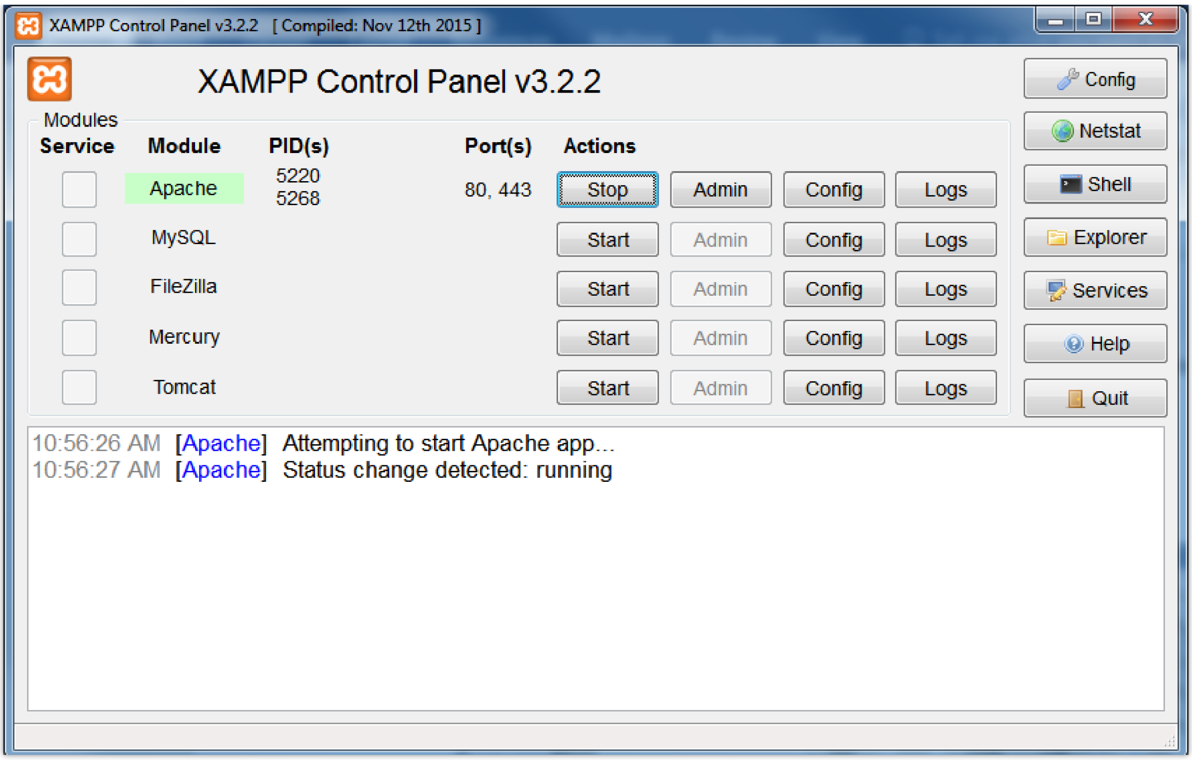
Modules

Service	Module	PID(s)	Port(s)	Actions			
□	Apache			Start	Admin	Config	Logs
□	MySQL			Start	Admin	Config	Logs
□	FileZilla			Start	Admin	Config	Logs
□	Mercury			Start	Admin	Config	Logs
□	Tomcat			Start	Admin	Config	Logs

XAMPP Control Panel

Uploading firmware file(s) to XAMPP HTTPS Server

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


XAMPP Control Panel v3.2.2 [Compiled: Nov 12th 2015]

XAMPP Control Panel v3.2.2

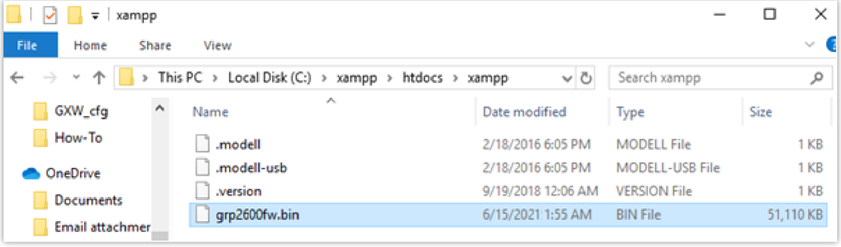
Modules

Service	Module	PID(s)	Port(s)	Actions
□	Apache	5220 5268	80, 443	Stop · Admin · Config · Logs
□	MySQL			Start · Admin · Config · Logs
□	FileZilla			Start · Admin · Config · Logs
□	Mercury			Start · Admin · Config · Logs
□	Tomcat			Start · Admin · Config · Logs

```
10:56:26 AM  [Apache]  Attempting to start Apache app...
10:56:27 AM  [Apache]  Status change detected: running
```

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***"

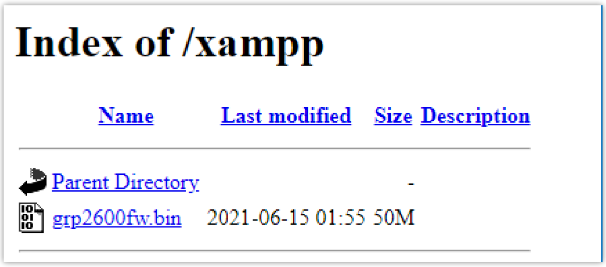

xampp

This PC › Local Disk (C:) › xampp › htdocs › xampp

Name	Date modified	Type	Size
.modell	2/18/2016 6:05 PM	MODELL File	1 KB
.modell-usb	2/18/2016 6:05 PM	MODELL-USB File	1 KB
.version	9/19/2018 12:06 AM	VERSION File	1 KB
grp2600fw.bin	6/15/2021 1:55 AM	BIN File	51,110 KB

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.


Index of /xampp

Name	Last modified	Size	Description
Parent Directory		-	
grp2600fw.bin	2021-06-15 01:55	50M	

Index of XAMPP Files

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:

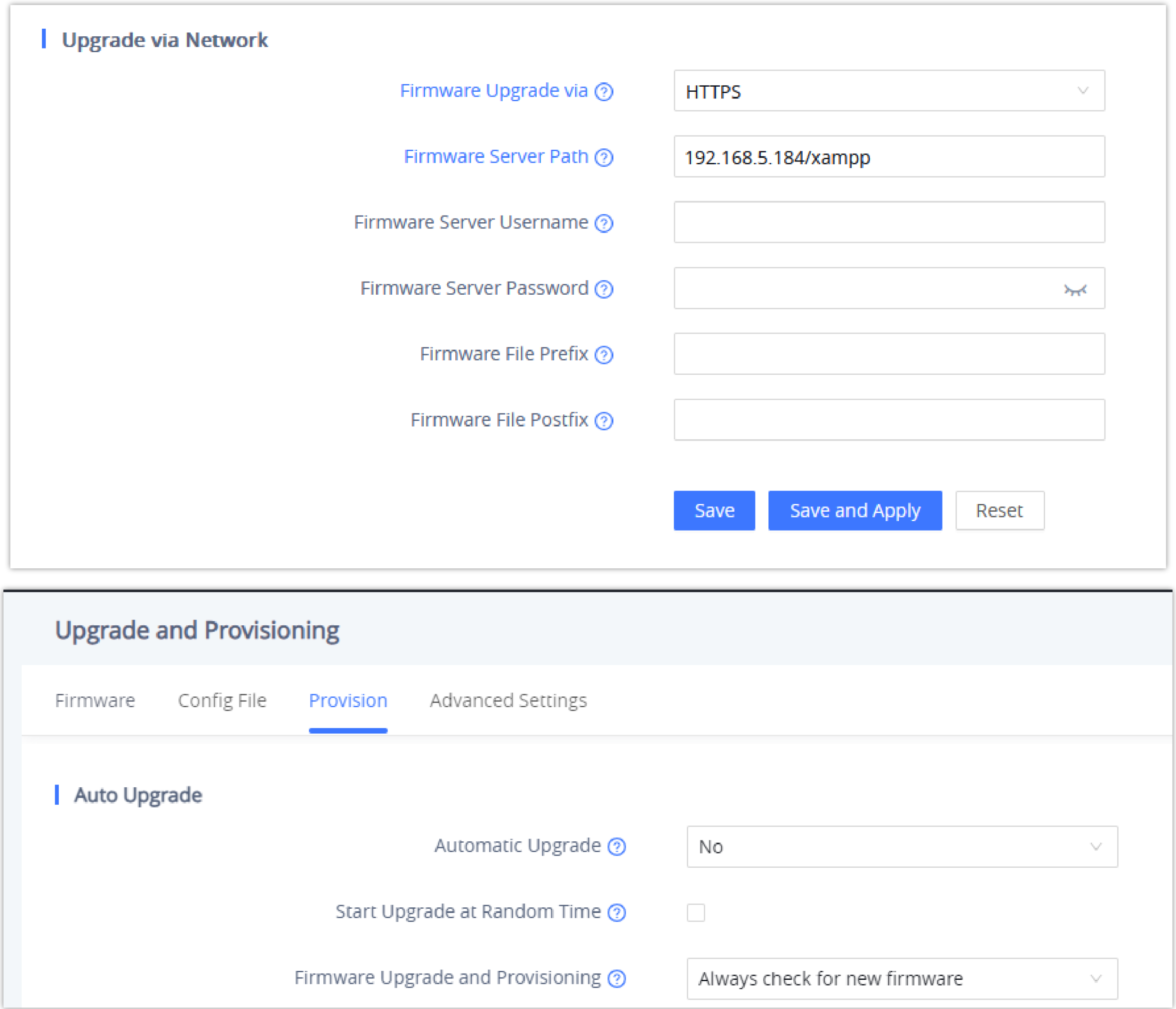
1. Access the Web GUI and navigate to "**Upgrade and Provisioning**" page.
2. Set "**Firmware Upgrade and Provisioning**" to "**Always Check for New Firmware**"
3. Go to "**Firmware**" section,

- 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.



Upgrade via Network

Firmware Upgrade via: HTTPS

Firmware Server Path: 192.168.5.184/xampp

Firmware Server Username:

Firmware Server Password:

Firmware File Prefix:

Firmware File Postfix:

Upgrade and Provisioning

Auto Upgrade

Automatic Upgrade: No

Start Upgrade at Random Time: □

Firmware Upgrade and Provisioning: Always check for new firmware

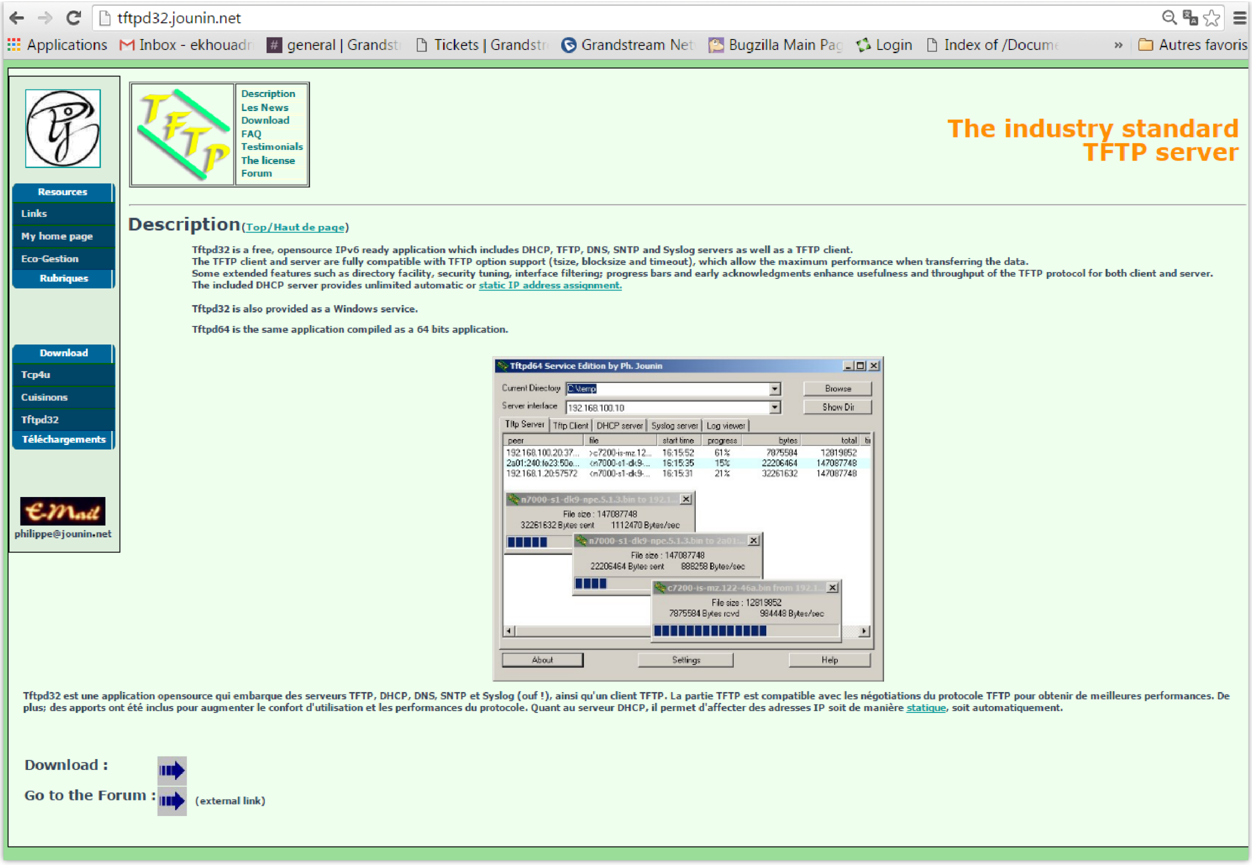
Example of Configuring the Upgrade via HTTPS on GRP26xx

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/



The industry standard
TFTP server

Description(Top/Haut de page)

Tftpd32 is a free, opensource IPv6 ready application which includes DHCP, TFTP, DNS, SNTP and Syslog servers as well as a TFTP client.
The TFTP client and server are fully compatible with TFTP option support (tsize, blocksize and timeout), which allow the maximum performance when transferring the data.
Some extended features such as directory facility, security tuning, interface filtering; progress bars and early acknowledgments enhance usefulness and throughput of the TFTP protocol for both client and server.
The included DHCP server provides unlimited automatic or static IP address assignment.

Tftpd32 is also provided as a Windows service.

Tftpd64 is the same application compiled as a 64 bits application.

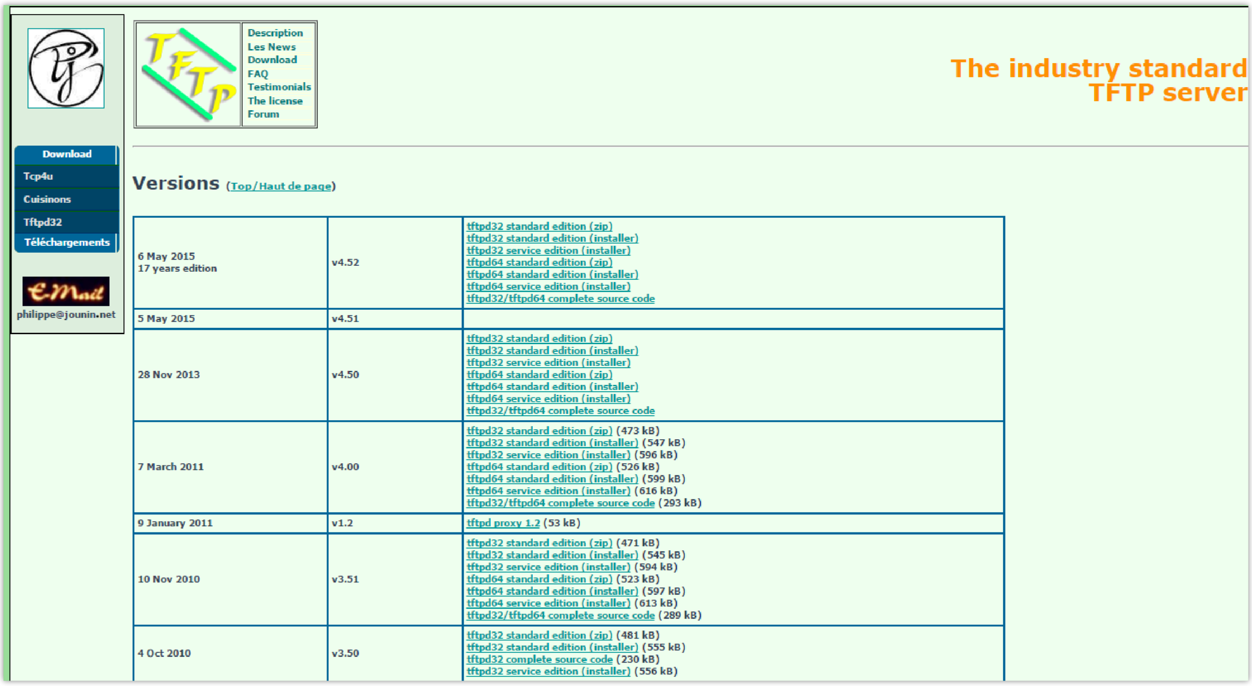
Tftpd32 est une application opensource qui embarque des serveurs TFTP, DHCP, DNS, SNTP et Syslog (ouf !), ainsi qu'un client TFTP. La partie TFTP est compatible avec les négotiations du protocole TFTP pour obtenir de meilleures performances. De plus; des apports ont été inclus pour augmenter le confort d'utilisation et les performances du protocole. Quant au serveur DHCP, il permet d'affecter des adresses IP soit de manière statique, soit automatiquement.

Download :

Go to the Forum : (external link)

Downloading the TFTP server

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



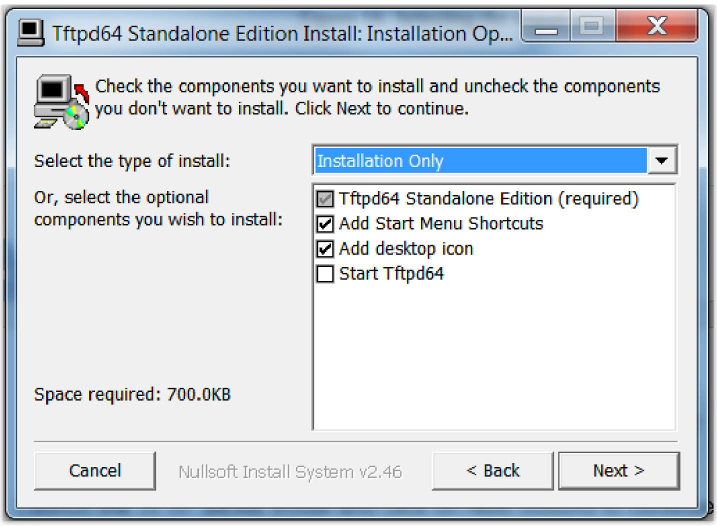
The industry standard
TFTP server

Versions (Top/Haut de page)

6 May 2015 17 years edition	v4.52	tftpd32 standard edition (zip) tftpd32 standard edition (installer) tftpd32 service edition (installer) tftpd64 standard edition (zip) tftpd64 standard edition (installer) tftpd64 service edition (installer) tftpd32/tftpd64 complete source code
5 May 2015	v4.51	
28 Nov 2013	v4.50	tftpd32 standard edition (zip) tftpd32 standard edition (installer) tftpd32 service edition (installer) tftpd64 standard edition (zip) tftpd64 standard edition (installer) tftpd64 service edition (installer) tftpd32/tftpd64 complete source code
7 March 2011	v4.00	tftpd32 standard edition (zip) (473 kB) tftpd32 standard edition (installer) (547 kB) tftpd32 service edition (installer) (596 kB) tftpd64 standard edition (zip) (526 kB) tftpd64 standard edition (installer) (599 kB) tftpd64 service edition (installer) (616 kB) tftpd32/tftpd64 complete source code (293 kB)
9 January 2011	v1.2	tftpd proxy 1.2 (53 kB)
10 Nov 2010	v3.51	tftpd32 standard edition (zip) (471 kB) tftpd32 standard edition (installer) (545 kB) tftpd32 service edition (installer) (594 kB) tftpd64 standard edition (zip) (523 kB) tftpd64 standard edition (installer) (597 kB) tftpd64 service edition (installer) (613 kB) tftpd32/tftpd64 complete source code (289 kB)
4 Oct 2010	v3.50	tftpd32 standard edition (zip) (481 kB) tftpd32 standard edition (installer) (555 kB) tftpd32 complete source code (230 kB) tftpd32 service edition (installer) (556 kB)

Selecting Install Version

2. Launch the TFTP server install wizard.



Tftpd64 Standalone Edition Install: Installation Op...

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select the type of install: Installation Only

Or, select the optional components you wish to install:

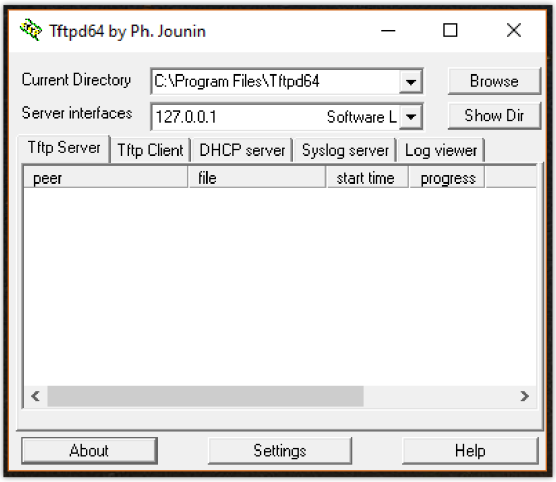
- ☑ Tftpd64 Standalone Edition (required)
- ☑ Add Start Menu Shortcuts
- ☑ Add desktop icon
- ☐ Start Tftpd64

Space required: 700.0KB

Nullsoft Install System v2.46

TFTP Server Installation

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



Tftpd64 by Ph. Jounin

Current Directory: C:\Program Files\Tftpd64

Server interfaces: 127.0.0.1 Software L

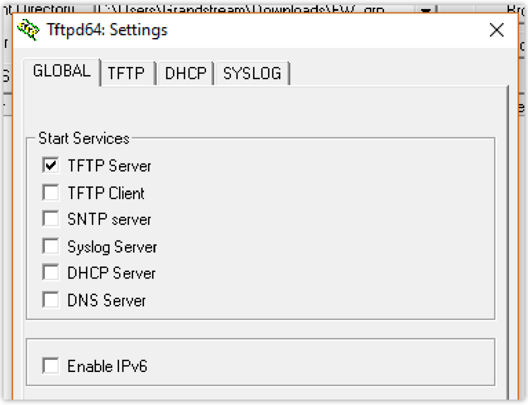
peer	file	start time	progress

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.



Tftpd64: Settings

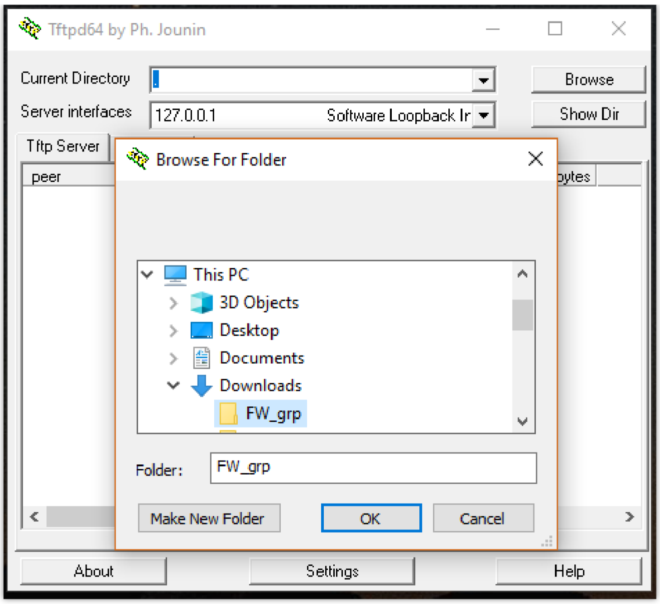
Start Services

- ☑ TFTP Server
- ☐ TFTP Client
- ☐ SNTP server
- ☐ Syslog Server
- ☐ DHCP Server
- ☐ DNS Server

☐ Enable IPv6

Selecting TFTP Server Services

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

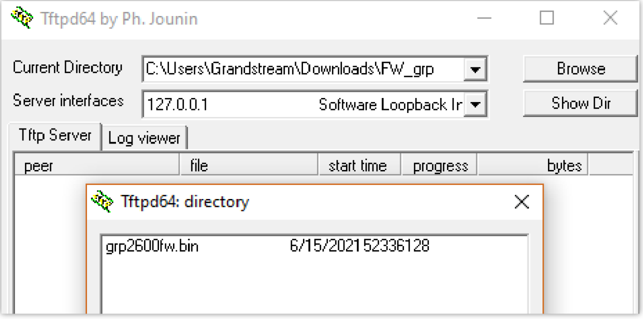


Server interfaces: 127.0.0.1 Software Loopback Ir

Folder: FW_grp

Selecting Local Directory containing Firmware File

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



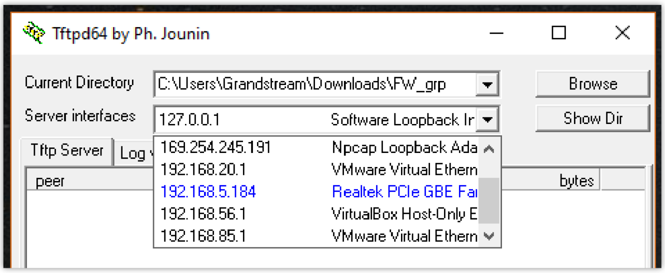
Current Directory: C:\Users\Grandstream\Downloads\FW_grp

Server interfaces: 127.0.0.1 Software Loopback Ir

```
grp2600fw.bin          6/15/2021 52336128
```

Firmware File Upload Verification

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



Current Directory: C:\Users\Grandstream\Downloads\FW_grp

Server interfaces: 127.0.0.1 Software Loopback Ir

```
169.254.245.191   Npcap Loopback Ada
192.168.20.1      VMware Virtual Ethern
192.168.5.184     Realtek PCIe GBE Fa
192.168.56.1      VirtualBox Host-Only E
192.168.85.1      VMware Virtual Ethern
```

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**".

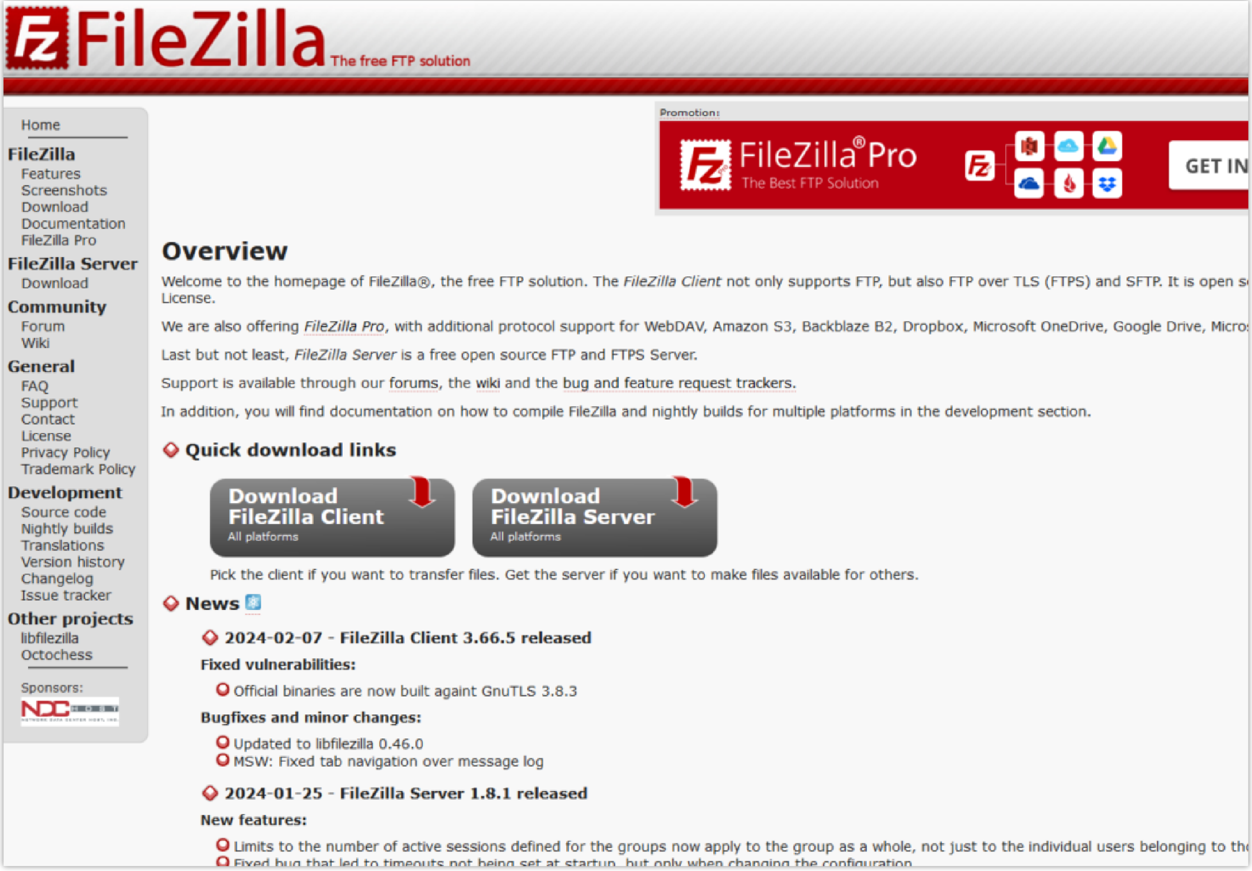
4. Press "**Save and Apply**" at the bottom of the page to apply the new settings.
5. **Reboot** the phone and wait until the upgrade process is completed.

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



Overview

Welcome to the homepage of FileZilla®, the free FTP solution. The *FileZilla Client* not only supports FTP, but also FTP over TLS (FTPS) and SFTP. It is open s License.

We are also offering *FileZilla Pro*, with additional protocol support for WebDAV, Amazon S3, Backblaze B2, Dropbox, Microsoft OneDrive, Google Drive, Micro

Last but not least, *FileZilla Server* is a free open source FTP and FTPS Server.

Support is available through our forums, the wiki and the bug and feature request trackers.

In addition, you will find documentation on how to compile FileZilla and nightly builds for multiple platforms in the development section.

Quick download links

Pick the client if you want to transfer files. Get the server if you want to make files available for others.

News

2024-02-07 - FileZilla Client 3.66.5 released

Fixed vulnerabilities:

- Official binaries are now built againt GnuTLS 3.8.3

Bugfixes and minor changes:

- Updated to libfilezilla 0.46.0
- MSW: Fixed tab navigation over message log

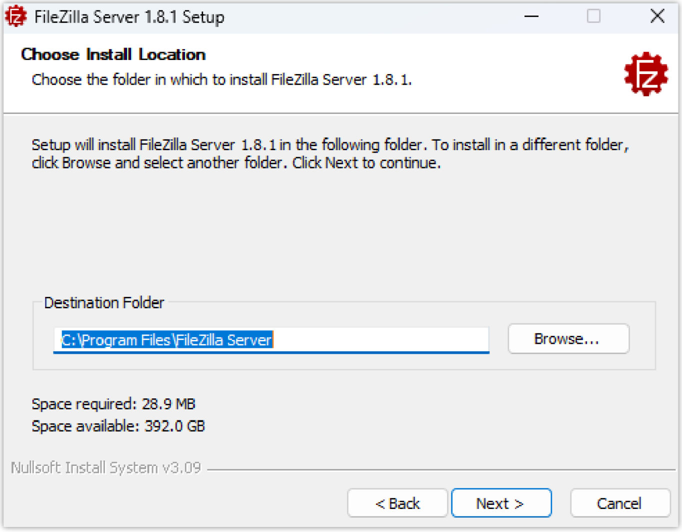
2024-01-25 - FileZilla Server 1.8.1 released

New features:

- Limits to the number of active sessions defined for the groups now apply to the group as a whole, not just to the individual users belonging to the
- Fixed bug that led to timeouts not being set at startup, but only when changing the configuration

FTP/FTPS Server Download Page

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



Choose Install Location

Choose the folder in which to install FileZilla Server 1.8.1.

Setup will install FileZilla Server 1.8.1 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

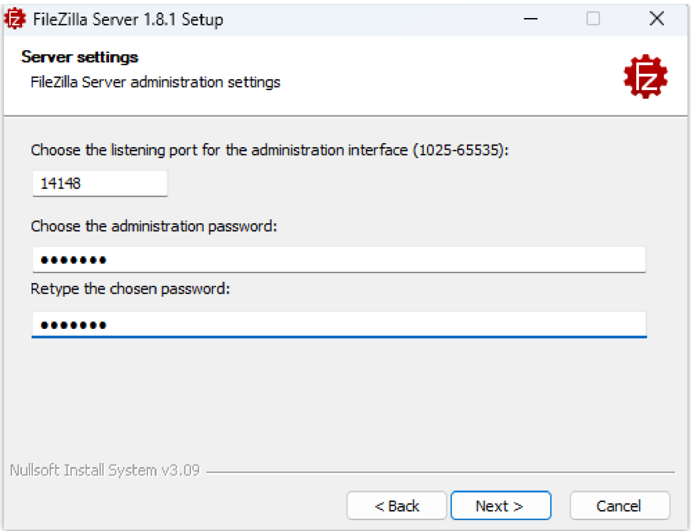
Destination Folder: C:\Program Files\FileZilla Server

Space required: 28.9 MB

Space available: 392.0 GB

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")*.



FileZilla Server 1.8.1 Setup

Server settings

FileZilla Server administration settings

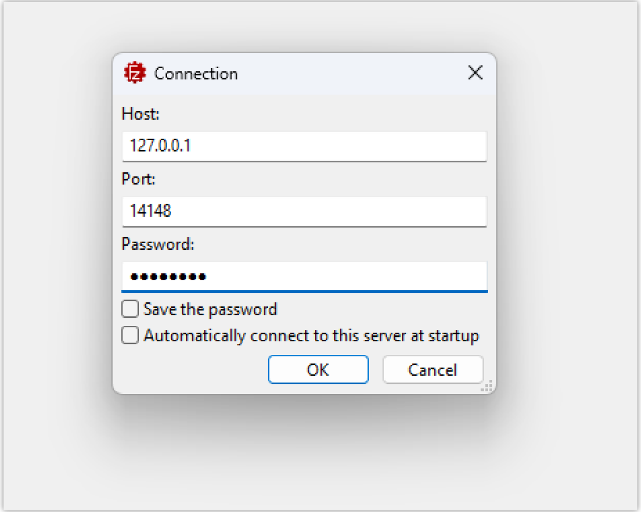
Choose the listening port for the administration interface (1025-65535): 14148

Choose the administration password: •••••••

Retype the chosen password: •••••••

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**.



Connection

Host: 127.0.0.1

Port: 14148

Password: ••••••••

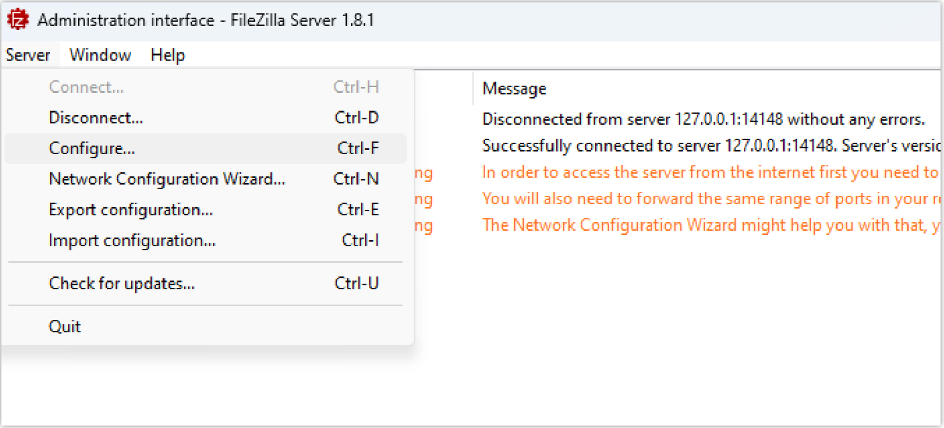
□ Save the password

□ Automatically connect to this server at startup

FTP/FTPS Server Connection Page

Configuring the FTP Server

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



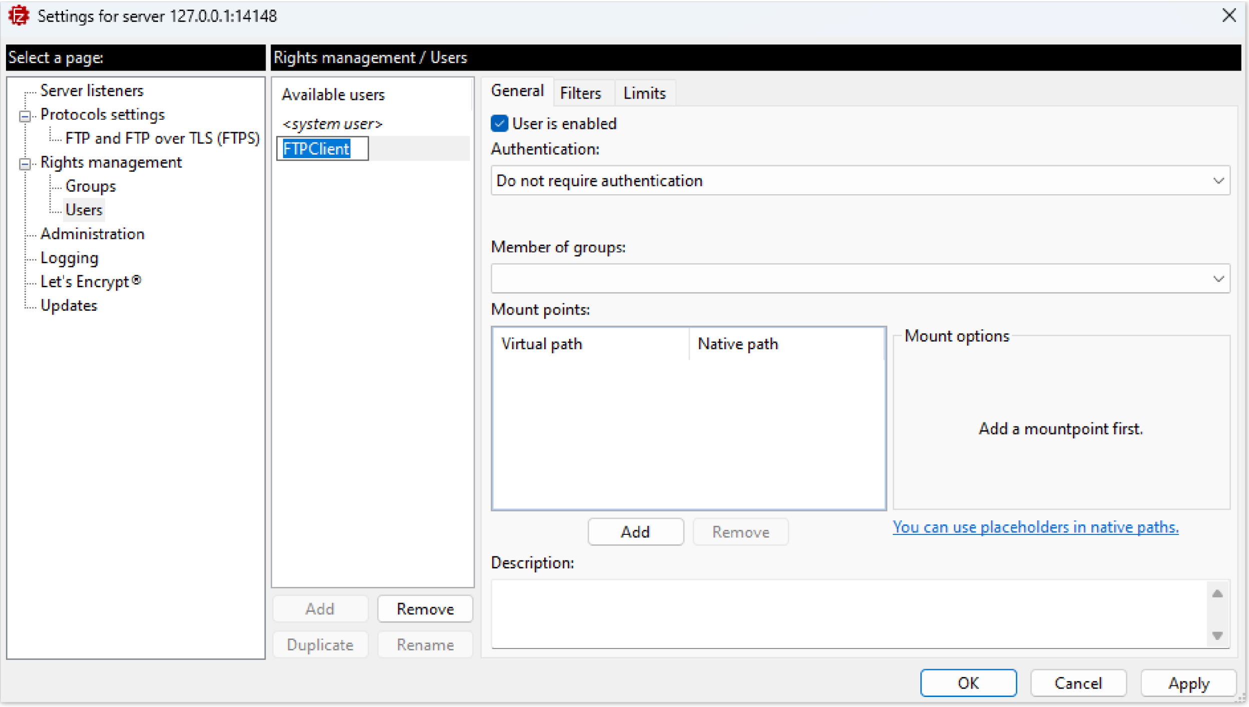
Administration interface - FileZilla Server 1.8.1

Server
Window
Help
Connect... Ctrl-H
Disconnect... Ctrl-D
Configure... Ctrl-F
Network Configuration Wizard... Ctrl-N
Export configuration... Ctrl-E
Import configuration... Ctrl-I
Check for updates... Ctrl-U
Quit

```
Message
Disconnected from server 127.0.0.1:14148 without any errors.
Successfully connected to server 127.0.0.1:14148. Server's versic
In order to access the server from the internet first you need to
You will also need to forward the same range of ports in your r
The Network Configuration Wizard might help you with that, y
```

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”).*



Settings for server 127.0.0.1:14148

Rights management / Users

Available users

<system user>

FTPClient

☑ User is enabled

Authentication: Do not require authentication

Member of groups:

Mount points:

Virtual path	Native path

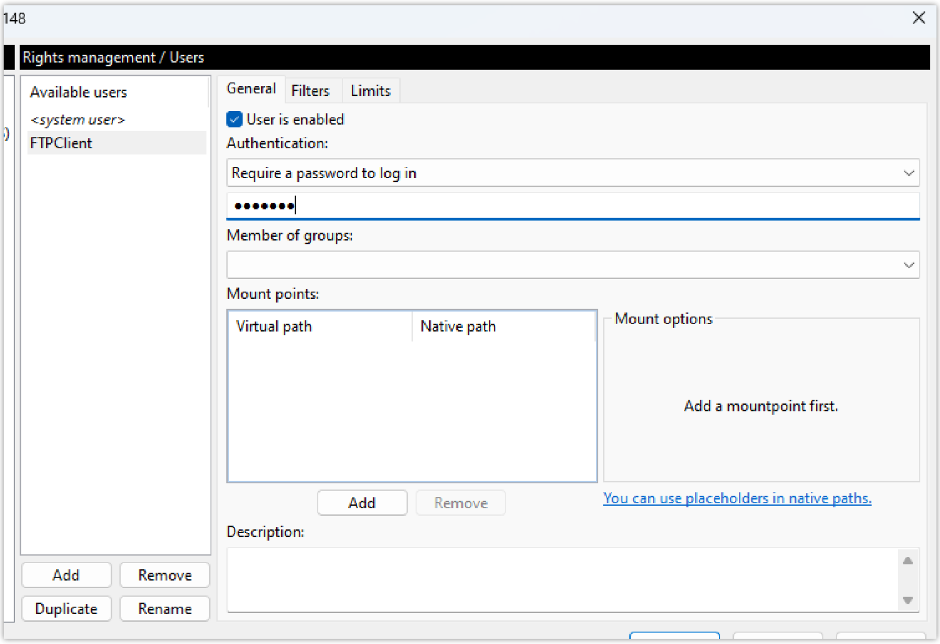
Mount options: Add a mountpoint first.

You can use placeholders in native paths.

Description:

Example of adding FTP user

3. For authentication, choose the option “**Require a password to log in**” and enter the user’s password.



Rights management / Users

Available users

<system user>

FTPClient

☑ User is enabled

Authentication: Require a password to log in

•••••••

Member of groups:

Mount points:

Virtual path	Native path

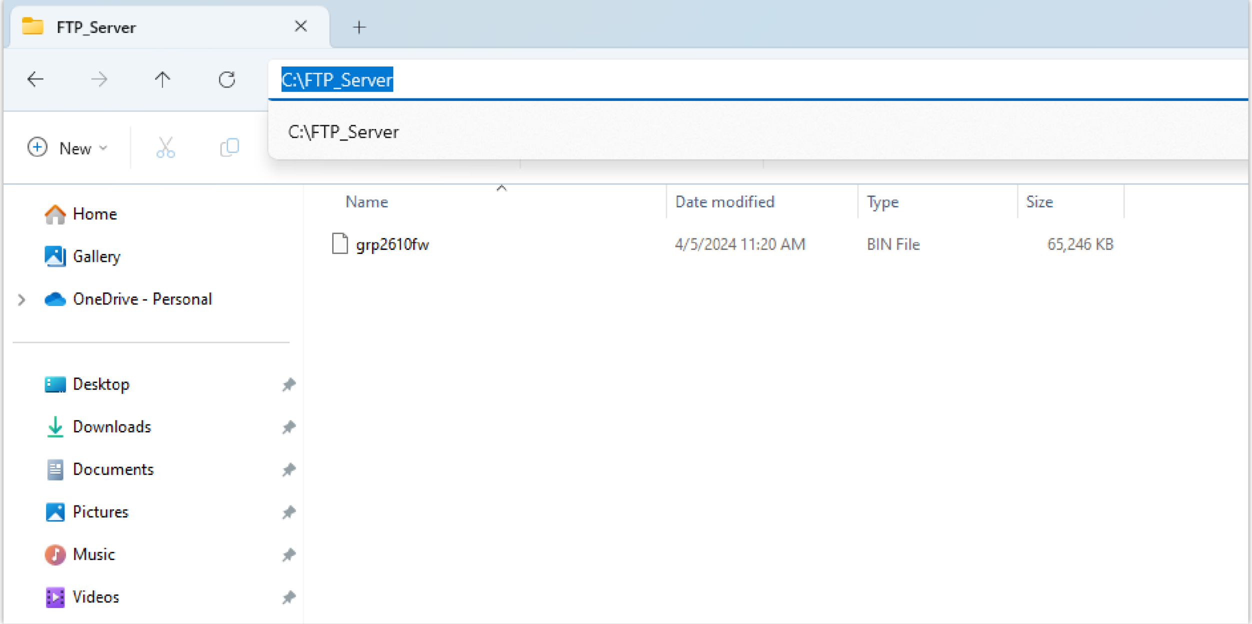
Mount options: Add a mountpoint first.

You can use placeholders in native paths.

Description:

FTP user authentication

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



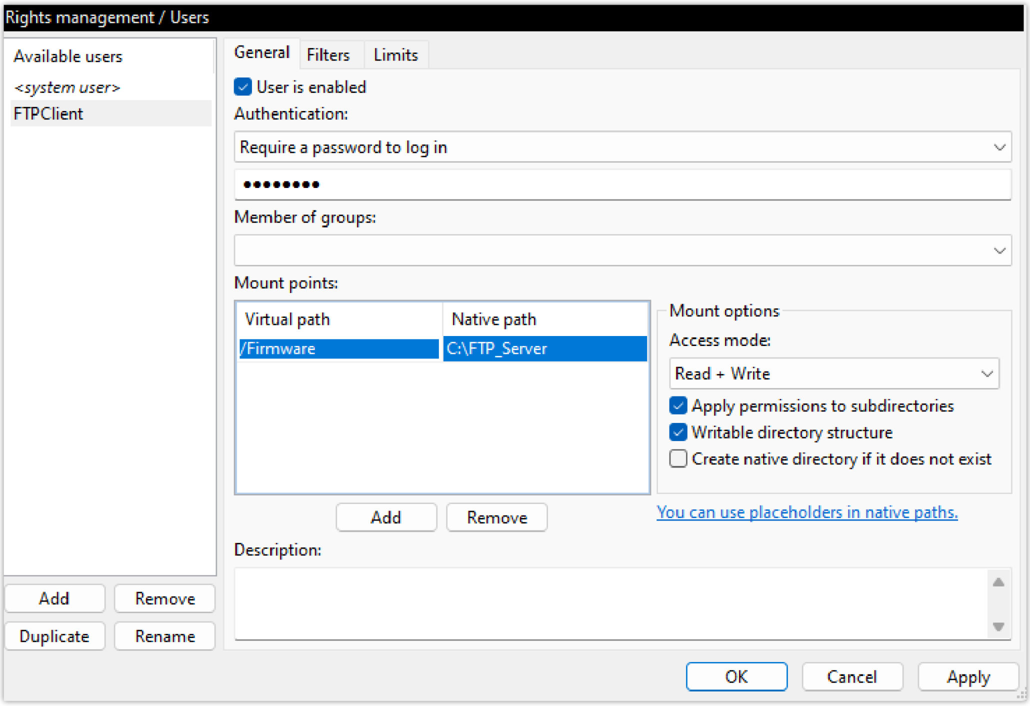
C:\FTP_Server

Name	Date modified	Type	Size
grp2610fw	4/5/2024 11:20 AM	BIN File	65,246 KB

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**").*



Rights management / Users

Available users

<system user>

FTPClient

☑ User is enabled

Authentication: Require a password to log in

••••••••

Member of groups:

Mount points:

Virtual path	Native path
/Firmware	C:\FTP_Server

Mount options

Access mode: Read + Write

☑ Apply permissions to subdirectories

☑ Writable directory structure

☐ Create native directory if it does not exist

You can use placeholders in native paths.

Description:

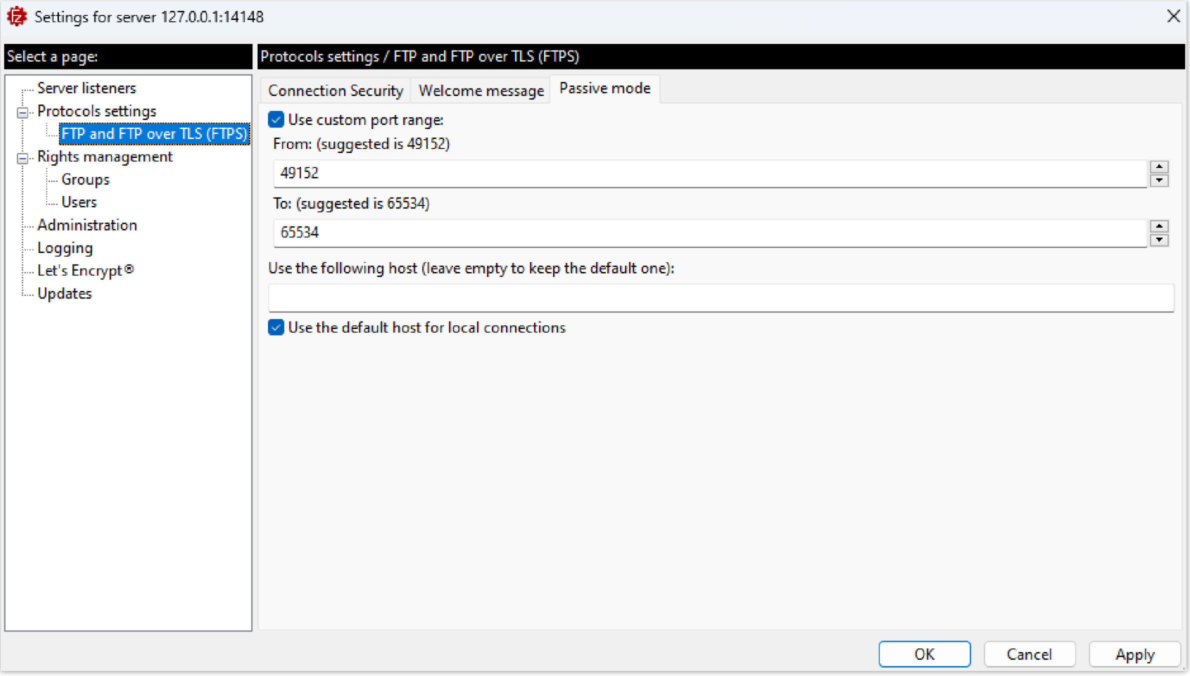
Adding Mount points for FTP user

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.



Settings for server 127.0.0.1:14148

Protocols settings / FTP and FTP over TLS (FTPS)

☑ Use custom port range:

From: (suggested is 49152)

49152

To: (suggested is 65534)

65534

Use the following host (leave empty to keep the default one):

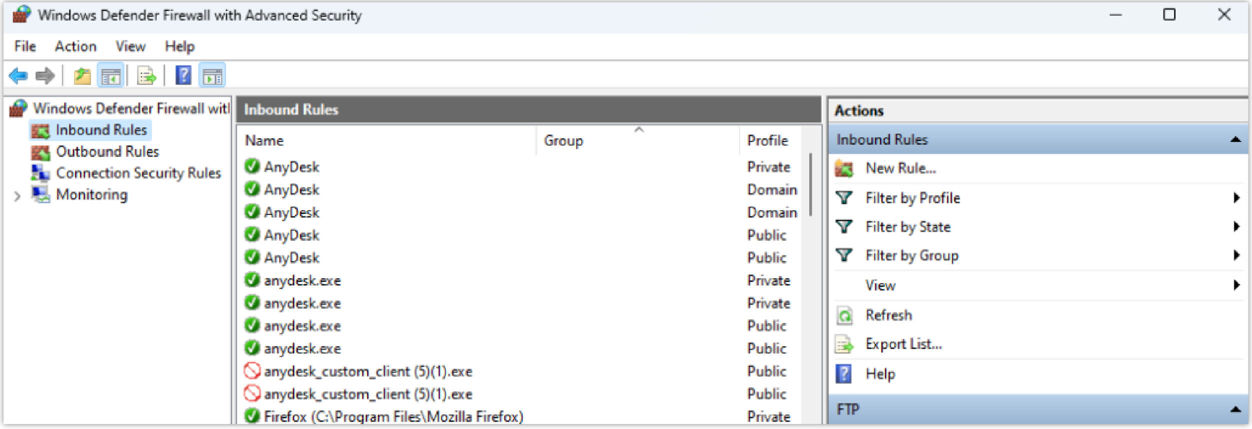
☑ Use the default host for local connections

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 well as 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**".



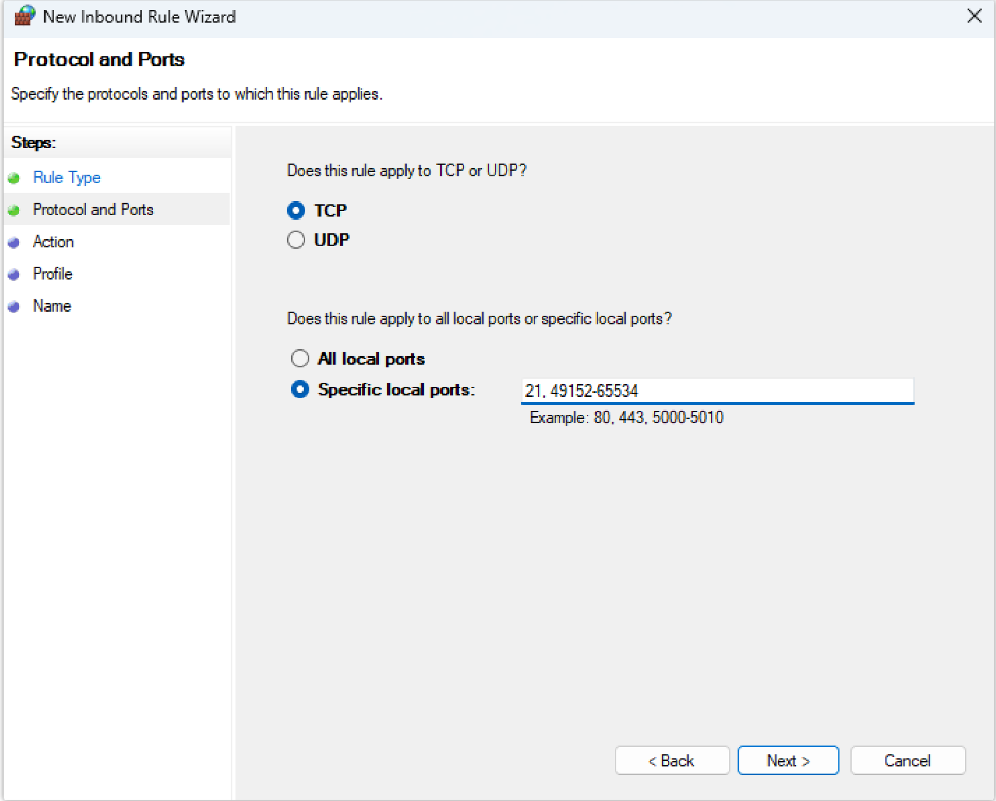
Windows Defender Firewall with Advanced Security

Inbound Rules

Name	Group	Profile
✓ AnyDesk		Private
✓ AnyDesk		Domain
✓ AnyDesk		Domain
✓ AnyDesk		Public
✓ AnyDesk		Public
✓ anydesk.exe		Private
✓ anydesk.exe		Private
✓ anydesk.exe		Public
✓ anydesk.exe		Public
⊘ anydesk_custom_client (5)(1).exe		Public
⊘ anydesk_custom_client (5)(1).exe		Public
✓ Firefox (C:\Program Files\Mozilla Firefox)		Private

Windows Defender Firewall with Advanced Security (Inbound Rules)

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


New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● TCP
○ UDP

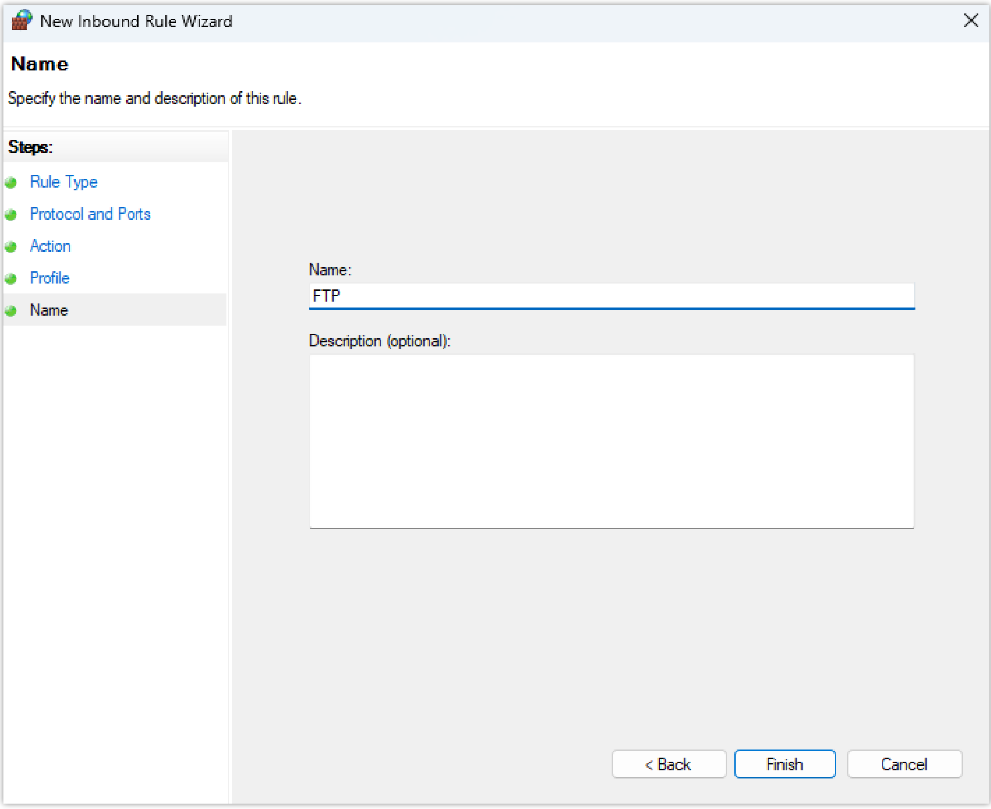
Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 21, 49152-65534

Example: 80, 443, 5000-5010

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 Wizard

Name

Specify the name and description of this rule.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name: FTP

Description (optional):

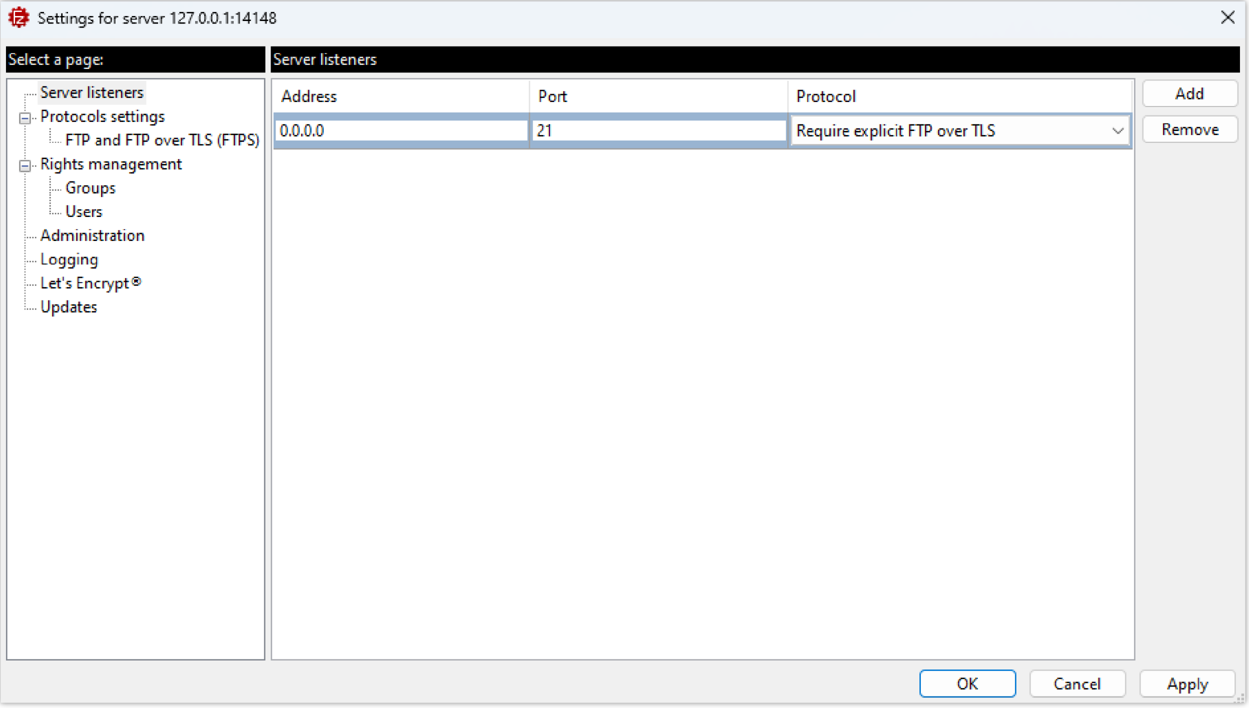
New Inbound Rule Name

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.



Server listeners

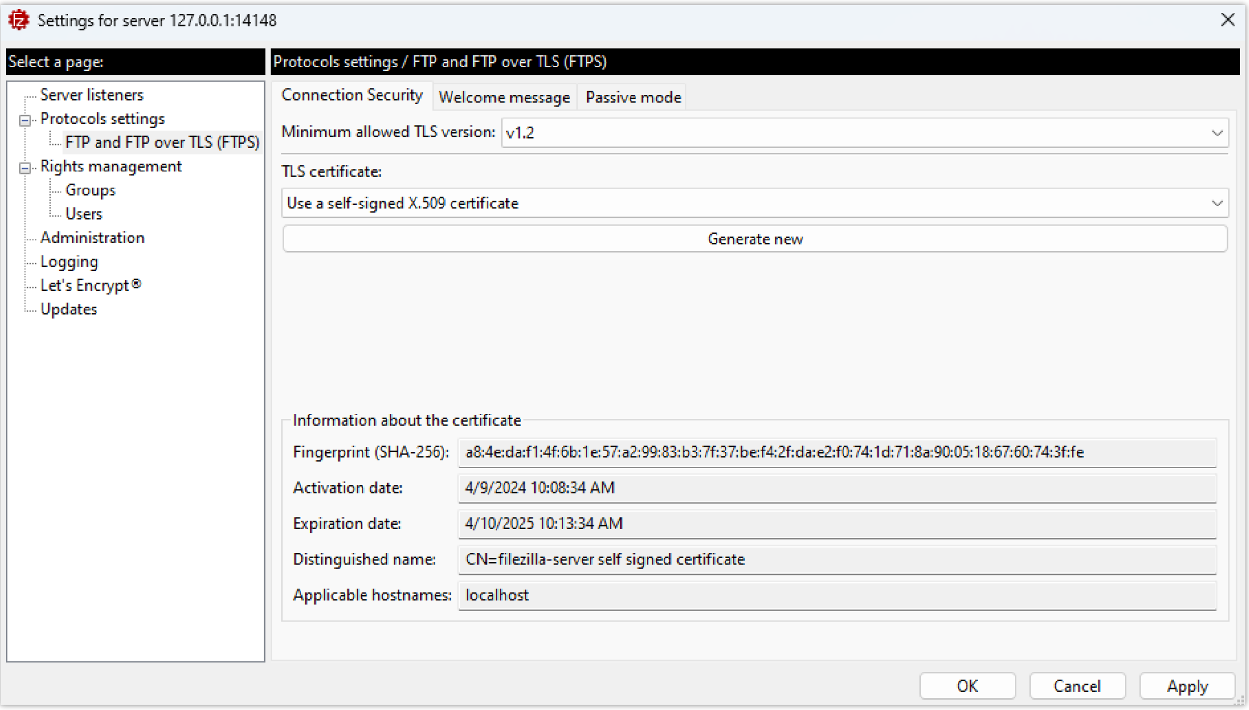
Address	Port	Protocol
0.0.0.0	21	Require explicit FTP over TLS

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 over TLS (FTPS)**” page from the server’s configuration settings.



Protocols settings / FTP and FTP over TLS (FTPS)

Minimum allowed TLS version: v1.2

TLS certificate: Use a self-signed X.509 certificate

Information about the certificate

Fingerprint (SHA-256):	a8:4e:da:f1:4f:6b:1e:57:a2:99:83:b3:7f:37:be:f4:2f:da:e2:f0:74:1d:71:8a:90:05:18:67:60:74:3f:fe
Activation date:	4/9/2024 10:08:34 AM
Expiration date:	4/10/2025 10:13:34 AM
Distinguished name:	CN=filezilla-server self signed certificate
Applicable hostnames:	localhost

TLS Certificate

Configuring Grandstream devices for local FTP/FTPS upgrade

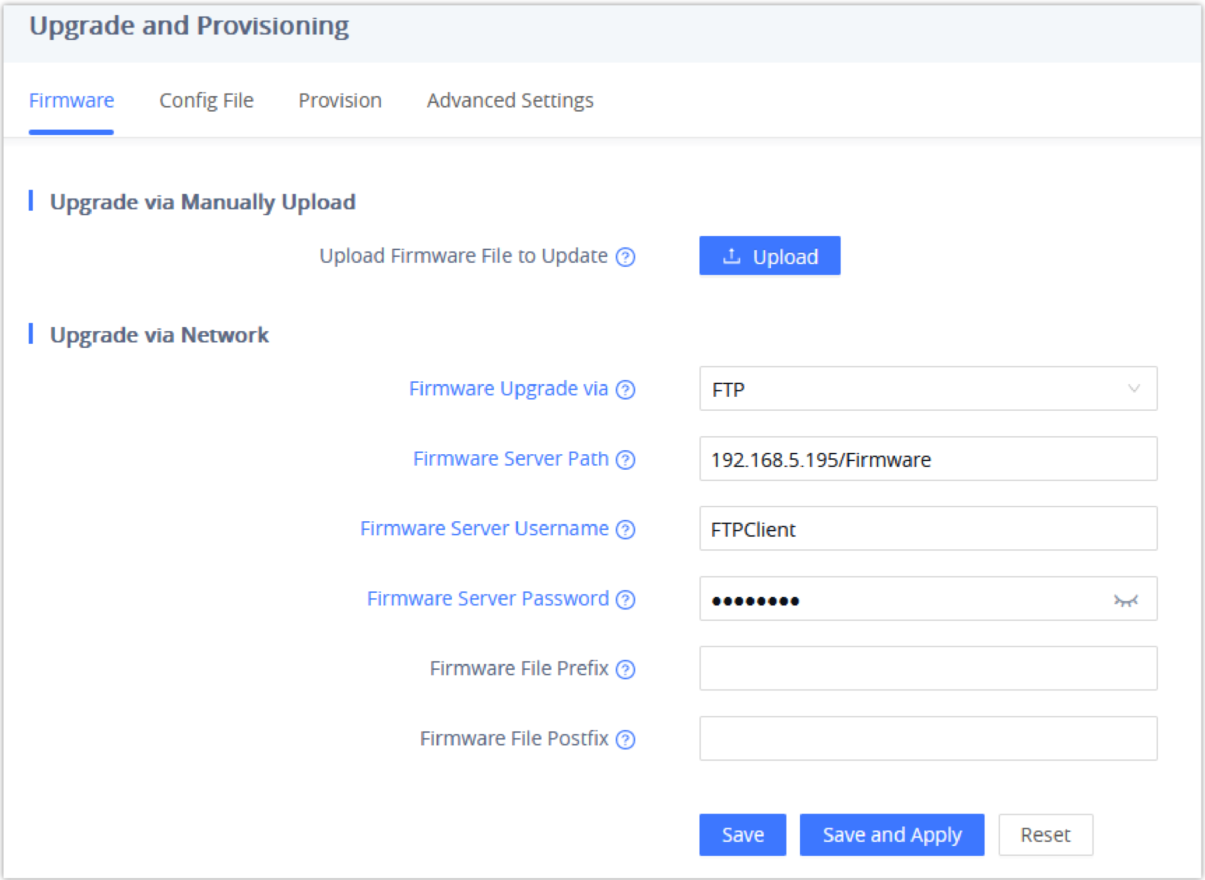
Please follow the steps below to configure Grandstream devices to upgrade their firmware via FTP:

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.


Upgrade and Provisioning

Upgrade via Manually Upload

Upload Firmware File to Update

Upgrade via Network

Firmware Upgrade via: FTP

Firmware Server Path: 192.168.5.195/Firmware

Firmware Server Username: FTPClient

Firmware Server Password: ••••••••

Firmware File Prefix:

Firmware File Postfix:

Example of configuring the Upgrade via FTP on GRP26xx

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.

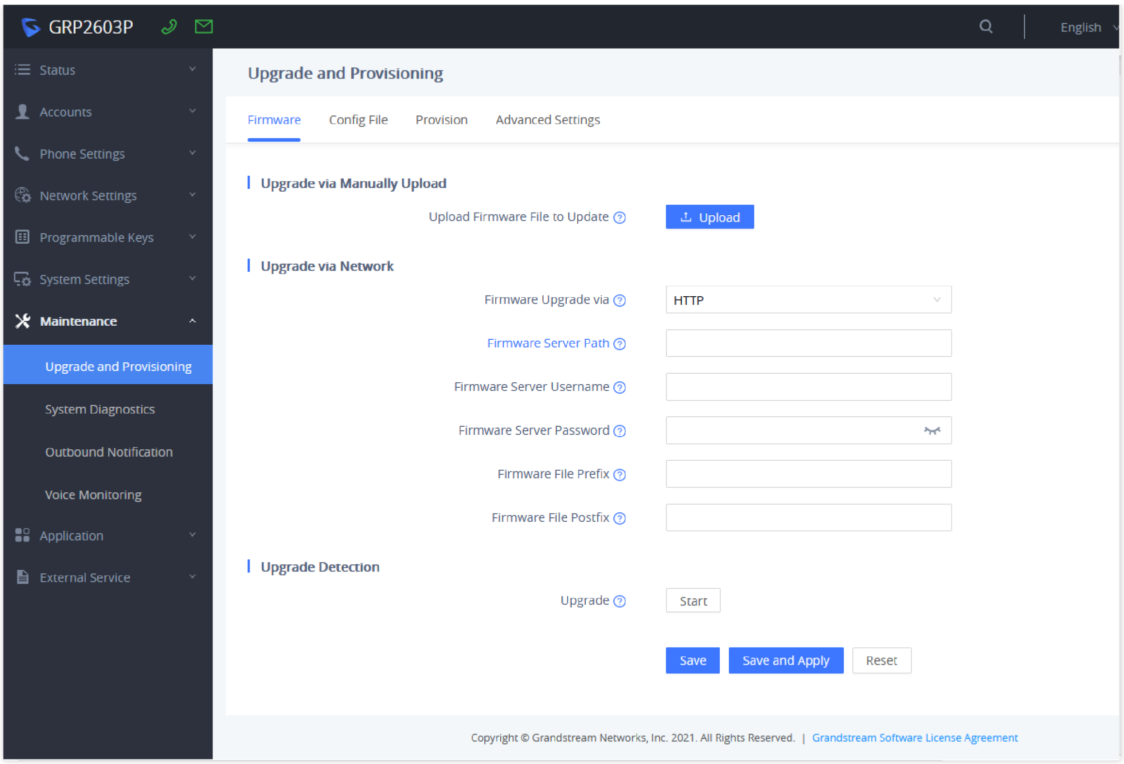
Scenario 3: Upgrade through Manual Upload

It is also possible to perform the firmware upgrade manually from the GRP26xx Web GUI.

To achieve this, first download firmware files for the appropriate device model from http://www.grandstream.com/support/firmware. Unzip downloaded package.

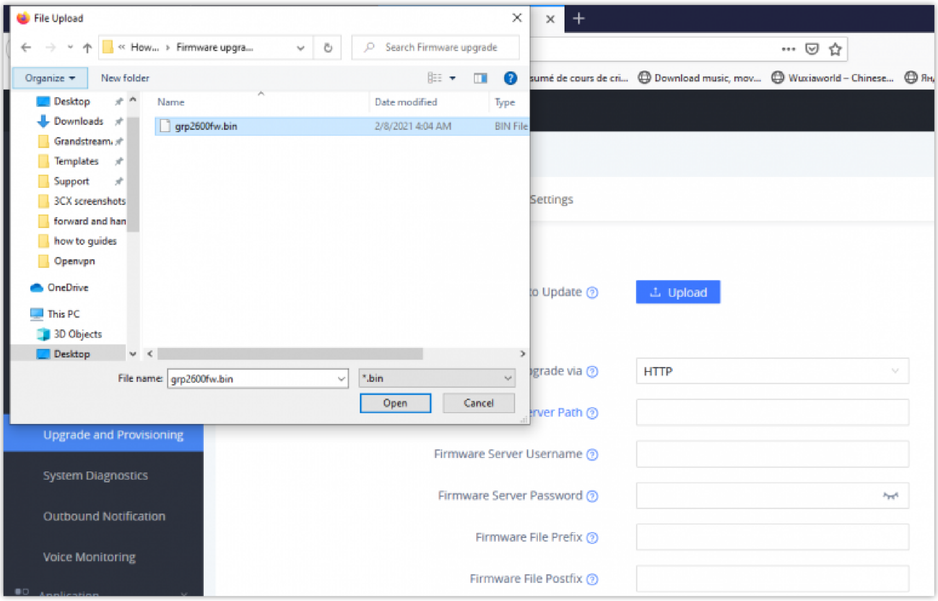
This method can only be done from the Web GUI.

1. Start by accessing the Web GUI and navigate to **Maintenance >> Upgrade and Provisioning**.



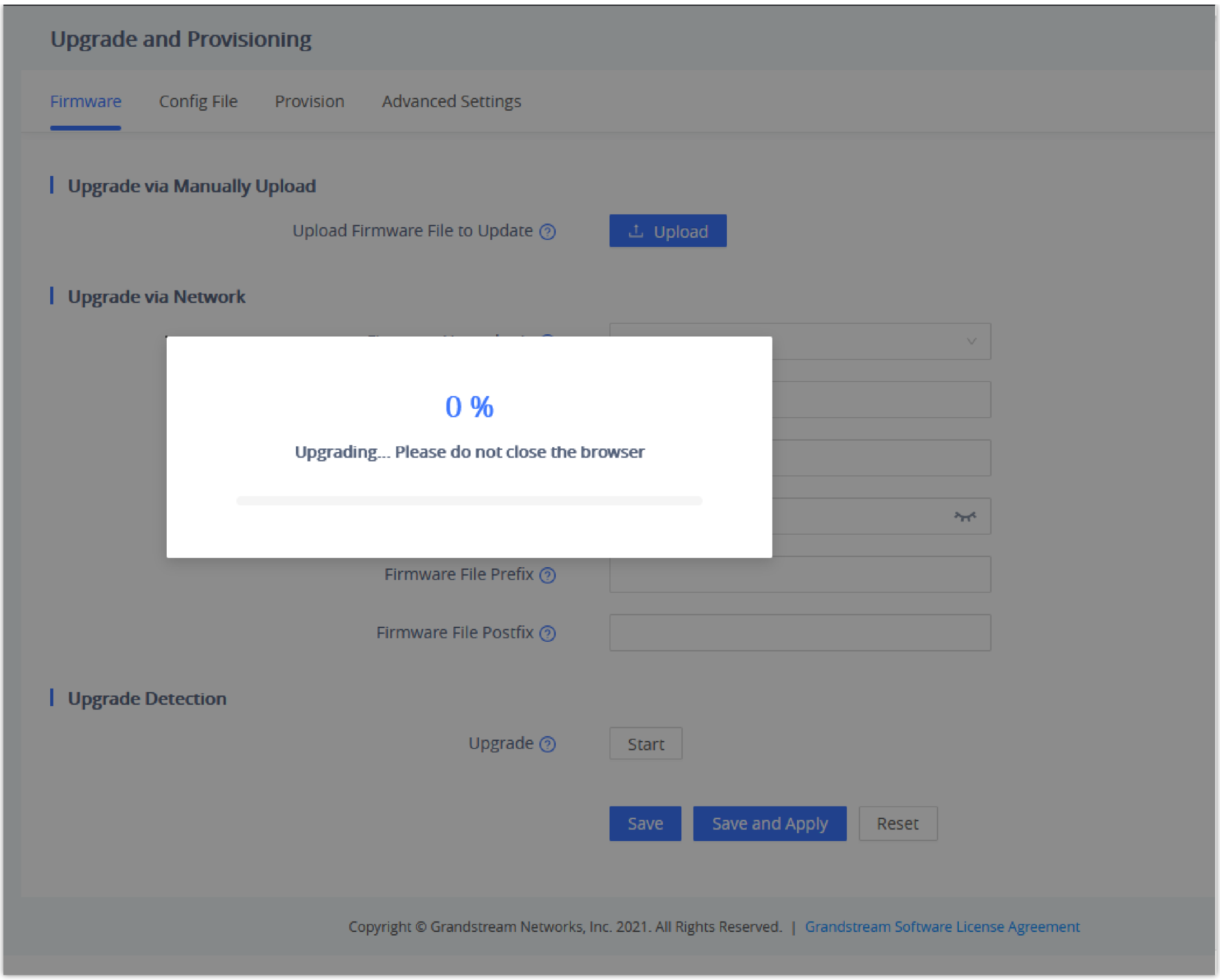
Manual upload page on GRP26xx

2. Click on Upload, and then browse to the firmware file downloaded and unzipped, this file is in BIN format, and select Open.



Browsing to the Firmware BIN file location For GRP26xx

3. The Phone GUI will show a bar describing the progress of the firmware upgrade , wait until the GRP26xx finishes the firmware Upgrade, and the phone will automatically reboot showing , once the firmware upgrade is done.



Upgrade and Provisioning

Upgrade via Manually Upload

Upload Firmware File to Update

Upgrade via Network

0 %

Upgrading... Please do not close the browser

Firmware File Prefix

Firmware File Postfix

Upgrade Detection

Upgrade

Copyright © Grandstream Networks, Inc. 2021. All Rights Reserved. | Grandstream Software License Agreement

Upgrade in progress for GRP26xx

Important:

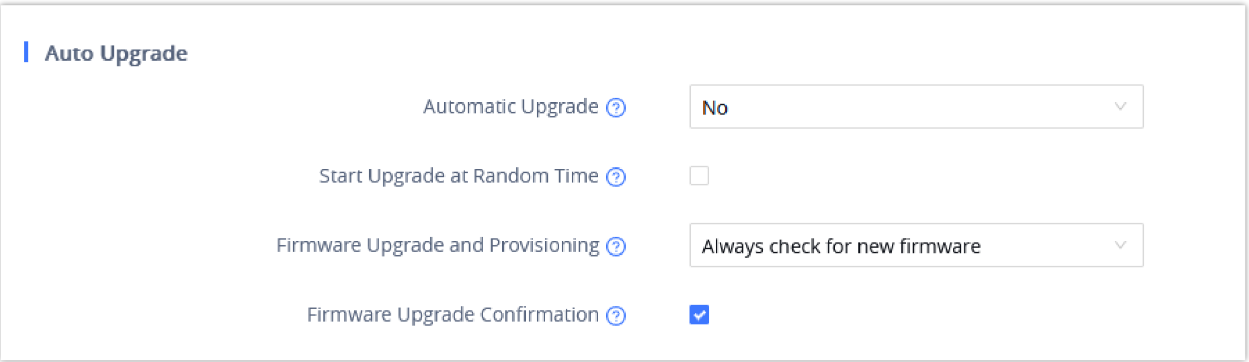
Do not close the browser when performing the Manual Upgrade.

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.

For the **GRP26xx**, navigate to **Maintenance → Upgrade and provisioning** under **Provision** Tab.



Auto Upgrade

Automatic Upgrade: No

Start Upgrade at Random Time: □

Firmware Upgrade and Provisioning: Always check for new firmware

Firmware Upgrade Confirmation: ☑

Example of Configuring Automatic Upgrade for 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)

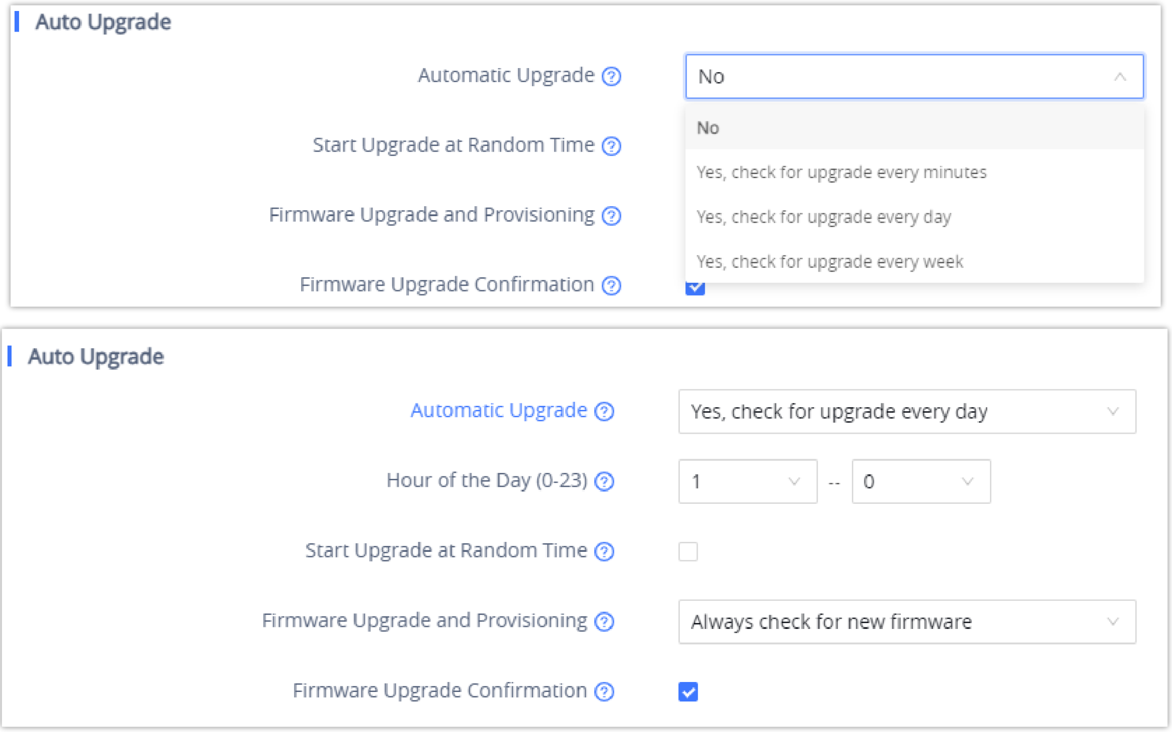
The device will check the firmware file availability in the specified time interval. If found, it will be downloaded, and the upgrade process will be initiated automatically.

Note:

For GRP26xx, in order to have the access to edit the check for the firmware schedule, we will need at first to change the Automatic Upgrade from No to one of the following :

- Yes, check for upgrade every Minute,
- Yes, check for upgrade every Day,
- Yes, check for upgrade every Week.

And then we can adjust the settings according to our deployment and our needs,



Auto Upgrade

Automatic Upgrade: No

No
Yes, check for upgrade every minutes
Yes, check for upgrade every day
Yes, check for upgrade every week
Start Upgrade at Random Time
Firmware Upgrade and Provisioning
Firmware Upgrade Confirmation

Auto Upgrade

Automatic Upgrade: Yes, check for upgrade every day

Hour of the Day (0-23): 1 -- 0

Start Upgrade at Random Time: □

Firmware Upgrade and Provisioning: Always check for new firmware

Firmware Upgrade Confirmation: ☑

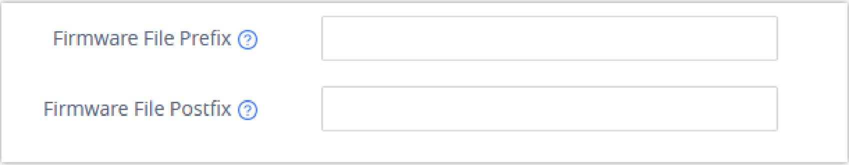
Example of Configuring Automatic Upgrade for GRP26xx

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**.

For **GRP26xx**, this can be found under the Firmware Tab.



Firmware File Prefix:

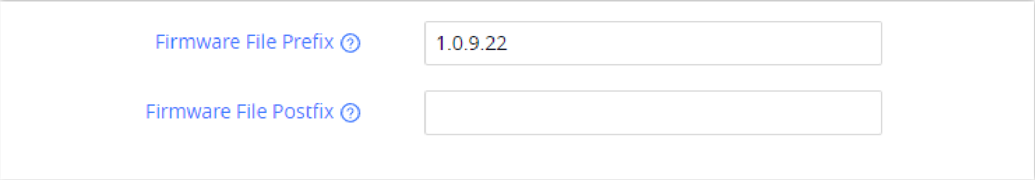
Firmware File Postfix:

Screenshot of Firmware file Prefix and Postfix fields for GRP26xx

Use Case Example:

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

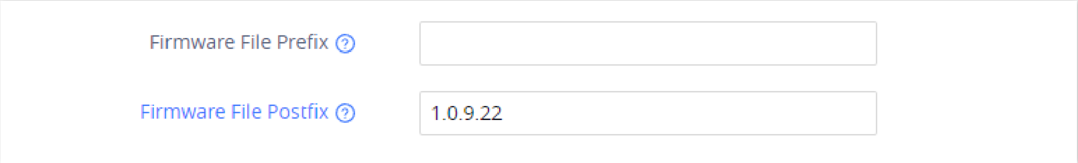
- If **Firmware File Prefix** is set to *1.0.9.22* on a GRP26XX series phone, for example, requested firmware file will be *1.0.9.22grp2610fw.bin*



Firmware File Prefix	1.0.9.22
Firmware File Postfix	

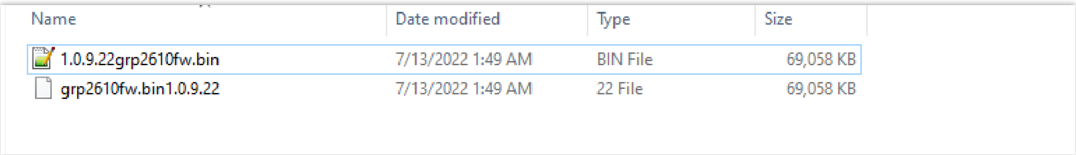
Configuring the Firmware File Prefix

- If **Firmware File Postfix** is set to *1.0.9.22* on a GRP26XX series phone, for example, requested firmware file will be *grp2610fw.bin1.0.9.22*



Firmware File Prefix	
Firmware File Postfix	1.0.9.22

Configuring the Firmware File Postfix



Name	Date modified	Type	Size
1.0.9.22grp2610fw.bin	7/13/2022 1:49 AM	BIN File	69,058 KB
grp2610fw.bin1.0.9.22	7/13/2022 1:49 AM	22 File	69,058 KB

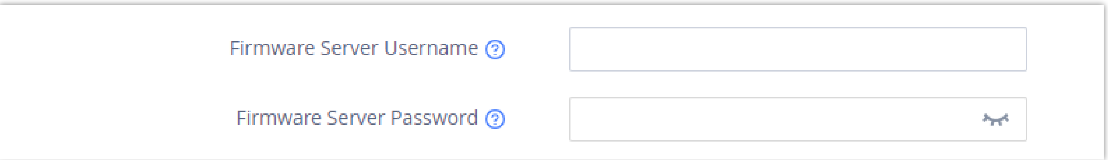
Firmware Files with Prefix/Postfix on the local directory

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 files before being challenged by the server. The default setting is "No".



Firmware Server Username	
Firmware Server Password	

Screenshot of Firmware Server Username and Password Fields for GRP26xx