Grandstream Networks, Inc.

SIP Device Provisioning Guide

Table of Content

OVERVIEW **4**

PROVISIONING FLOW **5**

CONFIGURATION PARAMETERS **6**

Generate Configuration Files 6

TFTP or HTTP/HTTPS for Configuration File 6

Firmware and Configuration File Prefix and Postfix 6

Firmware Server and Configuration File Server 7

Managing Firmware and Configuration File Download 8

Pre-configuration and configuration redirection 9

Automatic provisioning within the LAN 10

XML PROVISIONING SCHEMA AND EXAMPLE FILE **11**

XML File Encryption 11

Secure Provisioning 12

Table of Figures

Figure 1: Provisioning Flow. 5
Figure 2: firmware settings on Web UI 7
Figure 3 : Config File provisioning settings on Web UI. 8
Figure 4 : Firmware Upgrade settings on Web UI. 8
Figure 6 : DHCP Discover. 10
Figure 7 : DHCP Offer. 10
Figure 8 : Using Web UI to define XML Configuration File Password 11

OVERVIEW

Grandstream SIP Devices can be configured via the web interface as well as via the configuration file through TFTP or HTTP/HTTPS download. All Grandstream SIP devices support a proprietary binary format configuration file. Product families such as GXP(21xx/17xx/16xx), GXV3xxx, GRP26xx, DP7xx, HTxxx and WP8xx accept configuration files in XML format in addition to the legacy proprietary binary format. The XML provisioning implementation also allows generic XML configuration file in addition to the MAC based configuration file.

When a Grandstream device boots up or reboots, it issues a request for a configuration file named "cfgMAC.bin" where "MAC" is the MAC address of the device, for example, "cfg000b820102ab.bin", the configuration file name should be in lower case, the file "cfgMAC" is a proprietary binary format configuration file that must be generated by Grandstream configuration tools.

For devices that support XML provisioning, they will also issue a request for an XML configuration file "cfgMAC.xml".

Note that the provision program will apply and reload the settings after downloading the legacy binary cfgMAC config file. This means that a provision/re-direction server can redirect the device to an XML provision server without reboot. It can also be used to send the XML encryption password.

If the download of cfgMAC.xml and cfgModelName (e.g., cfggrp2614.xml) files is not successful, the provision program will download the generic cfg.xml file. This approach can be used to design a two-phase provision process. One example for such process is a user self-provision system using PIN codes. The provision server will at first, hand out a generic XML configuration file that allows the device to make calls to the automated provision center, after the user enters the number and PIN code, the actual per device configuration file is generated.

PROVISIONING FLOW

The following flowchart shows the provisioning process for GRP261x phones.

Other Grandstream products generally follow similar provisioning sequences, if not requesting the same set of files.

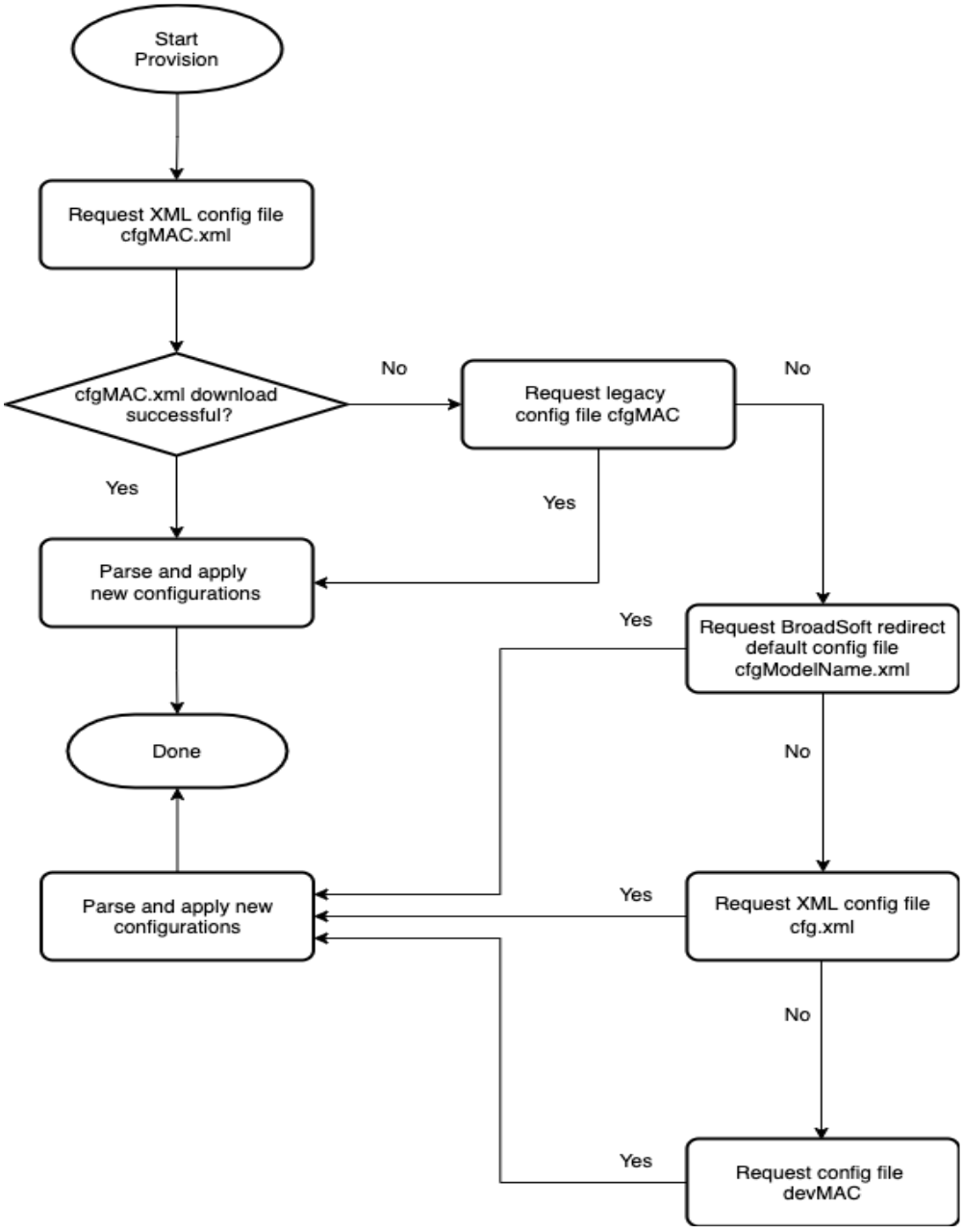

Figure 1: Provisioning Flow

CONFIGURATION PARAMETERS

A configuration parameter is associated with a particular setting's option in the Grandstream device's web configuration pages.
A parameter consists of a capital letter P and 1 to 5 digits numeric numbers. For example, P2 is associated with "Admin Password" in the web access page. P22120 is associated with "HTTP Web Port" in the Security page under Maintenance → Security Settings.
For a detailed parameter list, please refer to the corresponding firmware release configuration template, available for download under http://www.grandstream.com/support/tools.

Generate Configuration Files

Grandstream offers a free XML Configuration File Generator software in Windows and Linux/Unix platform. The XML Configuration File Generators can be downloaded from Grandstream official web site at http://www.grandstream.com/support/tools .

TFTP or HTTP/HTTPS for Configuration File

Traditionally, TFTP is used for configuration file download.
However, it is more popular today to use HTTP/HTTPS, which is more reliable and does not have NAT issue.

Firmware and Configuration File Prefix and Postfix

Firmware prefix and postfix allow the device to download firmware names with the matching prefix and postfix. Prefix and postfix for both firmware and configuration files are supported.

- Parameter P232 and P233 are for Firmware File Prefix and Postfix, respectively.
- Parameter P234 and P235 are for Config File Prefix and Postfix, respectively.

In addition, when Parameter P238 (Check New Firmware only when F/W pre/suffix changes) is set to 1, the device will only issue firmware upgrade requests if there are changes to the firmware prefix or postfix. For example, the firmware basic name for GRP261x is "grp2610fw.bin." If the service provider uses "gs_" as prefix, and "_1.0.5.44" as postfix, then the firmware file will be changed to: "gs_grp2610fw.bin_1.0.5.44".

Firmware prefix and postfix allow firmware with different versions to be stored in one single directory and differentiated by using the prefix or postfix, (i.e., all files with a postfix of "_1.0.5.44" belong to the firmware version 1.0.5.44.).

The same rule applies to configuration files, i.e., for configuration file named “cfg000b82000001”, there can be 3 versions:

“gs_cfg000b82000001_cfg001”,

“gs_cfg000b82000001_cfg002”,

and “gs_cfg000b82000001_cfg003”

Note: Here, the basic name of the configuration file is “cfg000b82000001”, but there are 3 different versions, and the one that will be accepted is the one with the matching prefix and postfix specified in the current configuration.

Firmware Server and Configuration File Server

In addition to the prefix and postfix for the firmware and configuration files, different server paths for firmware upgrade or configuration file server can be specified using different FQDN.

Figure 2: firmware settings on Web UI

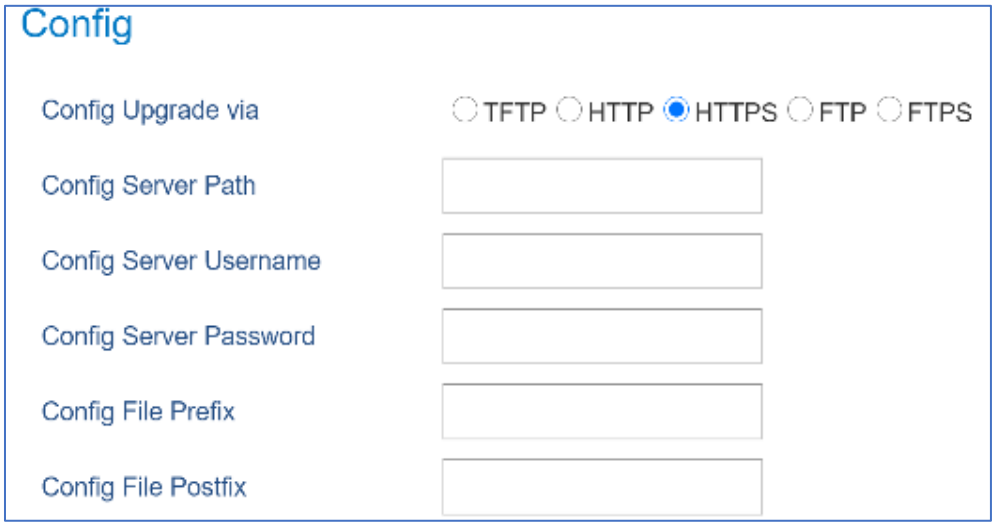

Figure 3 : Config File provisioning settings on Web UI

The parameters are P192 and P237 for Firmware Server Path and Config Server Path, respectively.

Managing Firmware and Configuration File Download

When the parameter P194 (Auto Upgrade) is set to 1, the service provider can use P193 (Auto Check Interval) to periodically check with either firmware server or config server whenever they are defined. This allows the device to periodically check if any new changes occur on a scheduled time. By defining different intervals in P193 for different devices, the service provider can distribute the firmware or configuration file download schedule to reduce the firmware or provisioning server load at any given time.

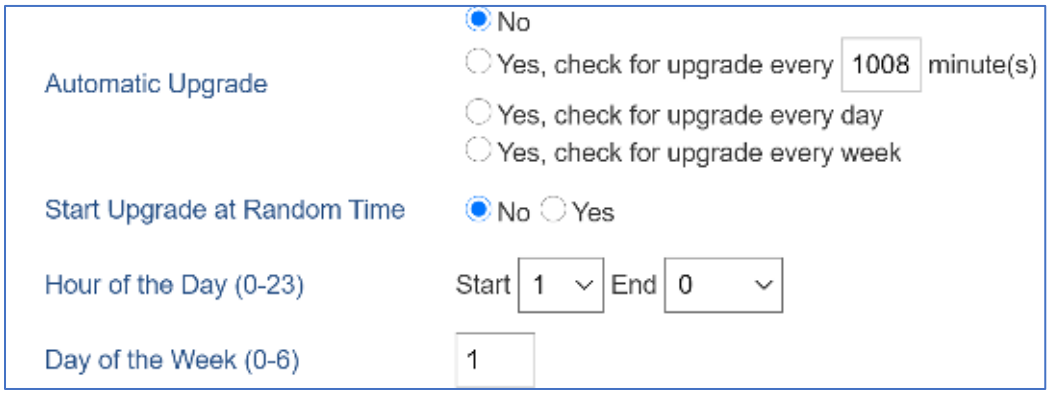

Figure 4 : Firmware Upgrade settings on Web UI

Pre-configuration and configuration redirection

For mass deployment, Grandstream provides TFTP/HTTP/HTTPS redirection service through our certified partners. Here is how redirection works: By default, all Grandstream products are configured with Grandstream provisioning system. When a Grandstream device is powered up, it will automatically contact our provisioning server. Our provisioning server will then redirect the device to customer's TFTP/HTTP/HTTPS server. The device will reboot and send further provisioning request asking for configuration file (or firmware file) from customer's TFTP/HTTP/HTTPS server.

Below is the information we need from service providers for TFTP/HTTP/HTTPS redirection:

1. MAC address range, this is printed on the carton box.
2. Your TFTP/HTTP/HTTPS server IP address.
3. Your company name and address.

Here is what service providers should do:

1. Create configuration files for all the devices and put them on your server.
2. Download the latest official firmware release from https://www.grandstream.com/support/firmware and put them on your server (same directory as above).
3. After we inform you that the devices have been entered into our central provisioning database, please try a few devices to test. Upon powering up, the devices should contact the provisioning server fm.grandstream.com/gs first, and then get redirected to your TFTP/HTTP/HTTPS server and before requesting the firmware files and the configuration files. The devices will be upgraded to the latest firmware with your configurations.

Grandstream also offers pre-configuration of our devices from the factory, but this will incur an extra cost to the products ordered.

Automatic provisioning within the LAN

Grandstream products support DHCP Option 66 or 43 for automatic provisioning within a Local Area Network. The provisioning server URL is embedded inside standard option 66 or 43 of DHCP responses. All Grandstream product families support DHCP Option 66 while the new product series GXP21xx/16xx/17xx and GRP26xx support both DHCP Option 66 and 43.

Grandstream SIP devices send out DHCP DISCOVER with the following information:

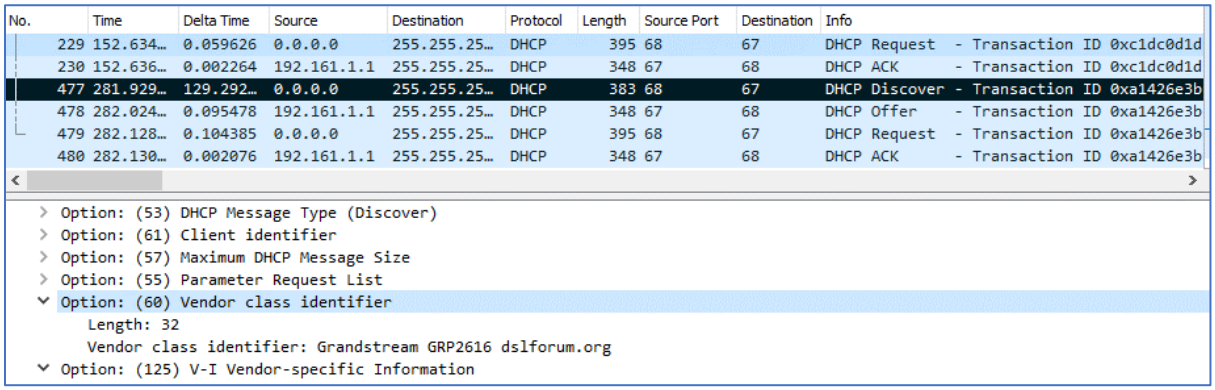

Figure 5 : DHCP Discover.

DHCP Server can be configured to send the following information in its DHCP OFFER. Please notice that in this example, a TFTP server Ip address 192.168.1.1 that is provided in the Option 66 “TFTP Server Name” field. Device will then issue HTTP requests instead of the traditional TFTP requests to the server. This design allows more flexibility in device provisioning. While all Grandstream SIP devices support DHCP Option 66, only new product series such as GXP21xx/17xx/16xx and GRP26xx, HT8xx, GXW4xxx, DP7xx, GXV3xxx and WP8xx support this additional flexibility.

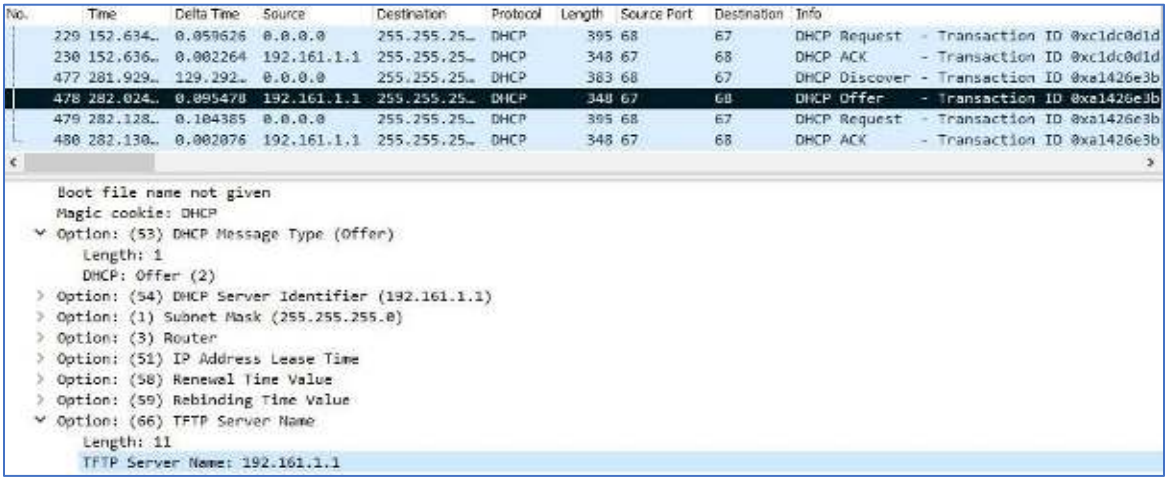

Figure 6 : DHCP Offer

XML PROVISIONING SCHEMA AND EXAMPLE FILE

The general XML syntax consists of a list of name-value pairs. The P-Value is the element, and the value of the element represents the setting for that specific configuration. For the complete P-value list, please refer to the legacy configuration templates at http://www.grandstream.com/support/tools

Example XML configuration file (cfgxxxxxxxxxxxx.xml):

```
<?xml version="1.0" encoding="UTF-8" ?>
<gs_provision version="1">
  <mac>000b82123456</mac>
  <config version="1">
    <P271>0</P271>
    <P270>Account name</P270>
  </config>
</gs_provision>
```

The <mac> element is not mandatory. It is designed this way because not all provision systems support MAC address. If it is present, the provision program will validate the <mac> element with the actual MAC address on the device.

XML File Encryption

The XML configuration file may be encrypted using AES-256-CBC algorithm. The encryption password is defined in P1359 (XML Config File Password) of the configuration file. The encryption may use salt to enhance security. The algorithm to derive the key and IV from a password is the same as the one used by OpenSSL.

The OpenSSL command-line to encrypt the file is as follows:
Openssl enc –e –aes-256-cbc –k password –in config.xml –out cfgxxxxxxxxxxxx.xml
Alternatively, users can also set the XML Config File Password in the web UI of the phone.

Figure 7 : Using Web UI to define XML Configuration File Password

When the XML configuration file is encrypted using this method, the phone would only be able to decrypt and parse the file if user sets the XML Config File Password in P1349 of binary configuration file or in the web UI.

Secure Provisioning

Although the XML configuration file can be encrypted and the encryption algorithm itself is regarded as safe and strong by using AES with 256-bit key length, it remains a question on how to bootstrap and provision the initial XML encryption password. There are several methods to provide solutions to this:

1. Use a legacy binary configuration file to set the initial XML encryption password. The legacy binary file is encrypted, and it is generally considered safe.
2. Use HTTPS and use client-side authentication. This is the industry standard approach and has the strongest safety.