



Grandstream Networks, Inc.

XML Provisioning Guide

GXV3140 IP Multimedia Phone

TABLE OF CONTENTS

XML PROVISIONING GUIDE

OVERVIEW	3
PROVISIONING FLOW	3
XML SCHEMA AND EXAMPLE FILE	3
XML FILE ENCRYPTION	4
SECURE PROVISIONING.....	4

TABLE OF FIGURES

XML PROVISIONING GUIDE

FIGURE 1: PROVISIONING FLOW.	3
FIGURE 2: USING THE GXV3140 WEB UI TO DEFINE THE XML CONFIG FILE PASSWORD.....	4

OVERVIEW

The XML provisioning system allows Grandstream phones to perform configuration updates via XML configuration files. In addition, the XML provisioning implementation may also allow generic XML configuration file on top of the MAC based configuration file.

Note: Currently, XML provisioning is only supported on the GXV3140 IP multimedia phone with firmware version 1.0.3.24 and onwards.

PROVISIONING FLOW

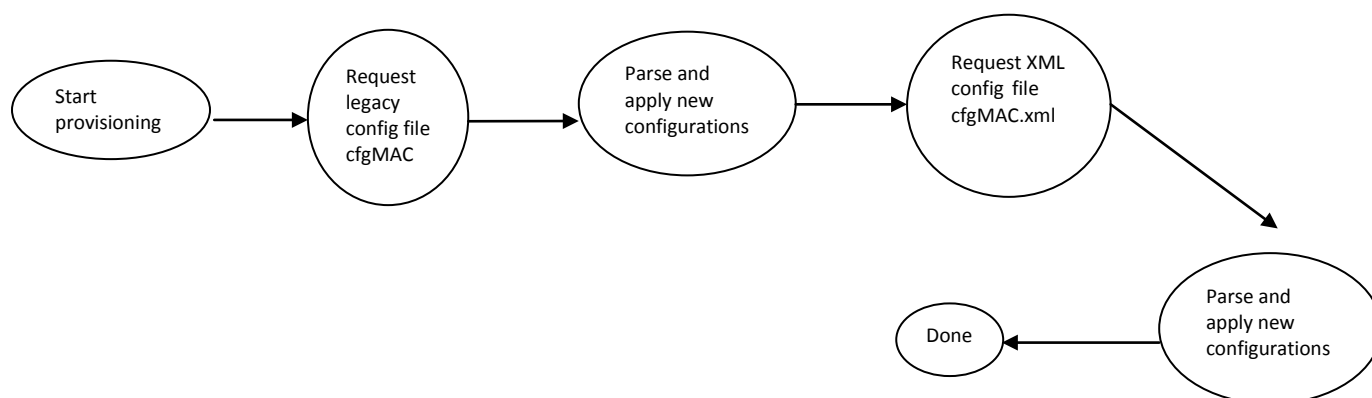


Figure 1: Provisioning Flow.

The provision program on the phone 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 a XML provision server without reboot. It can also be used to send the XML encryption password.

XML SCHEMA AND EXAMPLE FILE

The general XML syntax consists of a list of name-value pairs. P-Value is the element and the value of the element is represents the value for that particular configuration that the corresponding P-Value represents. For the complete P-value list, please refer to the legacy GXV3140 configuration templates at <http://www.grandstream.com/support/configurationtool.html>

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.

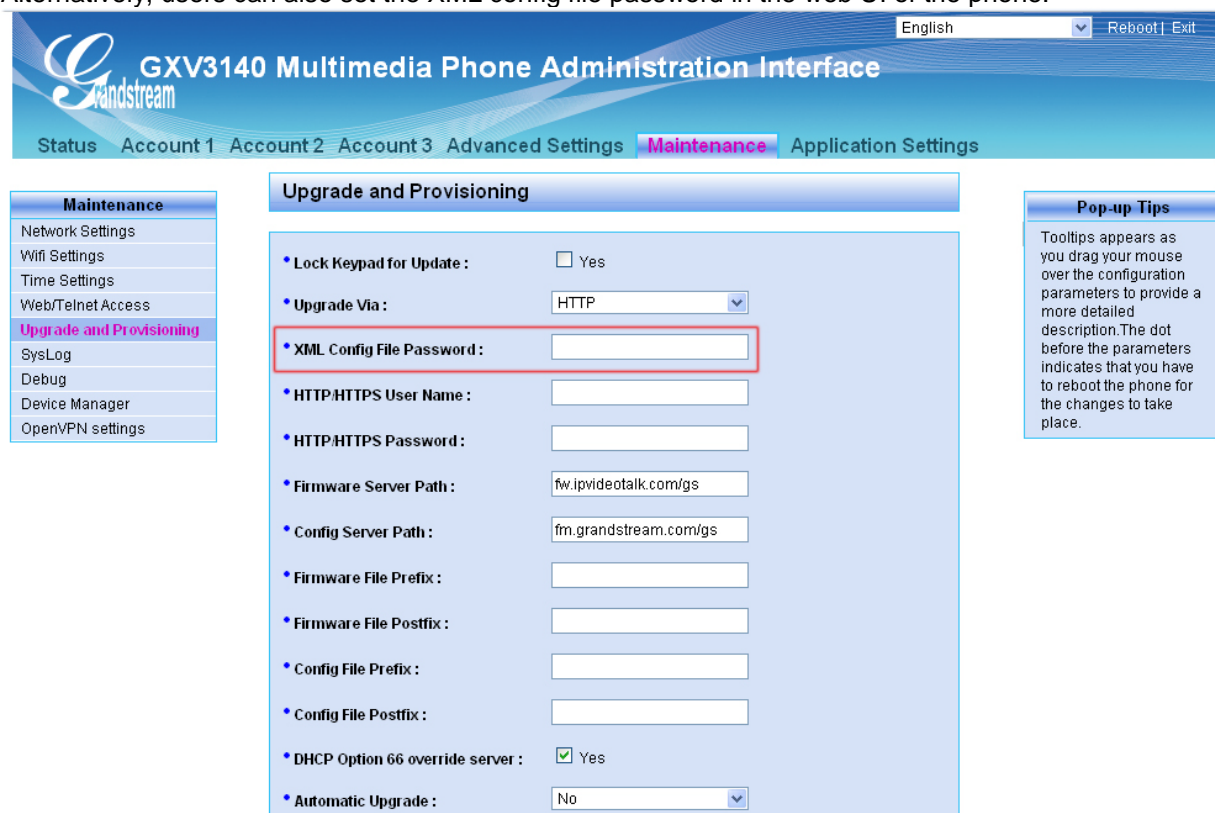
XML FILE ENCRYPTION

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.



The screenshot shows the 'GXV3140 Multimedia Phone Administration Interface' with the 'Maintenance' tab selected. The 'Upgrade and Provisioning' section contains the following fields:

- Lock Keypad for Update : Yes
- Upgrade Via : HTTP
- XML Config File Password :** (highlighted with a red box)
- HTTP/HTTPS User Name :
- HTTP/HTTPS Password :
- Firmware Server Path : fw.ipvideotalk.com/gs
- Config Server Path : fm.grandstream.com/gs
- Firmware File Prefix :
- Firmware File Postfix :
- Config File Prefix :
- Config File Postfix :
- DHCP Option 66 override server : Yes
- Automatic Upgrade : No

A 'Pop-up Tips' box on the right states: 'Tooltips appears as you drag your mouse over the configuration parameters to provide a more detailed description. The dot before the parameters indicates that you have to reboot the phone for the changes to take place.'

Figure 2: Using the GXV3140 web UI to define the 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 set the XML config file password in P1349 of binary configuration file or in the web UI.

SECURE PROVISIONING

Although the XML config 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 legacy binary config file to set the initial XML encryption password. The legacy binary file is encrypted and it generally regarded safe.
2. Use HTTPS and use client side authentication. This is the industry standard approach and has the strongest safety.