

Обеспечение параметрами (Provisioning)



SIP устройства Grandstream можно настраивать через встроенный Веб сервер или через Конфигурационный файл загружаемый по протоколам TFTP или HTTP/HTTPS.

Все SIP устройства Grandstream поддерживают проприетарный бинарный формат конфигурационного файла. Устройства серии GXP21xx/14xx/11xx, GXV31xx, HT50x, HT70x, GXW40xx и DP71x дополнительно поддерживают XML формат конфигурационного файла.

Когда устройство загружается при включении или при перезагрузке, оно запрашивает конфигурационный файл формата cfgMAC, где MAC это MAC адрес этого устройства, например cfg000b820102ab. Имя файла должно быть в нижнем регистре.

Файл формата cfgMAC это проприетарный бинарный формат конфигурационного файла может быть создан при помощи Grandstream configuration tools.

Устройства, которые поддерживают XML формат конфигурационного файла будут выполнять запрос файла cfgMAC.xml.

Схема процесса



Обратите внимание, что настройки будут применены после загрузки файла cfgMAC. Это означает, что сервер настройки подготовки к работе (Provisioning) может перенаправить устройство на XML сервер без перезагрузки. Это может быть использовано для передачи зашифрованных паролей XML.

Если загрузка cfgMAC.xml не прошла успешно, процесс настройки будет загружать файл cfg.xml. Этот подход может быть использован для реализации двухфазного Процесса подготовки к работе (Provisioning).

Параметры настройки

Параметры настройки связаны с полями на веб страницах устройства. Имя параметра начинается с буквы P и от 2 до 3 (возможно до 4 в будущем) цифр. Например, P2 это Admin Password на странице Advanced Page. Список параметров конкретного устройства связан с версией прошивки (firmware).

Шаблоны настроек

Для создание файлов Grandstream предлагает free Configuration File generator software in both Linux/Unix and Windows platform. Both Configuration File Generators can be downloaded from Grandstream official web site at <http://www.grandstream.com/support/tools>.

Традиционно для загрузки файлов конфигурации использовался TFTP. Однако, популярный сейчас HTTP/HTTPS более надежен и не имеет проблем с NAT.

Grandstream Configuration Generator позволяет шифровать файл настроек по алгоритму AES 128. Windows версия

программы позволяет не использовать шифрование, но это не рекомендуется.

Префикс и суффикс в именах файлов

Параметры P232 и P233 это префикс и суффикс для прошивок (Firmware), соответственно. Параметры P234 and P235 это префикс и суффикс для файла настроек, соответственно.

Префикс и суффикс в именах файлов прошивок разрешают устройству загружать соответствующую прошивку.

В дополнение параметр P238 (Проверять новую прошивку (Firmware) только если изменился префикс и суффикс) установить в 1, устройство будет обновлять прошивку если изменился префикс и суффикс файла.

Кроме базовых имен связанных с BT100: boot.bin, bt-110.bin, html110.bin, vocbt.bin, vp.bin. Можно использовать gs_ как префикс, и _1.0.7.5 как суффикс: gs_boot.bin_1.0.7.5, gs_bt-110.bin_1.0.7.5, gs_html110.bin_1.0.7.5, gs_vocbt.bin_1.0.7.5, gs_vp.bin_1.0.7.5

Цель этого в том, чтобы все прошивки с разных версии могли быть сохранены в одном каталоге, а для того, чтобы их отличить можно использовать префикс и суффикс файла, то есть, все файлы с суффиксом _1.0.7.5 принадлежат прошивке версии 1.0.7.5.

То же правило применяется и к файлам настроек, то есть, файл cfg000b82000001, может быть в 3 версиях: gs_cfg000b82000001_cfg001, gs_cfg000b82000001_cfg002 и gs_cfg000b82000001_cfg003. Здесь, базовое имя файла cfg000b82000001, но 3 различные версии отличаются префиксом и суффиксом.

Сервер прошивок и файлов настроек

В дополнение к префиксу и суффиксу можно использовать разные имена серверов (FQDN).

Например:

Параметр	Описание	Пример
P192	Путь к серверу прошивок	firmware.grandstream.com/HT502/1.0.7.6
P237	Путь к серверу настроек	provisioning.grandstream.com/HT502

Управление загрузкой файлов настроек и обновлений

Если параметр P194 (Автоматическое обновление) установлен в 1, можно использовать параметр P193 (Интервал автоматического обновления).

PRE-CONFIGURATION AND CONFIGURATION REDIRECTION

For mass deployment, Grandstream provides TFTP/HTTP redirection service. This service is free. Here is how redirection works. By default all Grandstream products point to our provisioning system. When a unit is powered up, it will automatically contact our provisioning server. Our provisioning server will then redirect the unit to customer's TFTP/HTTP/HTTPS server. The unit 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 redirection:

1. MAC address range, this should be printed on the carton box 2. Your TFTP/HTTP 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 TFTP/HTTP server 2. Download the latest official release from <http://www.grandstream.com/support/firmware> and put them on your TFTP/HTTP server (same directory as above) 3. After we inform you that the devices have been entered into our central provisioning database, please take out a few devices to test. Upon powering up, they should contact our provisioning server fm.grandstream.com/gs first, and then get redirected to your TFTP/HTTP server and pull out the firmware files and the configuration files. They will be upgraded to the latest firmware with your configurations.

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

Автоматическая подготовка к работе (Provisioning)

Устройства поддерживают DHCP опции 66 или 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/14xx/11xx

support both DHCP Option 66 and 43.

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

DHCP Server can be configured to send the following information in its DHCP OFFER. Please notice that in this example, an HTTP://URL 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 GXP21xx/14xx, GXV31xx, HT50x and GXW40xx support this additional flexibility.

XML PROVISIONING 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 configuration templates at

<http://www.grandstream.com/support/tools>

Example XML configuration file (cfgxxxxxxxxxxxx.xml):

```
<code>
<?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>
```

Grandstream Networks, Inc. SIP Device Provisioning Guide Page 8 of 9

www.grandstream.com Last Updated: 9/2012

```
</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 2: Using 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 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 legacy binary configuration 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.

Бинарный файл (.cfg)

Источник информации

Описание формата

Структура файла

Заголовок (16 байт)
Параметры устройства
&gnkey=0b82
If the length of this parameter string is not even, a zero byte is added to the string,(Padding byte if length is not even)

Заголовок

00 00 00 44 58 1b 00 0b 82 00 00 00 0d 0a 0d 0a	Пример заголовка в шестнадцатиричном виде
00 00 00 44 58 1b 00 0b 82 00 00 00 0d 0a 0d 0a	Выделен MAC адрес: 000b82000000
00 00 00 44 58 1b 00 0b 82 00 00 00 0d 0a 0d 0a	Выделены два CRLF
00 00 00 44 58 1b 00 0b 82 00 00 00 0d 0a 0d 0a	Самое интересное это первые 6 байт...
Байт	Значение
0x00	0x00
0x01	0x00
0x02	high of (length of parameter string) divided by 2
0x03	low of (length of parameter string) divided by 2
0x04	0x00 (replaced by high of checksum)
0x05	0x00 (replaced by low bytes of checksum)
0x06	1-ый октет MAC адреса
0x07	2-ый октет MAC адреса
0x08	3-ый октет MAC адреса
0x09	4-ый октет MAC адреса
0x0A	5-ый октет MAC адреса
0x0B	6-ый октет MAC адреса
0x0C	Символ «возврат каретки» (0x0C)

Байт	Значение
0x0D	Символ «перевод строки» (0x0A)
0x0E	Символ «возврат каретки» (0x0C)
0x0F	Символ «перевод строки» (0x0A)

You then compute a 16 bit checksum (initial value 0x0000 - adding the value of each individual byte) of the entire configuration string. This value is subtracted from 0x10000 and placed in bytes 4 and 5 of the header, then the header and parameter strings are written to a binary file.

This format has been tested and confirmed with firmware versions up to 1.0.6.0 of the grandstream and BudgeTon and HandyTone devices.

Параметры устройства

Параметры преобразуются в формат URL-encode.

Пример

До преобразования	После преобразования
P30=time.nist.gov P63=1 P31=1	P30=time.nist.gov&P63=1&P31=1

Стандартное шифрование cfg

Перевод:

Сам ключ генерируется из нескольких кусков информации: длина зашифрованных данных, MAC-адрес устройства, случайное 2-байтовое число, и, наконец контрольную сумму данными. Для устройства, расшифровка данных без этой информации была бы невозможна. Таким образом, вся эта информация (минус MAC-адрес) предваряется как 16 байт заголовка к зашифрованному конфигурационному файлу! Очевидно, что MAC-адрес не должен быть передан на устройство, как это уже знает, (не менее, имя файла конфигурации обычно содержит MAC адресом). Таким образом, с помощью заголовка файла конфигурации можно легко генерировать ключ, который был использован для шифровки данных, и с помощью симметричного алгоритма шифрования используется он также может быть использован для расшифровки данных.

[VOIPSEC] Security Vulnerability in the Grandstream HandyTone devices. Anon Anon yetanother at earthling.net Wed Mar 25 17:31:00 GMT 2009

The device can be configured in different ways this discussion will focus on how its generally used in large scale deployments. When the HandyTone is turned on, it sends an HTTP (or HTTPS) request to the manufacturers configuration server asking for a configuration file (cfg000B82XXXXXX) based on the MAC address. This configuration file changes the default configuration server from that of the manufacturer (fm.grandstream.com/gs) to that of the provider. Once again, the HandyTone requests a config file, but this time from the provider. The VoIP configuration file, among other things, contains the SIP account credentials. The only information provided to both of the configuration servers is the MAC address of the device.

Grandstream provides a small java application which can be used to generate configuration files. It takes a input config file, strips out the comments, and converts the ASCII text into ISO-8859-1. The application then enciphers the data with AES-128-CBC with an auto-generated key. The key itself is generated from several pieces of information: the length of the encrypted data, the MAC address of the device, a random 2-byte number, and finally a checksum of the data. For the device, deciphering the data without this information would be impossible. So, all of this information (minus the MAC address) is prepended as a 16 byte header to the encrypted configuration file! Obviously, the MAC address does not have to be transmitted to the device as it already knows it, (non-the less, the name of the configuration file usually contains the MAC address.) So, by using the header of the onfiguration file one can easily generate the key that was used to encipher the data. And since a symmetric encryption algorithm is used it can also be used to decrypt the data.

The configuration files, or more accurately the SIP credentials within can be obtained by performing a man-in-the-middle attack on a device. That is, an attacker can monitor the communication channel of the device as it requests the configuration file (assuming HTTP and not HTTPS is used). This attack is not very interesting because intercepting traffic on a large scale is

not feasible. The more interesting approach is for the attacker to pretend to be the device and do request the configuration file directly from the server (via HTTP or HTTPS). All the information one needs to preform this attack is the MAC address of the device, which can be obtained from network broadcasts or by simply guessing MAC addresses. If the MAC addresses are assigned in a linear fashion by Grandstream, then it makes this attack very easy to preform. If not, there are only ~17 million possible Grandstream MAC addresses. An exhaustive search for MAC addresses would not be infeasible. Although Grandstream and VoIP providers could implement some code to prevent exhaustive searches on their database it would not be very effective, since an attacker could simply use a botnet or even TOR.

In a few words, the consequences of this blatantly insecure authentication system allows anyone with little ambition to extract thousands of SIP credentials. Affected users are those who subscribe to VoIP providers which make use of this auto-configuration system, and there are plenty of providers out there, some of which have a very large subscriber base.

The quick fix to this problem is to shut down the auto-configuration servers both those of the providers and those of Grandstream. Unfortunately as a result of this, the users will have to configure the devices manually. A better fix would be to use asymmetric cryptography scheme, pre-load a unique private key onto the device and make a database of the public ones. The problem is that the key would have to be stored permanently on the device which, depending on the hardware, might not be feasible.

Attached is a utility for decrypting the encrypted config files.

PS.

I have contacted grandstream about this issue, unfortunately they did not appear to be overly concerned.

[\[VOIPSEC\] Security Vulnerability in the Grandstream HandyTone devices.](#)

Ссылки

[TR-069 Information](#)

[Общее описание технологии Provisioning \(на английском языке\)](#)

[Общее описание технологии Provisioning \(на английском языке\)](#)

<http://sysadminmosaic.ru/grandstream/provisioning>

2020-11-12 16:08

