

# Grandstream Networks, Inc.

---

WP820

## Wi-Fi Provision via USB Guide



## Table of Contents

<b>SUPPORTED DEVICES .....</b>	<b>3</b>
<b>OVERVIEW .....</b>	<b>4</b>
<b>WI-FI PACKAGE DETAILS .....</b>	<b>5</b>
Wi-Fi Package Format .....	5
Config.xml Template .....	5
USB File Path .....	8
<b>USAGE SCENARIOS .....</b>	<b>9</b>
Normal Use .....	9
Limited permission or lock screen enabled with password.....	9
Same Wi-Fi Configuration.....	10
Low Battery .....	11
Call during configuration .....	11
Web upgrade for firmware during configuration.....	11
There are firmware packages or CFG config files on the USB drive.....	11
<b>CONFIGURATION ERRORS.....</b>	<b>12</b>

## Table of Figures

Figure 1: Wi-Fi installation file.....	5
Figure 2: Wi-Fi Configuration file upload.....	9
Figure 3: Wi-Fi Configuration file upload with limited permission .....	10
Figure 4: Same Wi-Fi Configuration file uploaded .....	10
Figure 5: Battery level condition.....	11

## Table of Tables

Table 1 : Supported Devices.....	3
Table 2 : Error description.....	12



## SUPPORTED DEVICES

Following table shows Grandstream products supporting this feature:

**Table 1 : Supported Devices**

Model	Supported	Firmware
WP820	Yes	1.0.5.5 or higher



## OVERVIEW

In order to facilitate deployment of Wi-Fi configuration in the field, the WP820 supports provisioning of the Wi-Fi configuration via a USB flash drive. The user simply loads the Wi-Fi configuration package on a USB drive and then plug into the device. To ensure the security of the device, the USB provisioning of the Wi-Fi configuration will first verify the credentials of the administrator if screen lock is active and a password is set.

The provision function through the USB flash drive also includes additional features such as upgrading of the firmware and provisioning the device configuration. When the USB flash drive contains the firmware installation package, the configuration file and the Wi-Fi configuration installation package, the device will process the files as follows: (1) Firmware upgrade (2) Config provision (3) Wi-Fi configuration provision.



## WI-FI PACKAGE DETAILS

### Wi-Fi Package Format

The Wi-Fi installation package is a zip file named “wifiAutoConfig.zip.” It contains a configuration file “config.xml” and sample Wi-Fi certificate files as shown below (Note: Certificates are not necessary depending on the Wi-Fi authentication method used and included for demonstration purposes):

config.xml	5,027	1,435	XML Document
pbx_802.1x-2019.pfx	0	0	Personal Informati...
wpdev-gwn-802.1x-client.pfx	0	0	Personal Informati...

**Figure 1: Wi-Fi installation file**

### Config.xml Template

The configuration file “config.xml” provided contains all examples of Wi-Fi methods that are supported. It is recommended to only use the configuration that closely matches your network and remove the others. The config.xml format and instructions are as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<WifiAutoConfig>
<!--Unique id-->
<uuid>Grandstream-HZ-version1</uuid>
<!--Update Time-->
<updateTime>2019-07-18 15:45</updateTime>
<!--Clear previous WiFi configuration-->
<clearLast>1</clearLast>
<!--Whether to force configuration, 1 means it is mandatory.
The configuration will be applied without checking the uuid and updateTime.
Normally the configuration will not be updated if uuid and updateTime are both
the same as last time (indicating that config has not been changed). -->
<forceConfig>0</forceConfig>

<ssids>
<!-- Below SSID configurations serve as examples for different type of SSID
methods that are supported by the USB Wi-Fi provision function. It is
recommended to only use the example that closely matches your network's
configuration and remove the other configurations. -->

<!--EAP PEAP mode-->
<!--Here "id" is BSSID. If it is empty, it matches SSID (<name> field). If
there are multiple wireless networks with the same SSID in the environment, it
will match the network with the highest SSID priority. -->
```



```
<ssid id="00:0b:82:8b:57:96">
  <name>pbx_802.1x</name>
  <!-- SECURITY_NONE="NONE" SECURITY_WEP="WEP" SECURITY_PSK="PSK" -->
  <!-- SECURITY_EAP="EAP" -->
  <security>EAP</security>
  <!-- (PEAP TTLS PWD mode requires password) -->
  <password>strongpassword</password>
  <!-- PEAP TLS TTLS PWD -->
  <eapMethod>PEAP</eapMethod>
  <!-- NONE MSCHAPV2 GTC (PEAP TTLS mode requires parse2Method) -->
  <parse2Method>MSCHAPV2</parse2Method>
  <caCert>pbx_802.1x-2019.pfx</caCert>
  <caPassword>strongpassword</caPassword>
  <identity>peap1234</identity>
  <!-- Also can use anonymous identity (PEAP TTLS mode may use anonymous)
-->
  <anonymous>peap</anonymous>
  <isStaticIp>0</isStaticIp>
</ssid>

<!--EAP TLS mode-->
<ssid id="00:0b:82:8b:57:97">
  <name>gwn1-802.1x</name>
  <!-- SECURITY_NONE="NONE" SECURITY_WEP="WEP" SECURITY_PSK="PSK" -->
  <!-- SECURITY_EAP="EAP" -->
  <security>EAP</security>
  <!-- PEAP TLS TTLS PWD -->
  <eapMethod>TLS</eapMethod>
  <caCert>gwn-802.1x-client.pfx</caCert>
  <caPassword>strongpassword</caPassword>
  <!-- (TLS mode requires clientCert) -->
  <clientCert>gwn-802.1x-client.pfx</clientCert>
  <clientPassword>strongpassword</clientPassword>
  <identity>gs-tls</identity>
</ssid>

<!--EAP TTLS mode-->
<ssid id="00:0b:82:8b:57:98">
  <name>gwn2-802.1x</name>
  <!-- SECURITY_NONE="NONE" SECURITY_WEP="WEP" SECURITY_PSK="PSK" -->
  <!-- SECURITY_EAP="EAP" -->
  <security>EAP</security>
  <password>strongpassword</password>
  <!-- PEAP TLS TTLS PWD -->
  <eapMethod>TTLS</eapMethod>
  <!-- NONE MSCHAPV2 GTC (PEAP TTLS mode requires parse2Method) -->
  <parse2Method>MSCHAPV2</parse2Method>
  <caCert>pbx_802.1x-2019.pfx</caCert>
  <caPassword>strongpassword</caPassword>
  <identity>tls-gs</identity>
```



```

    <!-- Also can use anonymous identity (PEAP TTLS mode may use anonymous)
-->
    <anonymous>ttls</anonymous>
</ssid>

<!--EAP PWD mode-->
<ssid id="00:0b:82:8b:57:99">
    <name>gwn3-802.1x</name>
    <!-- SECURITY_NONE="NONE" SECURITY_WEP="WEP" SECURITY_PSK="PSK" -->
    <!-- SECURITY_EAP="EAP" -->
    <security>EAP</security>
    <!-- PEAP TLS TTLS PWD -->
    <eapMethod>PWD</eapMethod>
    <identity>md5</identity>
    <password>strongpassword</password>
</ssid>

<!--SECURITY_PSK mode-->
<!--Here "id" is BSSID, if it is empty, it matches SSID (<name> field). If
there are multiple wireless
networks with the same SSID in the environment,
It will match the network with the highest SSID priority. -->
<ssid id="">
    <name>LA-GWN</name>
    <!-- SECURITY_NONE="NONE" SECURITY_WEP="WEP" SECURITY_PSK="PSK"
SECURITY_EAP="EAP" -->
    <security>PSK</security>
    <password>strongpassword</password>
    <!-- Connect 1 means that the network is configured to be connected.
If not declared or not set to 1 means only save the configuration. If
multiple SSID
set connect to 1 then only the last entry will take effect -->
    <connect>1</connect>
</ssid>

<!--SECURITY_PSK mode static IPv4-->
<ssid id="00:0b:82:8b:57:99">
    <name>HZGWN1-5G</name>
    <!-- SECURITY_NONE="NONE" SECURITY_WEP="WEP" SECURITY_PSK="PSK"
SECURITY_EAP="EAP" -->
    <security>PSK</security>
    <password>somestrongpassword</password>
    <connect>1</connect>
    <!-- static IPv4-->
    <isStaticIp>1</isStaticIp>
    <ipv4>
        <ipAddress>11.20.1.119</ipAddress>
        <gateway>11.20.0.1</gateway>
        <prefixlength>23</prefixlength>
        <dns1>8.8.8.8</dns1>
        <dns2>8.8.4.4</dns2>
    </ipv4>

```



```
</ipv4>
</ssid>

<!--SECURITY_NONE mode static IPv6-->
<ssid id="00:0b:82:8b:57:77">
  <name>GSHZGWN2-5G</name>
  <!-- SECURITY_NONE="NONE" SECURITY_WEP="WEP" SECURITY_PSK="PSK" -->
  <!-- SECURITY_EAP="EAP" -->
  <security>NONE</security>
  <connect>0</connect>
  <!-- static IPv6 -->
  <isStaticIp>1</isStaticIp>
  <ipv6>
    <ip6Address>2001:db8:3::100a</ip6Address>
    <ip6Prefixlength>128</ip6Prefixlength>
    <ip6Dns1>240c: : 6666</ip6Dns1>
    <ip6Dns2>240c: : 6644</ip6Dns2>
  </ipv6>
</ssid>

</ssids>
</WifiAutoConfig>
```

## USB File Path

Place the Wi-Fi package directly in the root directory of the USB flash drive.





## USAGE SCENARIOS

### Normal Use

1. Download the zip file “wifiAutoConfig.zip” from the Grandstream WP820 resources page.
2. Configure config.xml and include any necessary certificates.
3. Transfer the file “wifiAutoConfig.zip” to a USB flash drive.
4. Use a USB OTG cable to connect the USB flash drive to WP820 and confirm the provision process.

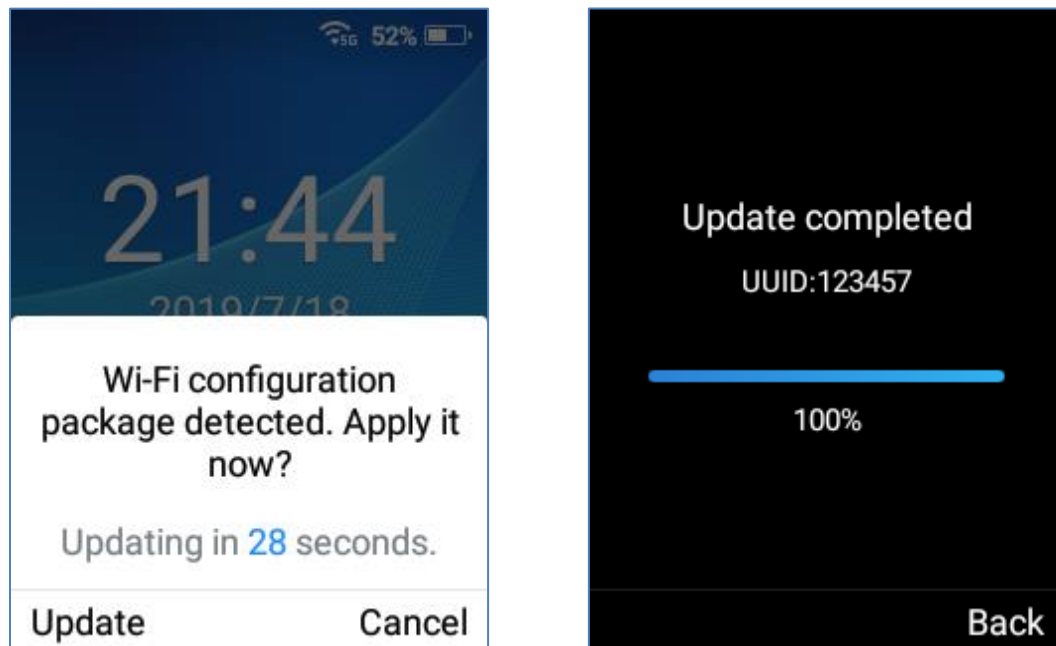


Figure 2: Wi-Fi Configuration file upload

### Limited permission or lock screen enabled with password

In the following situations, the WP820 will prompt for admin password prior to allowing Wi-Fi configuration:

1. The web UI setting “Configuration via Keypad Menu” is set to “basic setting only” or “basic setting & network setting” or “constraint mode.”
2. Lock screen is enabled with password.



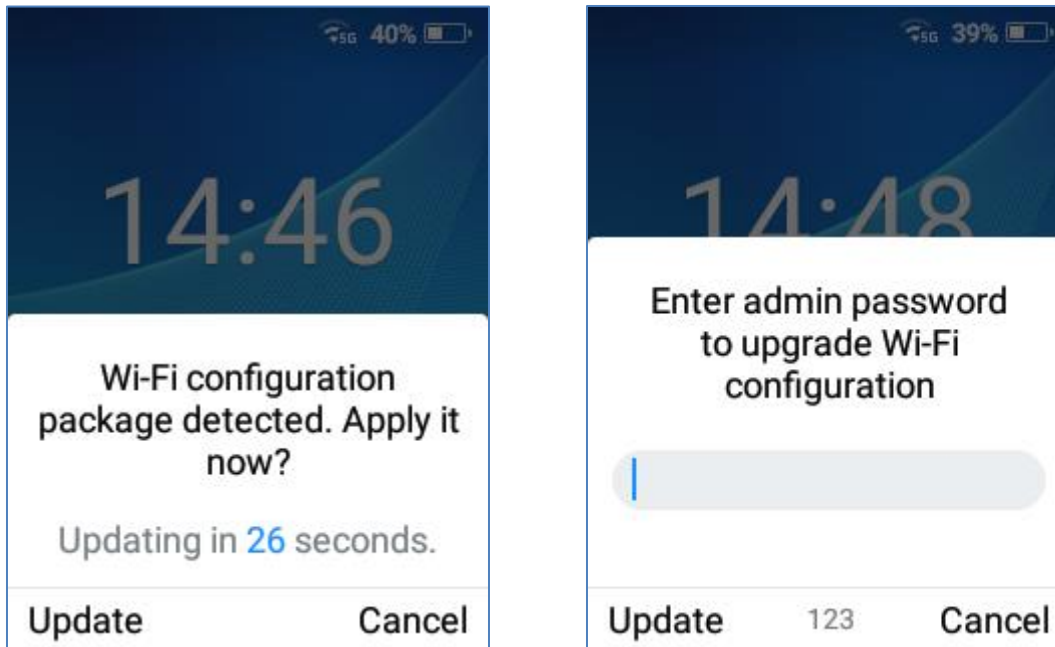


Figure 3: Wi-Fi Configuration file upload with limited permission

### Same Wi-Fi Configuration

If both the <UUID> and <updateTime> are same as previous provision, then no updates will be processed.

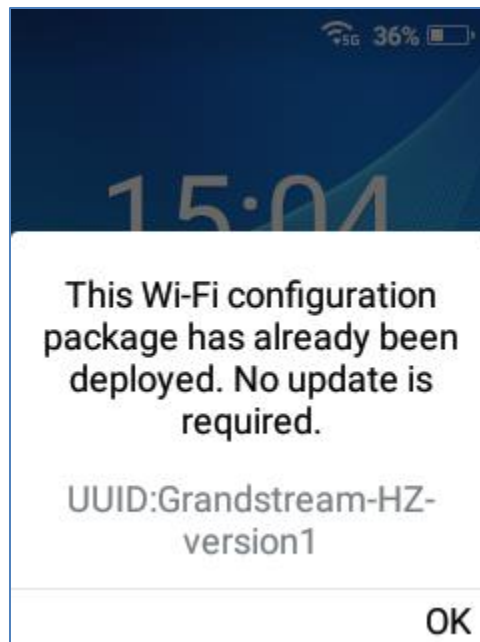


Figure 4: Same Wi-Fi Configuration file uploaded

## Low Battery

If the USB flash drive is inserted and the power is too low, the Wi-Fi upgrade cannot be performed. The process will need to be retried again when battery is above 15%.

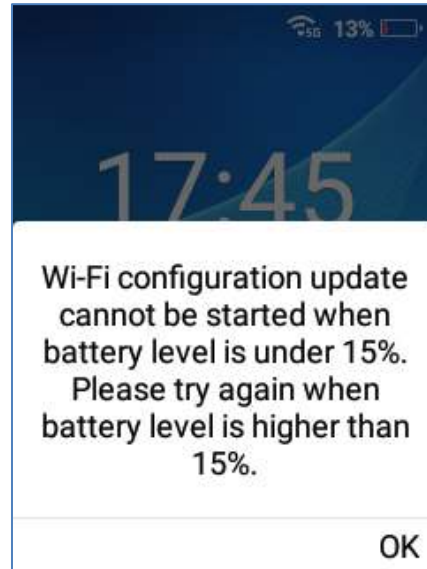


Figure 5: Battery level condition

## Call during configuration

The Wi-Fi provision prompt will not display during the call and the system will wait until the call is ended or canceled before showing the confirmation prompt.

## Web upgrade for firmware during configuration

The Wi-Fi provision prompt will not display during firmware upgrade and the system will wait until the upgrade is completed or canceled before showing the confirmation prompt.

## There are firmware packages or CFG config files on the USB drive

In the scenario where there are firmware files, cfg config file and Wi-Fi package on the USB drive the behavior will be as follows:

1. If a firmware package exists (wp820fw.bin), the upgrade prompt is displayed first.
2. If the firmware upgrade prompt is cancelled, it will check for the cfg configuration (cfg{mac}.xml) and provide a prompt.
3. If the cfg provision is cancelled, the device will detect for "wifiAutoConfig.zip" and a Wi-Fi configuration prompt will display.



## CONFIGURATION ERRORS

**Table 2 : Error description**

Error Type	Error Description
<b>USER_CANCEL</b>	The config has been cancelled by user.
<b>UNZIP_FAIL</b>	/path/wifiAutoConfig.zip:The file does not exist.
<b>UNZIP_FAIL</b>	/path/wifiAutoConfig.zip:Unzip path make or clear error.
<b>UNZIP_FAIL</b>	/path/wifiAutoConfig.zip:Unzip IO exception.
<b>PARSE_FAIL</b>	/path/wifiAutoConfig.zip:config.xml does not exist.
<b>PARSE_FAIL</b>	/path/wifiAutoConfig.zip:IO exception occurred during parsing.
<b>PARSE_FAIL</b>	/path/wifiAutoConfig.zip:Xml format error.
<b>CHECK_FAIL</b>	/path/wifiAutoConfig.zip:'uuid' of the config is required.
<b>CHECK_FAIL</b>	/path/wifiAutoConfig.zip:'id' or 'name' of SSID is required.
<b>CHECK_FAIL</b>	SSID_NAME:'security' of the SSID is invalid.
<b>CHECK_FAIL</b>	SSID_NAME:Current security does not require 'password'.
<b>CHECK_FAIL</b>	SSID_NAME:Current security does not require 'eapMethod' or 'parse2Method'.
<b>CHECK_FAIL</b>	SSID_NAME:Current security does not require 'caCert','userCert','caPassword' or 'clientPassword'.
<b>CHECK_FAIL</b>	SSID_NAME:Current security does not require 'identity' or 'anonymous'.
<b>CHECK_FAIL</b>	SSID_NAME:Current security requires 'password'.
<b>CHECK_FAIL</b>	SSID_NAME:'eapMethod' of the SSID is invalid.
<b>CHECK_FAIL</b>	SSID_NAME:Current EAP method does not require 'parse2Method'.
<b>CHECK_FAIL</b>	SSID_NAME:'parse2Method' of the SSID is invalid.
<b>CHECK_FAIL</b>	SSID_NAME:Current EAP method requires 'password'.
<b>CHECK_FAIL</b>	SSID_NAME:Current EAP method requires 'caCert'.



Error Type	Error Description
<b>CHECK_FAIL</b>	SSID_NAME:'caCert' does not contain '.', the correct format is similar to 'ca.crt'.
<b>CHECK_FAIL</b>	SSID_NAME:Current EAP method requires 'clientCert'.
<b>CHECK_FAIL</b>	SSID_NAME:'clientCert' does not contain '.', the correct format is similar to 'client.crt'.
<b>CHECK_FAIL</b>	SSID_NAME:IPv4 address cannot be empty. SSID_NAME:IPv6 address cannot be empty.
<b>CHECK_FAIL</b>	SSID_NAME:IPv4 address format error. SSID_NAME:IPv6 address format error.
<b>CHECK_FAIL</b>	SSID_NAME:IPv4 prefix length beyond range. SSID_NAME:IPv6 prefix length beyond range.
<b>CHECK_FAIL</b>	SSID_NAME:IPv4 gateway cannot be empty.
<b>CHECK_FAIL</b>	SSID_NAME:IPv4 gateway format error.
<b>CHECK_FAIL</b>	SSID_NAME:IPv4 DNS address requires at least one entry. SSID_NAME:IPv6 DNS address requires at least one entry.
<b>INSTALL_CERT_FAIL</b>	/path/wifiAutoConfig/ca.crt:The file does not exist. /path/wifiAutoConfig/ca.crt:IO exception. /path/wifiAutoConfig/ca.crt:File type is not supported. /path/wifiAutoConfig/ca.crt:Certificate installation Failed.