

Gil Reiter

IoT strategic marketing manager

Texas Instruments

A primer to Wi-Fi[®] provisioning for IoT applications

Introduction


Wi-Fi[®] is the most ubiquitous wireless connectivity technology today. After becoming a standard feature in all laptops, smartphones and tablets, Wi-Fi is being added to simpler products like home appliances, thermostats and many other home and building automation products that are feeding the exploding Internet of Things (IoT). Provisioning IoT products, that do not have a keyboard and display as a user interface, in a simple and robust way is a significant challenge. In this paper we review the main Wi-Fi provisioning methods that are available in the market and provide guidelines for choosing the right provisioning method for your product.

What is Wi-Fi provisioning?

Wi-Fi provisioning is the process of connecting a new Wi-Fi device (station) to a Wi-Fi network. The provisioning process involves loading the station with the network name (often referred to as SSID) and its security credentials. The Wi-Fi security standard distinguishes between *personal security*, mostly used in homes and businesses, and **enterprise security**, used in large offices and campuses. Provisioning a station for enterprise security usually involves installing certificates, which are used to verify the integrity of the station and the network by interaction with a security server managed by the IT department. Personal Wi-Fi security, on the other hand, needs to be handled by users at home, and it simply involves typing a pre-defined password. To provide robust security, the password can be as long as 64 characters.

We will restrict the discussion in this paper to personal Wi-Fi security networks, and to the challenge of easily loading an IoT Wi-Fi station with the network name and password by the user.

The challenge of wireless provisioning in IoT applications

Wi-Fi was created to allow nomadic devices such as laptops, and later on mobile devices such as cellphones and tablets, to wirelessly connect to the Internet. These personal computing devices naturally include a display and a keyboard for the user interface. The usual procedure for provisioning a cellphone, for instance, on a Wi-Fi network is done via the phone's Wi-Fi setting page. The phone scans for Wi-Fi networks and presents a list of available networks to the user. After choosing the network, the user is prompted for a password. If the password is typed correctly, the provisioning is successful, and often indicated by a  Wi-Fi symbol in a status bar.

The challenge in IoT products is that many of them do not have a display and a keyboard, and sometimes they don't even have a user interface at all. These *headless devices* need alternate methods to obtain the network name and password from the user. The alternate provisioning method has to be simple to use and secure. In most cases it uses a PC, a phone or a tablet as an extended user interface for the IoT device, allowing the user to provide the network information using the display and the keypad of the PC, the phone or the tablet.

In the next few paragraphs, we provide a brief overview of the popular provisioning methods in the market. Later we discuss the key considerations for choosing the right provisioning methods and provide guidelines to the system designer.

Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) is the only industry standard available today for provisioning of headless devices. It was introduced by the Wi-Fi Alliance in 2006 as an easy and secure method to provision devices without knowing the network name and without typing long passwords. The standard defines two mandatory methods for WPS-enabled Access Points (APs): *Personal Identification Number (PIN) method* and *Push-Button-Connect (PBC) method*.

In the PIN method, an 8-digit PIN is printed on a sticker on either the Access Point or the provisioned device. The user needs to read the PIN from one device and type it using a keypad on the other device. Since APs do not have keypads, the PIN is usually printed on the AP, and typed by the user at the provisioned device. The obvious drawback of this is that it doesn't work for headless devices – it requires at least a numerical key pad to type the PIN.

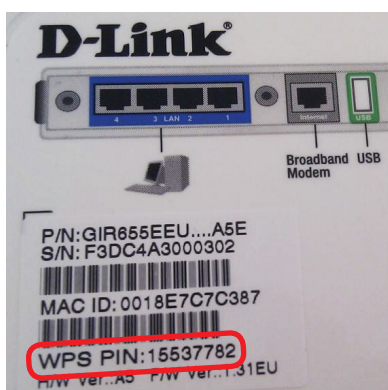


Figure 1. For example, WPS PIN printed on a D-Link® AP (left) and WPS push button on a Cisco AP (right)

In the PBC method, the user pushes a button on both the AP and the provisioned device. Once the button on the AP is pushed, WPS-enabled devices can freely join the network for a period of 2 minutes. The drawback of this method, beyond the lack of security during the 2-minute period, is that the user must have physical access to the AP. If the AP is located in a hard-to-reach place, the method can be cumbersome.

In both PIN and PBC methods, the AP and the provisioned device exchange a series of messages to establish a temporary secure connection that is used to deliver the SSID and the password from the AP to the provisioned device.

A major problem in WPS was unveiled in 2011 by Stefan Viehböck¹, who found a design flaw in the PIN method that allows brute-force attack to expose the network password in less than four hours. Since the PIN method is mandatory to achieve WPS certification, all new APs released to the market starting 2007 supported this method by default. Furthermore, many APs did not have an option to disable the WPS functionality.

Right after the security breach was discovered, most AP vendors came out with recommendations to disable WPS, and although most of them released product upgrades that prevented hacking, WPS received a bad reputation in the industry and is still avoided in some countries.

Access Point mode

Access Point (AP) mode is the most common provisioning method today for headless devices. In AP mode the un-provisioned device wakes-up initially as an AP with an SSID defined by the equipment manufacturer. Before trying to connect to the home network for the first time, the un-provisioned device creates a network of its own, allowing a PC or a smart phone to connect to it directly to facilitate its initial configuration.

In this mode, the un-provisioned device also includes an embedded web server. After the user connects his smartphone to the un-provisioned device's AP, he opens the smart phone's web browser and browses into the device's web site via a pre-defined local URL or IP address.

In the embedded web site, the user chooses (or types in) the home network name and password. The device stores the network credentials in nonvolatile memory and then it switches from AP mode to Station mode in order to connect to the home network using the stored network credentials.

Figure 2 is an iPad screen capture of the SimpleLink™ Wi-Fi CC3200 from Texas Instruments (TI) setup tab of the on-chip web site. The setup tab allows the user to provide the SSID and the security key for

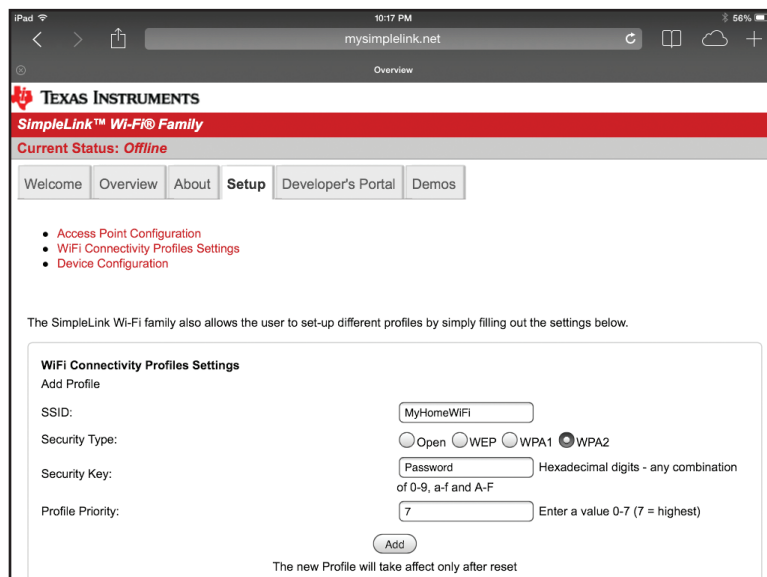


Figure 2. The SimpleLink Wi-Fi CC3200 on-chip web server setup page

multiple network profiles. After the configuration is done, the CC3200 (or CC3100) will automatically connect to one of the available networks, based on a user-configurable priority².

The primary benefit of AP mode provisioning is that it uses standard capabilities that exist in any smart phone, tablet and PC. Another benefit is that the vendors can add additional parameters to the embedded web site to configure other device functions at the same time when the device is provisioned on the Wi-Fi network.

For increased security a push button on the device can be used to activate the Access Point mode, and a pre-defined password for the configuration AP can be used.

A disadvantage of the AP mode is that when connecting to the configuration AP network of the un-provisioned device, the phone gets disconnected from the home network. This can cause data outage and trigger error messages. On a PC, if both Wi-Fi and Ethernet connections are active, the browser may prioritize the Ethernet connection and may not connect to the un-provisioned device over Wi-Fi. The user will have to disconnect the Ethernet connection before Wi-Fi provisioning in AP mode is used.

Recently released smartphones check that the Wi-Fi network is actually connected to the Internet. If Internet connection fails (like it would when the phone is connected to the AP of the un-provisioned device), these smartphones disconnect from the Wi-Fi network and then force a cellular data connection. Disabling this phone behavior is possible, but it requires advanced settings in the device configuration page which complicates the user experience.

Apple Wireless Accessory Configuration (WAC) feature

The Wireless Accessory Configuration (WAC) feature is an Apple MFi licensed technology designed for MFi accessories that connect to iPod, iPhone and iPad. MFi accessories that support WAC can be easily configured by an iPod, iPhone and iPad, without requiring the user to type in the network name and password. Detailed information about the WAC feature is available to Apple MFi Development and Manufacturing licensees.

SmartConfig™ Technology

SmartConfig technology is a TI proprietary provisioning method designed for headless devices introduced in 2012. It uses a mobile app to broadcast the network credentials from a smartphone, or a tablet, to an un-provisioned TI Wi-Fi device. When SmartConfig is triggered in the un-provisioned device, it enters a special scan mode, waiting to pick up the network information that is being broadcasted by the phone app. The phone needs to be connected to a Wi-Fi network to be able to transmit the SmartConfig signal over the air. Typically this is the same home network onto which the new device is going to be provisioned.

The Wi-Fi network name (SSID), that the phone is connected to, shows up automatically on the phone app. The user then adds the network password and presses the “Start” button to begin the process. There is also an option to add a device name, which is broadcasted by the phone, together with the network information and programmed to the Wi-Fi device memory. For enhanced security, SmartConfig has an option to encrypt the

broadcast data with a pre-shared key between the device and the phone. The pre-shared key is typically printed on a label on the device box, and could be scanned by the phone app before the SmartConfig process starts.

After the network credentials are picked up by the SimpleLink device, it connects automatically to the network and sends out a service discovery message back to the phone. The phone app picks the service discovery message and presents a notification to the user that a new device was provisioned successfully.

Figure 3 shows example screenshots of the SmartConfig App. On the left side screen shot, the user types in the password and a device name. On the right side screen we see a notification coming when the device provisioning is successful.

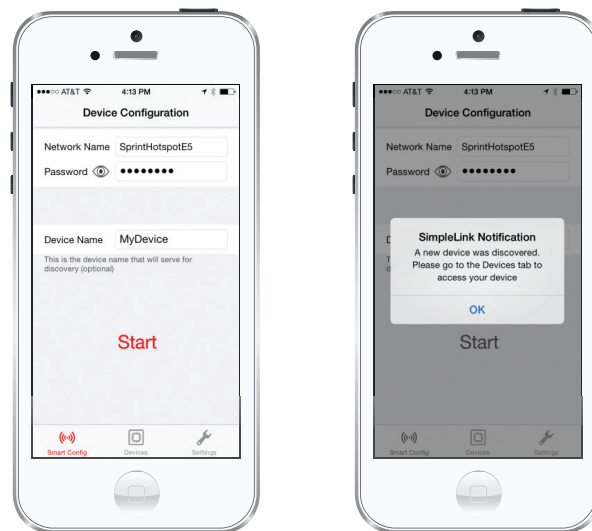


Figure 3. TI's SmartConfig phone app

TI provides a SmartConfig library for iOS and for Android™, and demo apps on the Apple App store and on Google Play. The source code of the app is available to download from the [TI web site](#). Many IoT products have phone apps that are used to control and monitor the IoT device, and to register the product online. Vendors can use the SmartConfig library to easily integrate the SmartConfig function into their own apps.

The two key benefits of SmartConfig are ease of use and the potential to integrate seamlessly into the phone app of the product. Another unique capability of SmartConfig technology is the ability to provision multiple devices simultaneously. If multiple Wi-Fi devices are in SmartConfig mode at the same time, one phone app can provision all of them at the same time.

Besides the fact that SmartConfig works only on TI devices, its main drawback is the fact that the phone needs to be connected to a network using frequency band and data rate that is supported by the un-provisioned device. For example, if the un-provisioned device supports only the 2.4GHz band, and the phone is using the 5GHz band to communicate with a dual-band network, then SmartConfig will not work, simply because the un-provisioned device is not listening on the 5GHz band. Some new routers and phones are using proprietary data rates to increase throughput and may also not work with SmartConfig.

Since the vast majority of routers are operating in the 2.4GHz band and using standard Wi-Fi rates, Smart-Config technology works well in most scenarios.

Out-of-band provisioning

The provisioning methods mentioned so far can be referred to as *in-band provisioning* because they are using the Wi-Fi radio to deliver the network information to the un-provisioned device. The benefit of in-band provisioning is that it does not require additional interfaces or system components to perform provisioning, but rather use the same Wi-Fi radio built into the product.

Out-of-band provisioning methods use a non-Wi-Fi medium to deliver the network information to the provisioned device. Out-of-band provisioning can be wired, for example using a USB interface, or wireless, for example using a near field communication (NFC) radio, or *Bluetooth*[®]. Adding out-of-band provisioning to a product adds robustness and flexibility, but increases the solution cost.

Design consideration

So far we reviewed the leading Wi-Fi provisioning methods in the market and discussed some of their key properties, their advantages and weaknesses. In the following sections we cover the essential considerations one should contemplate when choosing the provisioning method(s) and provide guidelines for choosing the right method for different applications. We will focus on the in-band provisioning methods, as they introduce the most questions and challenges.

Ease of use

Ease of use is a critical consideration in consumer products. Many simple IoT devices are targeting common home users, who have limited understanding of the provisioning process and sometimes have no or limited skills to operate computers. Because provisioning is the first thing users do when they open the product's box, it can shape their entire opinion about the product. In these cases, ease of use is a top priority for the designer.

In considering ease of use, we look at trivial things like the number of steps a user undergoes to provision a device. We also ask ourselves, if the user needs to exercise tools he already knows, or does he need to learn new tools to accomplish the task.

WPS, WAC and SmartConfig technology are the easiest to use methods. While WPS requires no knowledge and no tools what so ever, it does require physical access to the Wi-Fi router to push the WPS button. Since most smartphone users are familiar with downloading and using phone apps, SmartConfig technology offers a familiar interface to the user, but it does require the user to type in the network password.

Security

The two main security risks related to Wi-Fi provisioning are: (i) an eavesdropper can obtain the network password and use it to connect to the home network, and (ii) a malicious attacker can use the provisioning window of the device to take it over. In most cases the former risk is of most concern.

It is reasonable to say that security risks in Wi-Fi provisioning of IoT devices are limited in all provisioning methods that were covered in this paper, if used correctly. Since the provisioning is done only once in a product lifetime, or at least very rarely. Additionally, during provisioning the network password is transmitted over a short period, at a time controlled by the user. An attacker needs to know exactly when the provisioning is happening, and has a very short period of time to perform the attack. Moreover, the attacker needs to be within the Wi-Fi range of the network at the time the provisioning is taking place. Nevertheless, the importance of security should never be underestimated, and it is critical in many applications.

AP mode, WAC and SmartConfig technology have built-in security. While in AP mode and in SmartConfig the designer must choose to use security (that is, in AP mode the AP has to be configured for security, and in SmartConfig encryption has to be explicitly selected), in WAC, provisioning security is always used.

The security risk in the WPS push button method is that while the AP is in WPS mode, any Wi-Fi device around can use WPS to connect to the Wi-Fi network.

Robustness and flexibility

Robustness and flexibility are tightly coupled to ease of use, because they relate to the chances that provisioning won't work or will require troubleshooting. Yet, it deserves a parted discussion, as each of the provisioning methods bears some unique limitations.

The evident limitation of WPS is that not all APs support it. Many of the APs that do support WPS have disabled it by default because of the security breach in the PIN method that was discussed earlier. If WPS is disabled, the user will need to log into the web portal of the AP to enable the WPS function. This procedure is too complicated for many user.

SmartConfig technology has some inherent limitations that were discussed above, which can make it fail when provisioning to some APs using the 5GHz band or using proprietary data rates.

AP mode is probably the most robust and ubiquitous Wi-Fi provisioning method. Excluding some new phones that disconnect a Wi-Fi network that is not connected to the Internet, behavior that can be disabled as discussed above, AP mode provisioning will work in most cases. This is probably the reason most IoT devices and products today use it as their provisioning method.

In cases where robustness is the outmost consideration, an out-of-band provisioning method such as USB should be considered.

Unification

While WPS and WAC perform a single function – Wi-Fi provisioning – AP mode and SmartConfig technology can be nicely integrated into the product control framework and assimilate with other product functions. SmartConfig technology can be integrated with the products' phone app to provide a uniform user experience, allowing multiple configuration options to be carried through the same user interface. AP mode provides similar benefits while using a web browser to interact with multiple functions of the product in one place.

Conclusion

We've discussed the predominant Wi-Fi provisioning methods for headless devices and highlighted their merits and challenges. As it is palpable that no provisioning method is perfect, a good practical approach could be supporting more than one option in the product.

In the case of professional or industrial products, AP mode may be sufficient, as it has the best robustness and flexibility. Many IoT products today choose AP mode as their only provisioning method.

In the case of MFi accessories that connect to iPod, iPhone and iPad, WAC is the natural choice. To support provisioning with other kinds of phones, tablets or PCs, an additional provisioning method should be added to the accessory.

When ease of use is critical, WPS or SmartConfig technology are appropriate, because they provide the simplest user experience. SmartConfig technology is a natural choice when phone app experience is desired. WPS is the right choice when phone app is not mandated.

WPS or SmartConfig will cover the majority of products' installations but since they do not work in 100% of all cases, it is recommended to add AP mode as an option to the product as an "expert mode". Users can be directed to guidelines for operating AP mode in case they cannot run WPS or SmartConfig.

Provisioning with SimpleLink Wi-Fi CC3100 and CC3200

The SimpleLink Wi-Fi CC3100 and CC3200 platforms provide customers the most flexibility with provisioning methods by supporting all of the in-band methods discussed here. Through its novel SimpleLink APIs and autonomous Wi-Fi manager capabilities, CC3100 and CC3200 make provisioning a simple task to the product designer. The application can trigger any of the provisioning methods through simple API calls, and TI provides sample software for SmartConfig, AP mode and WPS. The Wi-Fi network name and password are automatically and securely stored in a serial Flash and used by the embedded Wi-Fi manager to connect to the network without any user involvement and with no application code.

The on-chip web server of CC3100 and CC3200 makes AP provisioning extremely easy to design. The designer can incorporate pre-defined configuration tokens into HTML web pages that are stored in the serial Flash and loaded automatically by the web server. To make things even easier, the CC3100 and CC3200 include a default on-chip web site for provisioning that makes AP provisioning work with no user code or effort at all. Learn more at www.ti.com/simplelinkwifi.

References

¹ **Viehböck, Stefan (2011-12-26). "Brute forcing Wi-Fi Protected Setup" (PDF)**

² Watch this **video** for a TI AP mode provisioning illustration

Important Notice: The products and services of Texas Instruments Incorporated and its subsidiaries described herein are sold subject to TI's standard terms and conditions of sale. Customers are advised to obtain the most current and complete information about TI products and services before placing orders. TI assumes no liability for applications assistance, customer's applications or product designs, software performance, or infringement of patents. The publication of information regarding any other company's products or services does not constitute TI's approval, warranty or endorsement thereof.

SimpleLink and SmartConfig are trademarks of Texas Instruments. All other trademarks are the property of their respective owners.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as "components") are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI's terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers' products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers' products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI's goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or "enhanced plastic" are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have **not** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

Products

Audio	www.ti.com/audio
Amplifiers	amplifier.ti.com
Data Converters	dataconverter.ti.com
DLP® Products	www.dlp.com
DSP	dsp.ti.com
Clocks and Timers	www.ti.com/clocks
Interface	interface.ti.com
Logic	logic.ti.com
Power Mgmt	power.ti.com
Microcontrollers	microcontroller.ti.com
RFID	www.ti-rfid.com
OMAP Applications Processors	www.ti.com/omap
Wireless Connectivity	www.ti.com/wirelessconnectivity

Applications

Automotive and Transportation	www.ti.com/automotive
Communications and Telecom	www.ti.com/communications
Computers and Peripherals	www.ti.com/computers
Consumer Electronics	www.ti.com/consumer-apps
Energy and Lighting	www.ti.com/energy
Industrial	www.ti.com/industrial
Medical	www.ti.com/medical
Security	www.ti.com/security
Space, Avionics and Defense	www.ti.com/space-avionics-defense
Video and Imaging	www.ti.com/video

TI E2E Community

e2e.ti.com