# Wi-Fi CERTIFIED Easy Connect™ Technology Overview


## June 2018

# Introduction

Providing a user-friendly, secure process for connecting Wi-Fi® devices to a network is essential for the continued growth and penetration of Wi-Fi technology. This is especially true for market segments such as smart home and Internet of Things (IoT) that include devices with limited or no interface. Configuring a Wi-Fi device to connect to a network requires the device to be given network information and security credentials. Adding devices with little or no user interface to a network can be cumbersome and is dependent upon vendor implementation. Using a standardized, simple method to configure Wi-Fi devices gives users more choice in selecting products from different vendors and provides a harmonized user experience across the ecosystem.

Wi-Fi Alliance® has created Wi-Fi CERTIFIED Easy Connect™ to simplify the process for adding devices—including those with little or no user interface—to a Wi-Fi network. Wi-Fi Easy Connect™ establishes a standardized mechanism for configuring Wi-Fi devices with greater simplicity, making setup as effortless as scanning a product quick response (QR) code with a smartphone to enable use on a Wi-Fi network.

Wi-Fi Easy Connect is an asset to the Wi-Fi Alliance portfolio, bringing new mechanisms that enable easy network setup and provisioning of client devices while providing a better user experience, enhanced security, and support for IoT device provisioning.

This document provides an overview of the Wi-Fi Easy Connect program and key components of the technology. Further details may be found in the Wi-Fi Alliance Device Provisioning Protocol Technical Specification.

# Wi-Fi Easy Connect basics

Wi-Fi Easy Connect allows a home or office network owner to use a trusted device, such as a smartphone, to set up an access point (AP) to authorize and manage network access by other client Wi-Fi devices. The Wi-Fi Easy Connect protocols help streamline the user experience while maintaining secure connectivity to that network using robust, well-established cryptographic principles.

## Device roles

### Configurator

In a Wi-Fi Easy Connect network environment, a main device is designated as a configurator. The configurator is a central point of configuration for all devices on the network, including the initial network AP. A Wi-Fi Easy Connect configurator can be on any trusted device within the Wi-Fi network. Deployment models possible for a configurator include:

**Mobile device**: Likely the most common deployment model, a device such as a smartphone or tablet may be used as a configurator, initiating the Wi-Fi Easy Connect protocol through an application on the device. The examples in this paper use a smartphone as the configurator.

**AP accessed through a web interface:** In this deployment model the user logs into the AP administration screen and runs the Wi-Fi Easy Connect configurator, initiating the protocol to provision a new enrollee.

**AP accessed through an application:** In this deployment model configurator functionality is on the AP but instead of a web interface, the network owner uses an application on a computer or mobile device to tell the configurator to initiate the protocol.

### Enrollee

Devices that the network owner wants to connect to the network are called enrollees. This includes any APs that are added to the network, as well as smart appliances, computers, printers, TVs and more. Any device with Wi-Fi capability that is not the configurator is considered an enrollee.

## Establishing the network

To set up a network using Wi-Fi Easy Connect, the configurator device runs the Wi-Fi Alliance Device Provisioning Protocol to provision an initial enrollee AP. It then provisions enrollee client devices, allowing them to discover, select, and connect to the network. During the initial enrollment process, shown in Figure *1*, the owner uses a mobile device as the configurator to configure the AP, which is considered the enrollee. This configuration, which can occur prior to network association, establishes the network.


Figure 1. Wi-Fi Easy Connect access point configuration

## Enrolling and connecting client devices to the network

Once the network is established, the network owner can begin enrolling devices, as shown in Figure 2. Each candidate device, or enrollee client, obtains its own configuration, enabling it to join the target network. The configuration process produces security credentials unique to that network and Wi-Fi device resulting in a mutually trusted connection to the Wi-Fi network (see Device Provisioning Protocol section for more detail).

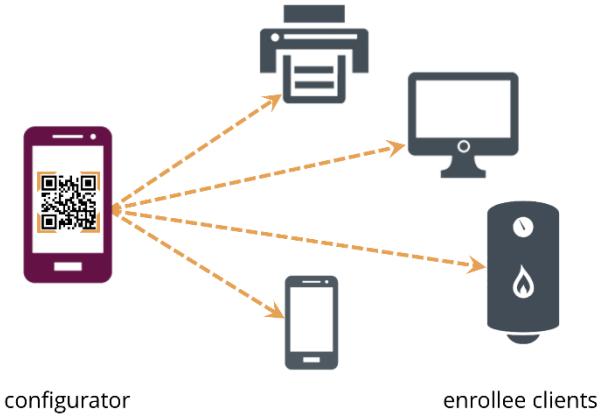


Figure 2. Enrollment of devices using Wi-Fi Easy Connect

Once a Wi-Fi device has been enrolled, it uses its configuration to discover and connect to the network through an AP. This is shown in Figure 3.

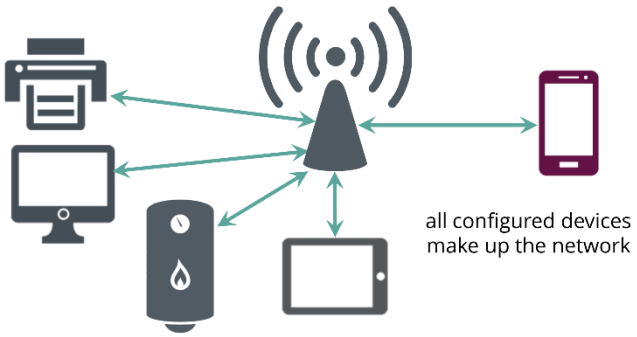


Figure 3. Devices associated to an AP after Wi-Fi Easy Connect enrollment

Networks set up using Wi-Fi Easy Connect technology are easy to keep current: replacing an AP may be completed without the need to re-enroll all client devices.

## Improving the user experience for adding devices to Wi-Fi networks

Wi-Fi Easy Connect was developed to make the user experience of adding devices to a Wi-Fi network much simpler and streamlined. Wi-Fi Easy Connect supports several different mechanisms, called bootstrapping mechanisms, that allow the secure introduction of configurator and enrollee devices while minimizing the need for manual interaction on each device. To bring this concept to reality, Wi-Fi Easy Connect employs QR codes, such as the one in Figure 4, for enrollee devices. QR codes are capable of housing a lot of information, including security keys and unique identifiers for a device. They are easily read by any device that has the ability to scan a QR code, eliminating the burden of manually entering information to authenticate a device as well as data entry errors which cause frustration for the user.

Figure 4. QR code

An example user experience for provisioning using QR codes and a mobile device as configurator follows:

1. The user utilizes the camera on the configurator device to scan the QR code displayed by the enrollee device. Note that the QR code could be displayed using a sticker or card.
2. After the configurator reads and decodes the QR code, it automatically discovers and sets up a secure Wi-Fi communication link with the enrollee device.
3. The configurator uses the secure channel to configure the Wi-Fi network information on the enrollee device.
4. Once configured, the enrollee device uses the Wi-Fi network information delivered by the configurator to discover, select, and connect to the Wi-Fi network without the need for human intervention.

If the configurator and enrollee device do not have the capability to read or display a QR code, they may still be configured using a manually entered human-readable string, which sets up the secure communication link for automatic configuration and connectivity.

Wi-Fi Easy Connect technology is flexibly designed to accommodate many ways to provision devices and supports either the configurator or the enrollee initiating the provisioning protocol. As described in examples above, a smartphone acting as a configurator can be used to scan the QR code of an IoT enrollee device and provision Wi-Fi network configuration. Alternatively, the configurator could display a QR code for an enrollee device to scan and be provisioned with Wi-Fi configuration. For instance, a hotel network configurator can send a QR code to one of the hotel room TVs. The guest can use their smartphone to scan the code on the TV. The protocol runs and onboards the smartphone to the hotel Wi-Fi network.

## Device Provisioning Protocol (DPP)

Created by Wi-Fi Alliance, DPP consists of a four-step process: bootstrapping, authentication, configuration, and network access. The first three steps require one device acting as a configurator and a peer device acting as the enrollee. A configurator is responsible for configuring devices connecting to the network or, in the case of an AP, providing network access. An enrollee is either a client device or an AP. Once configured, an enrollee can either connect to an AP to establish network access, or act as an AP to provide network access.

### Bootstrapping

Every device capable of using Wi-Fi Easy Connect ships with an identity. These identities are contained in a QR code or human-readable string, either printed or digitally available, in the form of public and private keys. The public key is shared; the private key is kept secret but is decodable when a secure connection occurs between the two devices. During this process, called bootstrapping, the configurator and enrollee establish a trust relationship that allows them to authenticate and establish a secure connection. Bootstrapping involves the

exchange of public keys, which can be exchanged in one or both directions, depending upon whether mutual authentication is required. Bootstrapping is performed by either scanning the QR code or exchanging a human-readable string that is then used to securely exchange public bootstrapping keys to establish contact. Public keys are not part of the security credential that an enrollee receives during configuration.

The bootstrapping information encoded in a QR code is a Uniform Resource Identifier (URI) that includes the bootstrapping public key of the device, in compressed form and base64uri-encoded, displaying the QR code along with additional information to set up a secure link for the exchange of configuration information. The bootstrapping URI includes the public key of the device and can optionally include channel information, the device medium access control (MAC) address, or any other information to establish a secure link.

For example, the following URI includes a public key as well as operating channels of 1 and 36. Figure 5 shows the representative QR code:

> DPP:C:81/1,115/36;K:MDkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDIgADM2206avxHJaHXgLMkq/24e0rsrfMP9K1Tm8gx+ovP0I=;;

Figure 5. Example QR code for Bootstrapping

## Authentication and configuration

Once bootstrapping has completed, the configurator and enrollee use the DPP authentication protocol to establish a secure Wi-Fi connection. After the secure connection has been established, the enrollee initiates a transaction to obtain configuration from the configurator. Once the configuration transaction has successfully completed, the enrollee is configured to either operate as an AP or discover and securely connect to the target AP.

The encoded configuration information includes a configuration object which contains the configuration objects below:

- A Wi-Fi technology object which specifies the type of connection, such as an AP infrastructure connection
- A discovery object which includes the service set identifier (SSID)
- A credential object which includes the security credential information

During the configuration process, provisioning of security credentials and network information, such as the SSID, is passed from configurator to the enrollee. The security credentials can include a connector, which is a credential signed by the configurator to allow an enrollee client device to connect to an enrollee AP. Each enrollee connector consists of a public key, a network role, group attribute information, and is signed by the configurator. The public key provides the identity of the enrollee device. The network role indicates whether the device is permitted to be an enrollee client device or an enrollee AP. The group attribute information is used by the enrollees to determine whether they are permitted to establish network connectivity. The connector signature proves that the connector content has been generated by the configurator. Since the connector contains a public key and not a passphrase, the security credential is unique to the Wi-Fi device owning it. This means that no other device can use the connector to gain access to a network and, in case the connector belongs to an AP, that no other AP can masquerade as that AP.

An enrollee client device uses the network information to discover the enrollee AP. It then uses its connector to authenticate and establish network connectivity using the network introduction protocol. An advantage of using connectors is that each device connecting to an AP has a unique security credential.

### Network access

The network introduction protocol allows an enrollee client device to securely connect to an enrollee AP using connectors provided by a configurator. During the network introduction protocol:

- Enrollee client device and enrollee AP validate that each connector is signed by the configurator
- Enrollees validate that their roles are complementary: an enrollee client is establishing communications with an enrollee AP
- Enrollees validate that the group attributes match
- Enrollee client and enrollee AP mutually derive a unique pairwise master key (PMK) based on their public connector keys
- Enrollee client and enrollee AP establish connectivity

## Prerequisite requirements

Devices seeking to receive Wi-Fi CERTIFIED Easy Connect certification shall implement and pass at least one of the following Wi-Fi Alliance certifications as a prerequisite, as well as Wi-Fi CERTIFIED WPA2™ with Protected Management Frames:

- Wi-Fi CERTIFIED™ a
- Wi-Fi CERTIFIED b
- Wi-Fi CERTIFIED g
- Wi-Fi CERTIFIED n
- Wi-Fi CERTIFIED ac

## Summary

Wi-Fi Easy Connect is a technology that allows secure Wi-Fi configuration and network access with minimal user interaction. It brings a standardized approach that makes securely adding devices to Wi-Fi networks much simpler than ever before. The technology is easy to use and very flexible: enrollment of devices can be done through secure device-to-device connections and enables the replacement of APs without requiring re-enrollment of client devices. Wi-Fi Easy Connect is applicable for different classes of Wi-Fi devices on the market today, including those with little or no interface such as IoT equipment, Wi-Fi capable appliances, and mobile devices.

More information about Wi-Fi Easy Connect is available at: www.wi-fi.org/discover-wi-fi/wi-fi-easy-connect.

## About Wi-Fi Alliance®

www.wi-fi.org

Wi-Fi Alliance® is the worldwide network of companies that brings you Wi-Fi®. Members of our collaboration forum come together from across the Wi-Fi ecosystem with the shared vision to connect everyone and everything, everywhere, while providing the best possible user experience. Since 2000, Wi-Fi Alliance has completed more than 40,000 Wi-Fi certifications. The Wi-Fi CERTIFIED™ seal of approval designates products with proven interoperability, backward compatibility, and the highest industry-standard security protections in place. Today, Wi-Fi carries more than half of the internet's traffic in an ever-expanding variety of applications. Wi-Fi Alliance continues to drive the adoption and evolution of Wi-Fi, which billions of people rely on every day.