



Wi-Fi Easy Connect using DPP URIs or QR Codes APPNOTE-38



Table of Contents

1 Scope	3
2 Theory of Operation	4
3 How to Configure	6
3.1 Configuring the Extender	6
3.1.1 Accessing the terminal	6
3.1.2 Generate a private key	7
3.1.3 Configure wpa_supplicant	7
3.1.4 Record the DPP URI (which includes the public key)	7
3.1.5 Confirm that wpa_supplicant is working	7
3.2 Configuring the Access Point	8
3.2.1 Determine the current Wi-Fi credentials	8
3.2.2 Configure hostapd and register the DPP URI	8
3.2.3 Verify that your Extender is correctly provisioned	9
4 How to Verify	10
5 FAQs	11
What happens if I change the SSID/password on an AP after provisioning devices?	11
Can I use DPP URIs with HaLowLinks out of the box?	11
How would I use DPP URIs in a product?	11
How can an Access Point ever read a QR code if it doesn't have a camera?	11
6 Revision History	12

1 Scope

This document briefly introduces the rationale for Wi-Fi Easy Connect and provides manual instructions that demonstrate Wi-Fi credential sharing between two HaLowLink devices via a Device Provisioning Protocol (DPP) Uniform Resource Identifier (URI).

DPP URIs are frequently printed as QR codes, but the QR code on the HaLowLink label does **not** contain a DPP URI; it is rather a Wi-Fi credentials URI¹ which is only useful for devices that can read QR codes directly. Therefore, this App Note will involve using the terminal and manually copying the DPP URI from one device to the other. To make this suitable for end users, you would need to build additional software to automate the process.

The prerequisites for this application note are:

- 2 x [Morse Micro HalowLink](#) (1 or 2) devices with the latest software installed (this guide was written based on Morse Micro OpenWrt v2.11)
- 1 x Laptop with two USB-C ports (or USB-A to USB-C adapters)

¹ This is defined in section 7 of the [WPA3 Specification](#).

2 Theory of Operation

With traditional computers and mobile devices, users typically enter Wi-Fi credentials through a user interface to connect to a network; in most cases, the user types a known SSID and key into their computer. Devices without an easily accessible user interface need another method to securely obtain Wi-Fi credentials.

The Wi-Fi Easy Connect standard defines the Device Provisioning Protocol (DPP) as a way to share credentials. DPP supports several mechanisms, and by default, HaLowLink supports using push buttons to initiate DPP².

Some devices lack buttons or a user interface, so they must use an alternate credential sharing technique - such as by scanning a QR code³; using NFC or Bluetooth⁴; or by using a trusted third party⁵. Many of these techniques work by encoding the credential bootstrapping information into a DPP URI⁶ and then sharing that URI securely.

In this app note, the DPP URI is shared as a trusted third party that has secure access to both devices via SSH. Designing a production-ready solution depends on a product's deployment and commissioning requirements, but it might involve encoding and scanning QR codes; implementing Bluetooth-based DPP via a smartphone; or distributing DPP URIs via a cloud-based service.

The basic principle is that a configurator is provided with the enrollee's public key, which allows the configurator and enrollee to establish a secure, encrypted connection and for the configurator to provide the enrollee with credentials for the Wi-Fi network. Then only the configurator needs a UI; the enrollee (i.e., the new device) does not. In this document, the Access Point (running hostapd) will function as the configurator, and the Clients/Stations (running wpa_supplicant) will be the enrollees.

This will work as follows:

1. A HaLowLink Extender which is configured with a public-private key pair (**A-a**)
2. A DPP URI is generated containing the HaLowLink Extender's MAC address and public key (**A**)
3. A HaLowLink Access Point where hostapd is a DPP Configurator
4. The DPP URI is provided to the DPP Configurator on the Access Point
5. The Extender emits DPP Presence Announcements until the Access Point detects it
6. The DPP Configurator on the Access Point recognizes the Extender as its key (**A**) was registered in (4)
7. The DPP Configurator on the Access Point securely provides the Extender with credentials

² See section 5.8 of the [Wi-Fi Easy Connect Specification v3.0](#)

³ See section 5.3 "Scanning a QR code" in the Wi-Fi Easy Connect Specification

⁴ See sections 5.4 "NFC" and 5.5 "Bluetooth" in the Wi-Fi Easy Connect Specification

⁵ See section 5.7 "Bootstrapping Using a Trusted Third Party"

⁶ See section 5.2 "Bootstrapping information", and 5.2.1 for the URI encoding

In this document, hostapd will act as the DPP Configurator, but depending on requirements, other services can act as the configurator, and indeed may not even be running on the Access Point (which could be an enrollee). For technical details about hostapd's DPP implementation, refer to [README-DPP](#).

For further information about Wi-Fi Easy Connect, refer to:

- [Wi-Fi Easy Connect™: Simple and secure onboarding for IoT](#)
- [Wi-Fi Easy Connect](#)
- [Wi-Fi Easy Connect Specification v3.0](#)

3 How to Configure

3.1 Configuring the Extender

By default, the HaLowLink is configured as a router with an access point. To reset the device into Extender mode:

- Connect your laptop to the device via USB-C.
- Wait for the Status LED to turn **solid green or aqua**.
- Reset the device by holding down the **mode** button on the bottom of the device until the Status LED starts **rapidly flashing aqua**, then release the button.
 - It will first flash green slowly. Keep holding the button down until it flashes aqua. If you accidentally release it earlier, wait until it's solid green again.
- Wait until it's **solid aqua**.

Because the device is now in Extender mode, it does not have a DHCP Server. However, you can use the static emergency recovery IP (10.22.121.111) to access it if you manually configure your laptop's Ethernet connection with the IP 10.22.121.110 (subnet mask 255.255.255.0).

3.1.1 Accessing the terminal

Now, we can use the terminal to set up DPP:

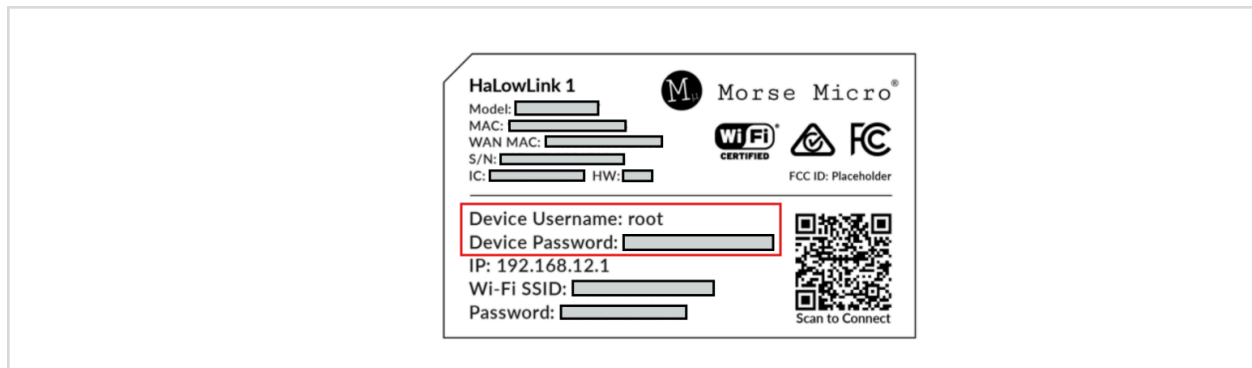


Figure 1: HaLowLink device sticker

- Go to <http://10.22.121.111> and log in using the username and password on your device.
- On the left-hand side menu, click **Advanced**, then go to **Services -> Terminal**, and use the same password as above to log in

3.1.2 Generate a private key

Generate the private key (/etc/dpp_key.pem is the default path used for the dpp_key variable in our wpa_supplicant configuration file; it is also possible to get wpa_supplicant to generate a key at runtime):

```
root@halowlink1-1947:~# openssl ecparam -genkey -name prime256v1 \
-noout -outform PEM > /etc/dpp_key.pem
```

3.1.3 Configure wpa_supplicant

Set the HaLow radio to emit DPP Presence Announcements (which will include the public key), confirming that radio1 is the correct radio (if it's not, try radio0):

```
root@halowlink1-1947:~# uci show wireless.radio1.type
wireless.radio1.type='morse'
root@halowlink1-1947:~# uci set wireless.default_radio1.dpp=1
root@halowlink1-1947:~# uci commit
root@halowlink1-1947:~# reload_config
```

3.1.4 Record the DPP URI (which includes the public key)

Determine the DPP URI beginning with "DPP:" and save this to use it later:

```
root@halowlink1-1947:~# wpa_cli_slg dpp_bootstrap_get_uri 1; echo
Selected interface 'wlan0'
DPP:M:94bb43dcf993;V:3;K:MDkwEwYHKOZIzj0CAQYIKoZIzj0DAQcDIgADpfVUMG
W64skm+qzbmcn1nw3cgZw+fA2oJgEYSIO6oAk=;;
```

3.1.5 Confirm that wpa_supplicant is working

Follow the logs to confirm that DPP-TX is happening. We suggest leaving this terminal open while you configure the Access Point:

```
root@halowlink1-1947:~# logread -f
wlan0: DPP-TX dst=ff:ff:ff:ff:ff:ff freq=5745 type=13
wlan0: DPP-TX dst=ff:ff:ff:ff:ff:ff freq=5805 type=13
wlan0: DPP-TX dst=ff:ff:ff:ff:ff:ff freq=5865 type=13
wlan0: DPP-TX dst=ff:ff:ff:ff:ff:ff freq=5745 type=13
wlan0: DPP-TX dst=ff:ff:ff:ff:ff:ff freq=5805 type=13
wlan0: DPP-TX dst=ff:ff:ff:ff:ff:ff freq=5865 type=13
```

3.2 Configuring the Access Point

By default, the HaLowLink is configured as a router with an access point. If you have modified the configuration, we suggest performing a factory reset before following this guide:

- Connect your laptop to the device via USB-C.
 - Do not remove the Extender. You should now have two HaLowLink devices connected to your laptop.
- Wait for the Status LED to turn **solid green or aqua**.
- Reset the device by holding down the **mode** button on the bottom of the device until the Status LED starts **flashing green**.
- Wait until it's **solid green**.

Now, we can make sure it's a configurator and register the Extender's public key:

- Go to <https://192.168.12.1> in a new tab/window, and access the terminal as you did for the Extender (but with the Access Point's username and password)

3.2.1 Determine the current Wi-Fi credentials

Get the SSID and key as hexadecimal values after confirming that radio1 is correct:

```
root@halowlink1-f4a1:~# uci get wireless.default_radio1.ssid |  
    tr -d '\n' | hexdump -v -e '/1 "%02x"'; echo  
68616c6f776c696e6b312d66346131  
root@halowlink1-f4a1:~# uci get wireless.default_radio1.key |  
    tr -d '\n' | hexdump -v -e '/1 "%02x"'; echo  
6c617a7930387465
```

Use these hexadecimal values for the **SSID** and **password (pass)** in the following section.

3.2.2 Configure hostapd and register the DPP URI

Connect to `hostapd_cli_s1g`, set it up as a configurator, and register the DPP URI from above. You **must** use the values that were determined above for `dpp_uri/key/ssid`:

```
root@halowlink1-f4a1:~# hostapd_cli_s1g dpp_configurator_add  
Selected interface 'wlan0'  
1  
root@halowlink1-f4a1:~# hostapd_cli_s1g set dpp_configurator_params  
    'conf=sta-sae ssid=<ssid> pass=<pass>'  
Selected interface 'wlan0'  
OK  
root@halowlink1-f4a1:~# hostapd_cli_s1g dpp_qr_code '<dpp_uri>'  
Selected interface 'wlan0'  
1
```

3.2.3 Verify that your Extender is correctly provisioned

Check the logs:

```
root@halowlink1-f4a1:~# logread -l 100 -f
...
wlan0: DPP-RX src=28:d0:43:80:f8:d6 freq=5280 type=13
wlan0: DPP-RX src=28:d0:43:80:f8:d6 freq=5805 type=13
wlan0: DPP-RX src=28:d0:43:80:f8:d6 freq=5280 type=13
wlan0: DPP-RX src=28:d0:43:80:f8:d6 freq=5805 type=13
wlan0: DPP-RX src=28:d0:43:80:f8:d6 freq=5280 type=13
wlan0: DPP-CHIRP-RX id=1 src=28:d0:43:80:f8:d6 freq=5280 hash=...
wlan0: DPP-TX dst=28:d0:43:80:f8:d6 freq=5280 type=0
wlan0: DPP-TX-STATUS dst=28:d0:43:80:f8:d6 result=SUCCESS
wlan0: DPP-RX src=28:d0:43:80:f8:d6 freq=5280 type=1
wlan0: DPP-AUTH-DIRECTION mutual=0
wlan0: DPP-TX dst=28:d0:43:80:f8:d6 freq=5280 type=2
wlan0: DPP-TX-STATUS dst=28:d0:43:80:f8:d6 result=SUCCESS
wlan0: DPP-AUTH-SUCCESS init=1 pkhash=... own=-1 peer=1
wlan0: DPP-CONF-REQ-RX src=28:d0:43:80:f8:d6
wlan0: DPP-BAND-SUPPORT 115,118,121,124,125
wlan0: DPP-ENROLLEE-CAPABILITY 1
wlan0: DPP-RX src=28:d0:43:80:f8:d6 freq=5280 type=11
wlan0: DPP-CONF-SENT conf_status=0
wlan0: STA 28:d0:43:80:f8:d6 IEEE 802.11: associated (aid 1)
wlan0: WDS-STA-INTERFACE-ADDED ifname=wlan0.sta1
sta_addr=28:d0:43:8
wlan0: AP-STA-CONNECTED 28:d0:43:80:f8:d6 auth_alg=sae
wlan0: STA 28:d0:43:80:f8:d6 RADIUS: starting accounting session...
wlan0: STA 28:d0:43:80:f8:d6 WPA: pairwise key handshake completed.
wlan0: EAPOL-4WAY-HS-COMPLETED 28:d0:43:80:f8:d6
```

4 How to Verify

After following the previous steps, the purple Wi-Fi HaLow LED light on the Extender should come on. You can verify that it's connected to your Access Point by going to the Access Point interface at <https://192.168.12.1> and clicking on the Access Point card to see the associated Clients:

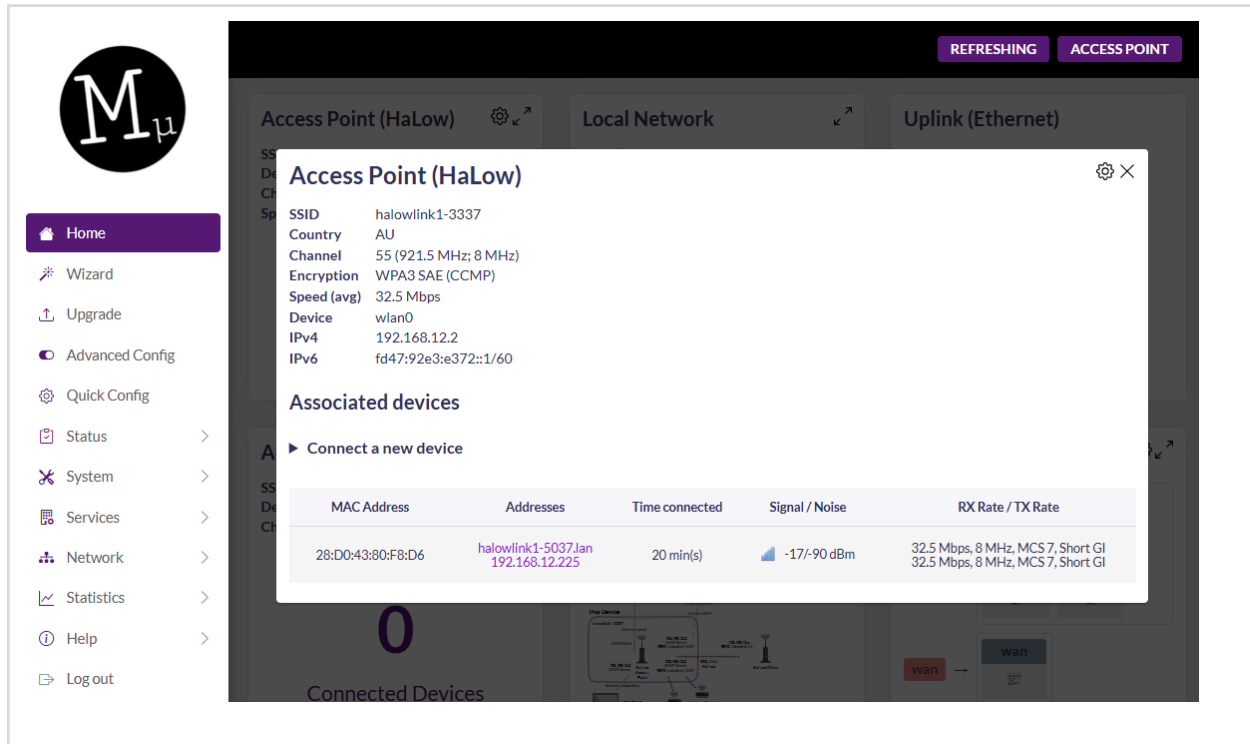


Figure 2: Expanded Access Point card with client list

You can also go back to the user interface of the Extender and click on the 'Uplink' card to confirm that it now contains the correct credentials.

Now that the credentials are stored, DPP has no further role, and you will be able to remove power from the devices, set them up elsewhere, and the Extender will re-authenticate with the Access Point.

5 FAQs

What happens if I change the SSID/password on an AP after provisioning devices?

With the mechanism described, because they are no longer using DPP and have stored the normal credentials, they will lose access. The devices would have to move back into DPP Presence Announcement mode (i.e., set dpp=1), and because hostapd's built-in configurator does not persist the DPP URIs, you would need to resubmit the enrollee's URI. You can and should use the same URI as before.

Can I use DPP URIs with HaLowLinks out of the box?

No, HaLowLink devices do not support this mechanism. This document describes how to experiment with using DPP URIs for those who might like to use them in a product, but there are missing pieces:

- HaLowLink devices are not provisioned with a DPP key on the device;
- HaLowLink devices do not have a DPP QR code containing the DPP URI printed on the device (the QR code on the device is rather the Wi-Fi credentials QR code);
- There is no user-friendly mechanism to read the DPP URI from an Extender and provide it to an Access Point (i.e., hostapd);
- When factory reset into Extender mode, they are not set to emit DPP Presence Announcements.

How would I use DPP URIs in a product?

One approach is to use the interaction described in this document, but fix the deficiencies discussed above. However, you may also consider:

- Using a custom configurator (e.g., a mobile application) which configures both Access Points and Clients. Depending on the device, this could even use 2.4 GHz Wi-Fi to do the credentials exchange;
- Provide the DPP URI of devices via some other mechanism; for instance, a trusted service could pre-populate DPP URIs. See section 5.7 of the Wi-Fi Easy Connect Specification v3.0 for a discussion of approaches.

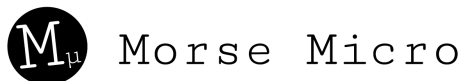
How can an Access Point ever read a QR code if it doesn't have a camera?

This could be done via the web UI (if run on a phone with a camera) or via a mobile app which could securely communicate with the Access Point.

6 Revision History

Version Number	Release Date	Release Notes
1	17 Sep 2026	Initial Release

Morse Micro provides this information "as is" without warranties of any kind, express or implied. No guarantee is made as to the accuracy, completeness, or suitability of this information or Morse Micro's products for any specific purpose. Use of this information and products is at the user's sole risk. Morse Micro products are not designed or tested for use in mission-critical systems, and should not be used in such applications. Performance specifications are based on internal testing and are believed to be reliable; however, they are not guaranteed. It is the Buyer's responsibility to test and validate all product performance, compatibility, and compliance, both in isolation and within end applications. Morse Micro assumes no liability for the use or application of any product, circuit, or information described herein. No license or other rights—express or implied—are granted under Morse Micro's intellectual property. This document contains proprietary information of Morse Micro and is subject to change without notice. Wi-Fi®, Wi-Fi HaLow™, and the Wi-Fi logo are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.



Morse Micro Pty. Ltd. Corporate Headquarters

Level 8, 10-14 Waterloo Street, Surry Hills, NSW 2010, AUSTRALIA

Email: sales@morsemicro.com

Copyright © Morse Micro Pty. Ltd.