



**COVR-2202 Tri-Band Whole Home Wi-Fi System
FAQ_English Ver.1.3**

HW Version	Firmware Version	App Name	App Version
A1	1.04	D-Link Wi-Fi	1.1.9 build 19 for Android; 1.1.9 build 23 for iOS

**Written By
Customer Service Department I of DHQ on Aug 29th, 2019**

Revision History

Revision	Date	Description
1.0	Aug 24 th , 2018	First Release
1.1	Sep 26 th , 2018	<ol style="list-style-type: none">1. Add 3rd party integration in Q10.2. Modify the content of Q7: Support up to 4 COVR Points3. Remove Q33: How do I connect COVR-2202 behind another router?
1.2	Jun 27 th , 2019	<ol style="list-style-type: none">1. Add Q33: Setting up bridge mode.2. Correct the content of Q10. Remove the wrong information of Google Assistance section below: <i>For Android devices, log in to Google app as your own Google account. Please set the language of your mobile device as English.</i>
1.3	Aug 29 th , 2019	Add 13-1~13-29: D-Link defend App for McAfee services

Contents

Device Setup/Installation	6
1-1: How do I set up my network with COVR-2202?	6
Method 1: Using the D-Link Wi-Fi App	6
Method 2: Using the web UI	25
1-2: How do I log in to my Covr Router?	32
1-3: How do I change the admin password on my router?	33
1-4: How do I change the wireless settings?	34
1-5: Why does my Covr Point keep losing connection?	35
1-6: Which Ethernet port can be used as WAN port?	37
1-7: How many Covr Points will work on my Covr-2202 Wi-Fi system?	38
1-8: How large is the coverage range of COVR-2202?	38
1-9: If I don't have ISP service at home, can I still create a LAN environment using COVR-2202?	38
1-10: Does COVR-2202 support Alexa/Google Assistant?	39
Google Assistant	39
Amazon Alexa	42
1-11: Does COVR-2200 support VLAN feature?	44
1-12: Can I adjust the 2.4GHz or 5GHz wireless bands for COVR-2202?	44
1-13: Can I turn off the LED (for both COVR router and COVR point(s)) for COVR- 2202?	45
1-14: What does the LED behavior on my COVR-2202 system mean?	47
Firmware Upgrade/Checking	49
2-1: How do I check the firmware version of my COVR-2202 system?	49
2-2: How do I upgrade the firmware on my Covr-2202?	50
Configuration Backup/Factory Reset	54
3-1: How do I backup/restore the configuration settings of my Covr router?	54
3-2: How do I reset my Covr router to factory default settings?	56
General Setting	57
4-1: How do I set up parental control features?	57
4-2: How do I configure DHCP IP reservation settings?	59
4-3: How do I change the router's IP address?	61
4-4: How do I enable remote management for my router?	62
Guest Zone Setting	64
5-1: How do I enable Guest Zone/Guest Access on my Covr router?	64
Port Forwarding/Virtual Server Setting	65
6-1: How do I enable DMZ on my router?	65
6-2: How do I open ports on my router?	66
Website Filter Setting	70
7-1: How do I set up a website filter on my router?	70

System Log & Statistics	72
8-1: How do I check the system log of my router?	72
8-2: How do I check network statistics for my router?	75
DNS/DDNS.....	76
9-1: How do I configure Dynamic DNS on my router?.....	76
QoS Setting	78
10-1: How do I configure QoS on my router?	78
Time/Schedule	79
11-1: How do I configure the time on my router?	79
11-2: How do I create a schedule on my router?.....	80
Bridge Mode.....	82
12-1: How do I configure my router to bridge mode?	82
D-Link defend App for McAfee services	84
13-1: What is Secure Home Platform?	84
13-2: How do I check the SHP and D-Link defend app version?	84
13-3: What do the security levels mean?	85
13-4: What information can we check of each client device in the device list?.....	87
13-5: How do I edit a device?.....	89
13-6: How do I block a device from the Internet access?	91
13-7: How do I install McAfee Antivirus protection on a mobile device or PC?	92
13-8: How do I remove a device which you no longer manage?	96
13-9: If a client device switches from a wired connection to wireless (or from wireless to wired), will the client device be discovered as a new device?	97
13-10: When a device is disconnected from the network, why does it still appear as online in the D-Link defend app?.....	97
13-11: Can parents be notified if new devices connect to your router?	98
13-12: How do I set up Parental Controls via D-Link defend app?	99
13-13: How does SHP make sure that a specific website is categorized as blocked or allowed?	104
13-14: Why does a certificate warning page appear when kids browse a blocked webpage?	104
13-15: Can SHP still prevent a device from visiting malicious sites when VPN is enabled or when proxy is set?	105
13-16: When the Internet is paused, why do some mobile apps, such as Facebook, stay connected to the Internet?	105
13-17: Why are video streaming still running after pausing the Internet?	105
13-18: What does vulnerability scan do?.....	106
13-19: What kinds of devices will be scanned when users scan vulnerability?.....	107
13-20: How do I check the SHP status in D-Link defend app?.....	109
13-21: Can users turn off SHP services in the D-Link defend app?	110

13-22: How do I manage my SHP-enabled routers in the D-Link defend app?.....112
13-23: How do I use D-Link defend features by Amazon Alexa voice commands? ..115
13-24: Does D-Link defend support The Google Assistant?.....117
13-25: How do I set up Away mode?.....118
13-26: How do I perform factory reset in the D-Link defend app?121
13-27: What features are available for SHP devices?122
13-28: Can I remotely control the D-Link defend app of my SHP-enabled router? ..122
13-29: If your network uses IPv6 only, would SHP work correctly on SHP-enabled
router?122

Device Setup/Installation

1-1: How do I set up my network with COVR-2202?

Method 1: Using the D-Link Wi-Fi App

Step 1: Download the D-Link Wi-Fi app from the App Store or Google Play:



Step 2: Launch D-Link Wi-Fi App. Tap **Install New Device**. Follow the on-screen instructions to complete the setup:



Note:

1. You'll be asked if you allow D-Link Wi-Fi to access your device's location after you launch the app. Please select **ALLOW**:



2. If you've installed before then re-install COVR-2202, you may see the screen below. Tap **Install new device** to continue the setup process:



Step 3: Select **Yes** to scan the QR code of your COVR-2202:

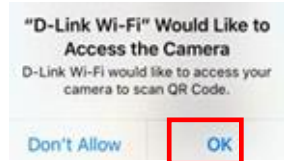
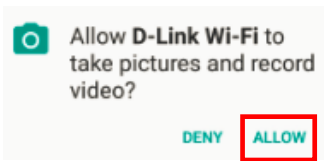


Note:

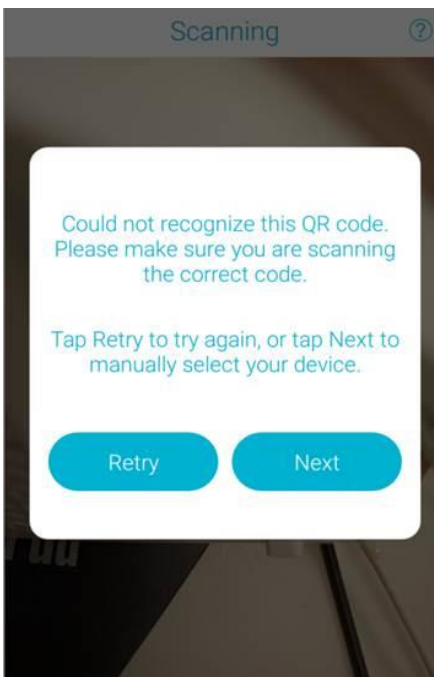
1. You'll be asked if you allow D-Link Wi-Fi to access your camera (for iOS)/take pictures and record video (for Android) to scan the QR code. Select OK/Allow to allow D-Link Wi-Fi app to access your camera.

Android:

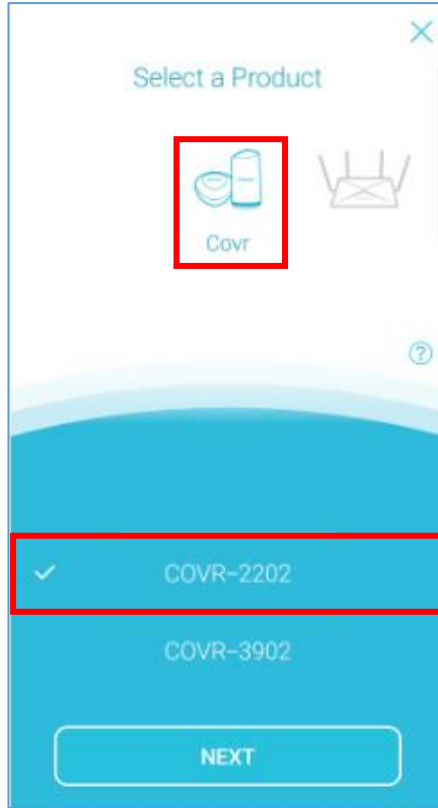
iOS:



2. If your mobile device can't successfully scan the QR code after a period of time, the below screen will pop up with the indication of recognizing QR code failed. Tap either "**Retry**" to try again, or "**Next**" to skip scanning and change to manual selection mode:

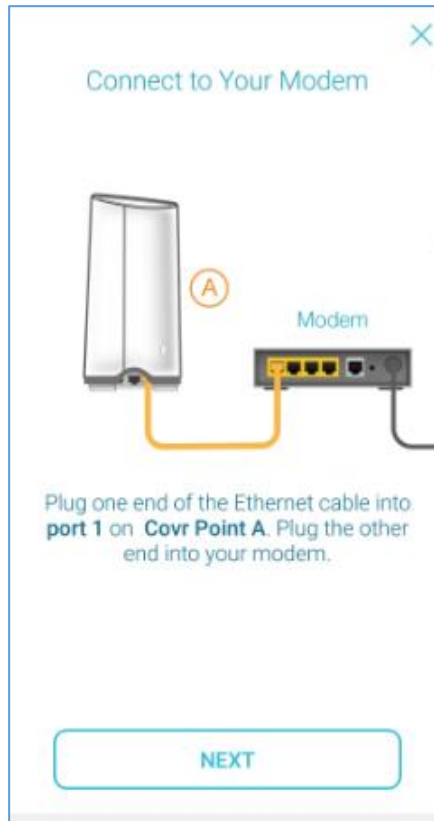
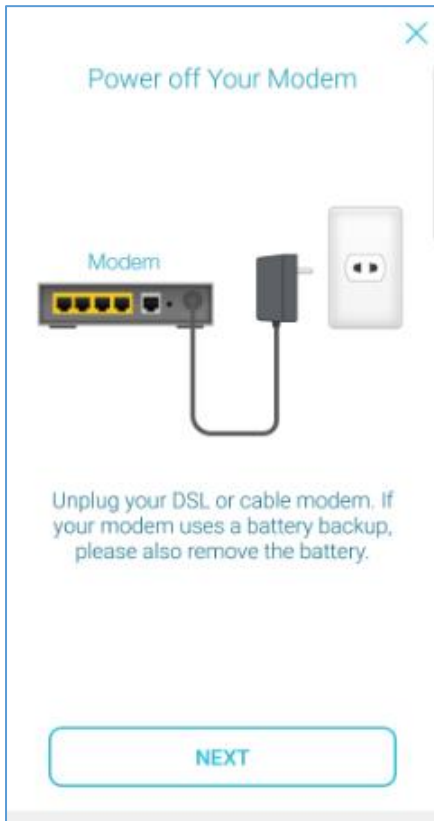


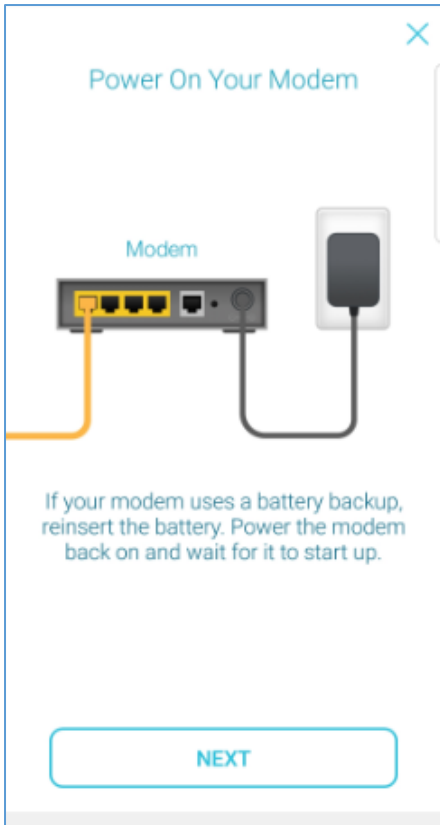
3. If there's no QR code on your device, please tap **"No"** and manually select **"Covr"** -> **"COVR-2202"**, then tap **NEXT**:



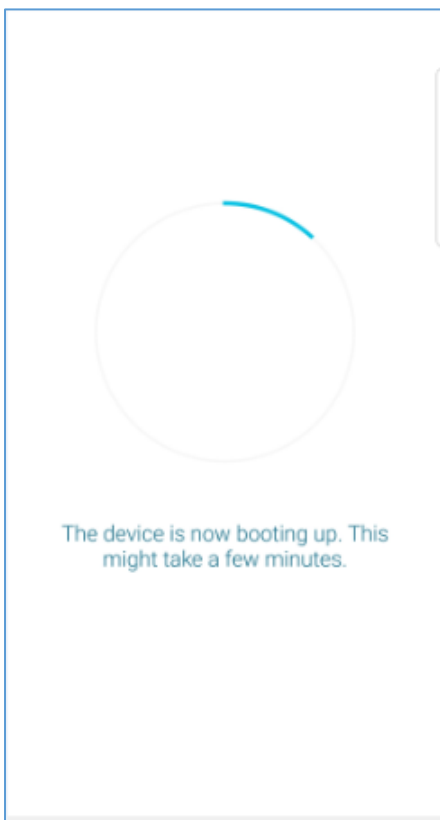
Step 4:

- Unplug your modem or gateway.
- Plug one end of the Ethernet cable into **port 1** on the **Covr Point A**.
- Plug the other end into your modem or gateway.
- Power the modem back on.
- Plug Covr Point A into a power socket. Then tap **NEXT**.

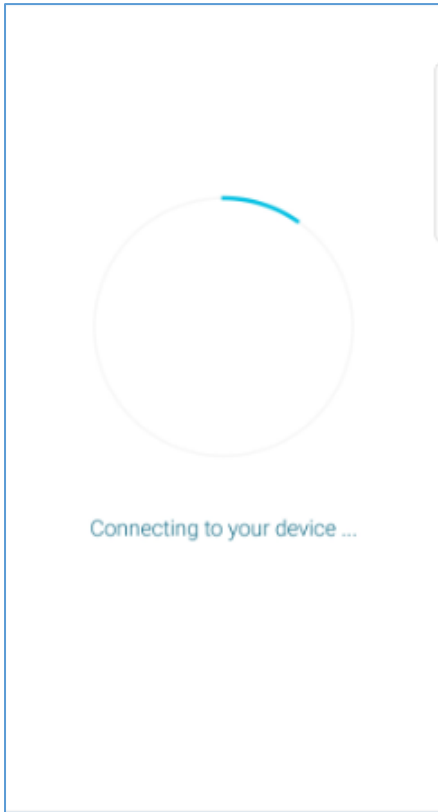




Step 5: Your device will start boot-up process. Wait till the COVR LED turns blinking orange, then tap **NEXT:**

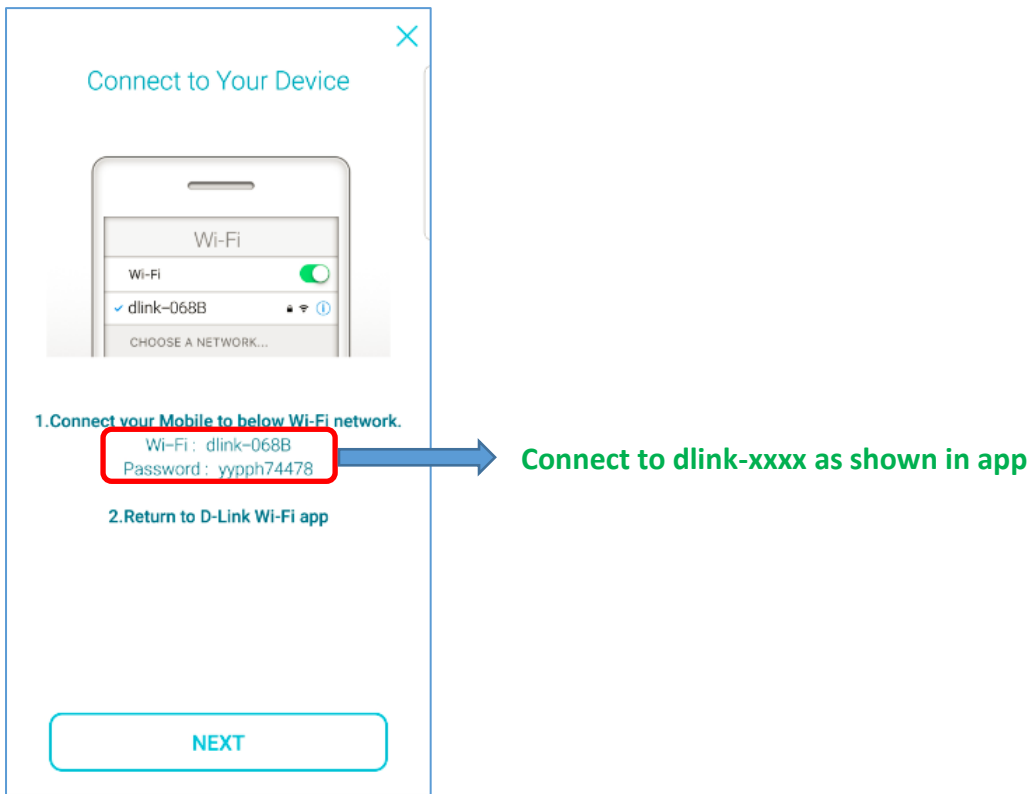


Step 6: Your device will initiate the connecting process:

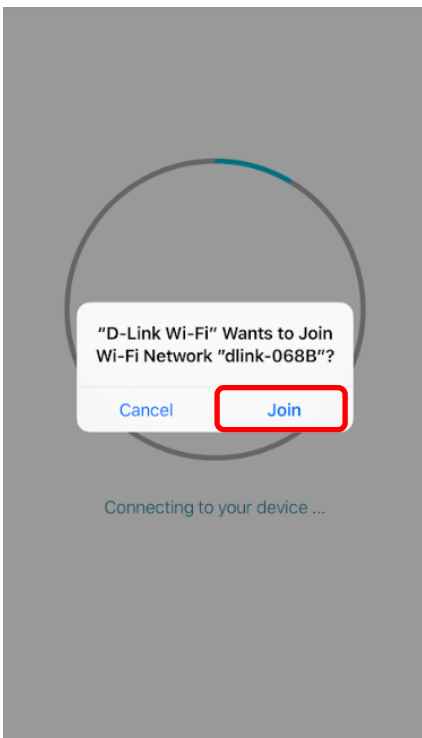


Step 7: Connect your mobile device or tablet to the Wi-Fi network (SSID) printed on the device label or included Wi-Fi configuration card (The default name will be in the format: "dlink-xxxx"). Once connected, return to the app and tap **NEXT** to continue:

Android:

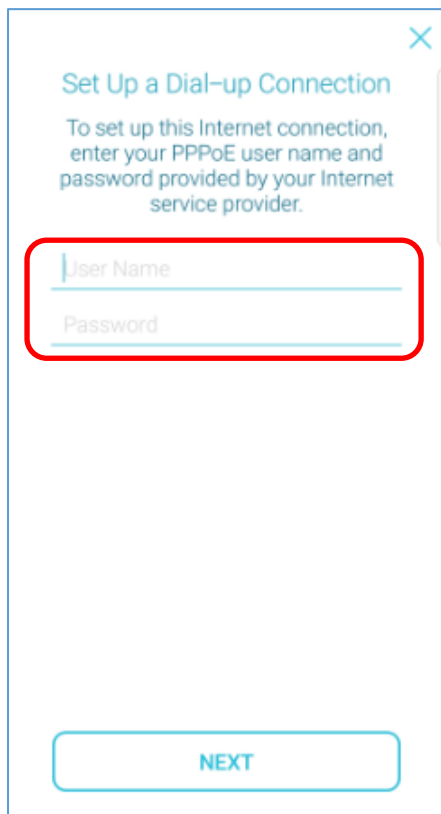


iOS: Please tap **"Join"** to connect your mobile to the Wi-Fi network (SSID) printed on the device label or included Wi-Fi configuration card:



Note: If already connected to D-Link network, you won't see this page.

Step 8: If a PPPoE connection is detected, enter your PPPoE user name and password provided by your ISP, then tap **NEXT**:



Set Up a Dial-up Connection

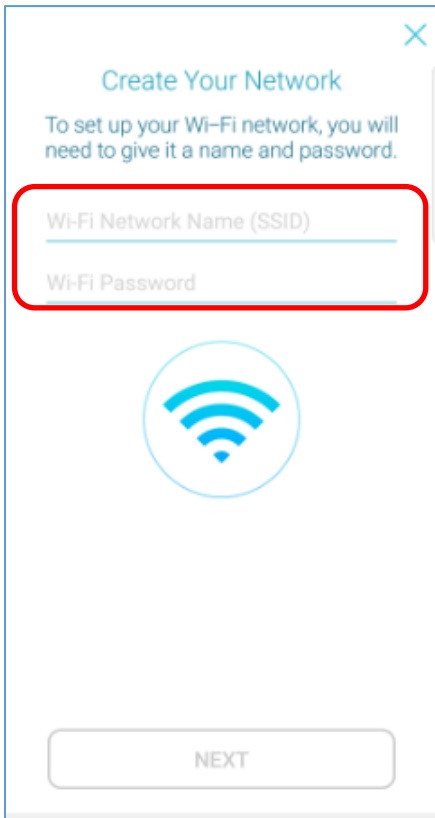
To set up this Internet connection, enter your PPPoE user name and password provided by your Internet service provider.

User Name

Password

NEXT

Step 9: Enter a Wi-Fi name (SSID) and password for your Covr Wi-Fi network, then tap **NEXT**:



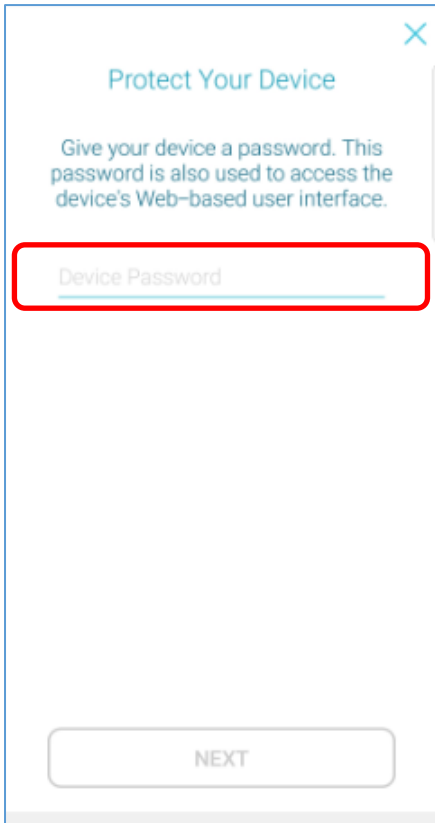
The screenshot shows a mobile application window titled "Create Your Network" with a close button (X) in the top right corner. Below the title is the instruction: "To set up your Wi-Fi network, you will need to give it a name and password." There are two input fields: "Wi-Fi Network Name (SSID)" and "Wi-Fi Password". Both fields are currently empty. A red rectangular box highlights both input fields. Below the fields is a large blue Wi-Fi signal icon. At the bottom of the screen is a "NEXT" button.

Note: Password length must be at least 8 characters long. If less than 8, the message will pop up to inform you to revise your password setting till you get a valid one:



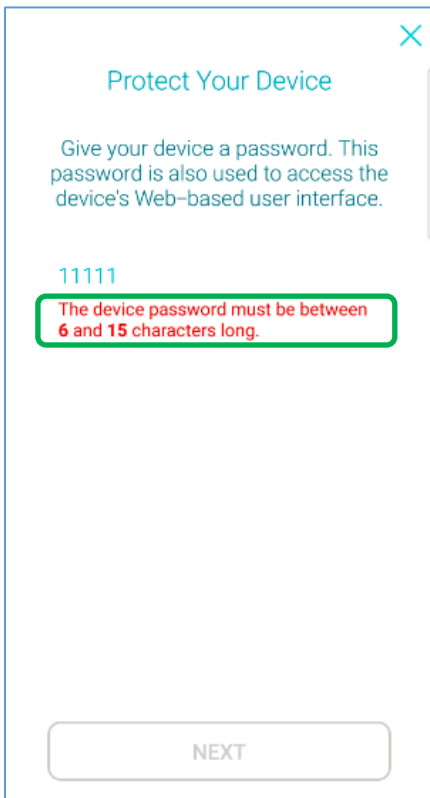
The screenshot shows the same "Create Your Network" screen. The "Wi-Fi Network Name (SSID)" field now contains the text "COVR-2202" and has a green checkmark on the right side. The "Wi-Fi Password" field contains the text "12". A red error message box is overlaid on the password field, containing the text: "The password must be at least 8 characters long." The Wi-Fi icon and "NEXT" button are also visible.

Step 10: Enter a 6-15 characters long device password. This password will be used to access the web UI and the Wi-Fi app for both the COVR router and COVR Point. Tap **NEXT** to continue:



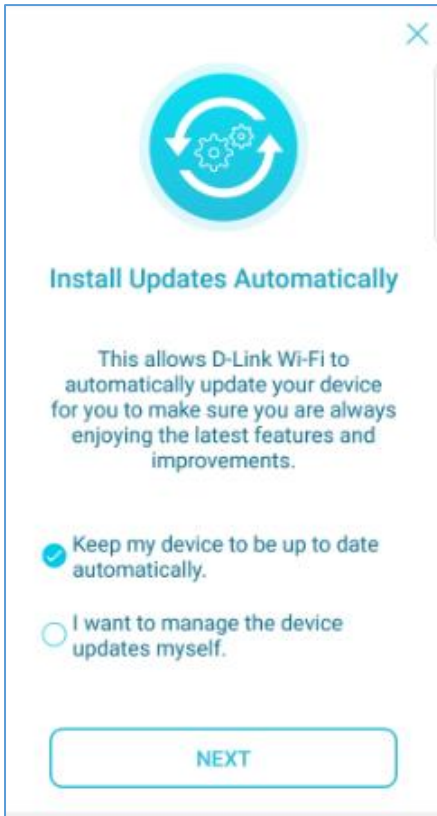
The screenshot shows a mobile application window titled "Protect Your Device" with a close button (X) in the top right corner. Below the title is the instruction: "Give your device a password. This password is also used to access the device's Web-based user interface." A text input field labeled "Device Password" is highlighted with a red border. At the bottom of the screen is a "NEXT" button.

Note: If password is less than 6, the message will pop up to inform you to revise your password setting till you get a valid one:

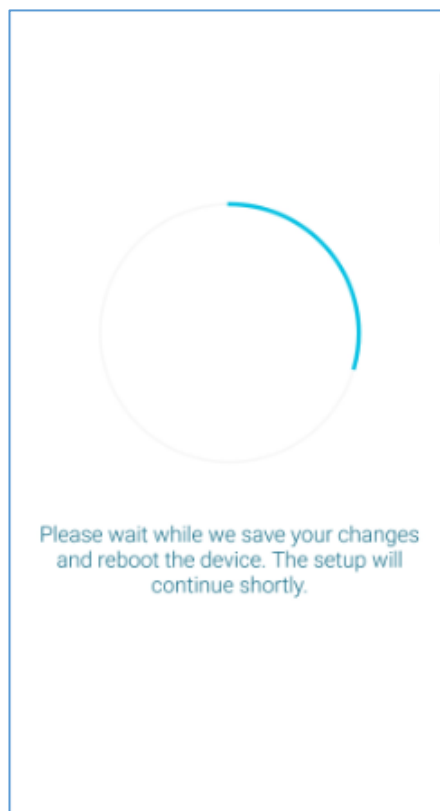
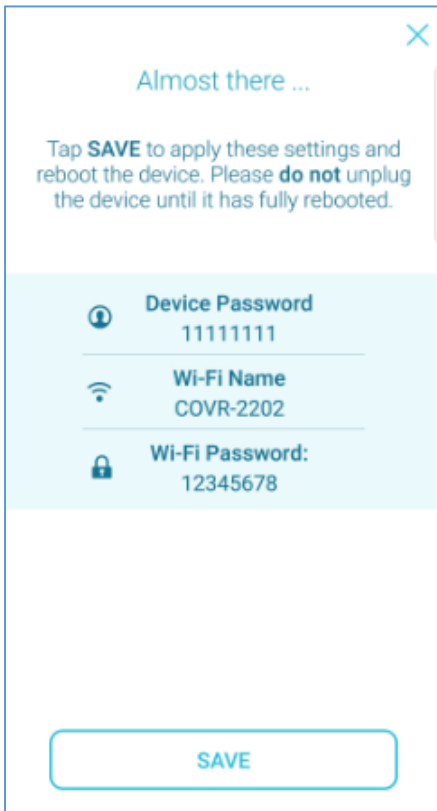


The screenshot shows the same "Protect Your Device" screen. The password input field now contains "11111" and is highlighted with a green border. Below the input field, a red error message is displayed: "The device password must be between 6 and 15 characters long." The "NEXT" button remains at the bottom.

Step 11: You'll be asked if you would like to allow D-Link Wi-Fi to automatically download and install updates. Select the item which fits your need:



Step 12: A summary page will display your settings. Tap **SAVE** to save your settings:



Step 13: Register your mydlink account to enable 3rd party services, including D-Link defend, Amazon Alexa and The Google Assistant.

Cloud Service

By registering your device with a D-Link account, you will be able to use the 3rd party services below to control and manage your device.

- D-Link defend**
Control who can access your Wi-Fi and protect your kids when they go online.
- Amazon Alexa**
Control your device with your Amazon Echo through the D-Link Cloud Service.
- The Google Assistant**
Control your device with the Google Assistant through the D-Link Cloud Service.

Register

Sign Up

A D-Link account allows you to enjoy a range of D-Link services with one convenient login.

Continue with Facebook

Sign in with Google

or

Sign up with Email

By continuing, you agree to D-Link's [Terms of Use](#) and [Privacy Policy](#). We may use your email for updates on D-Link's products and services. You can unsubscribe the newsletter at any time on the side menu.

Already have an account? **Log In**

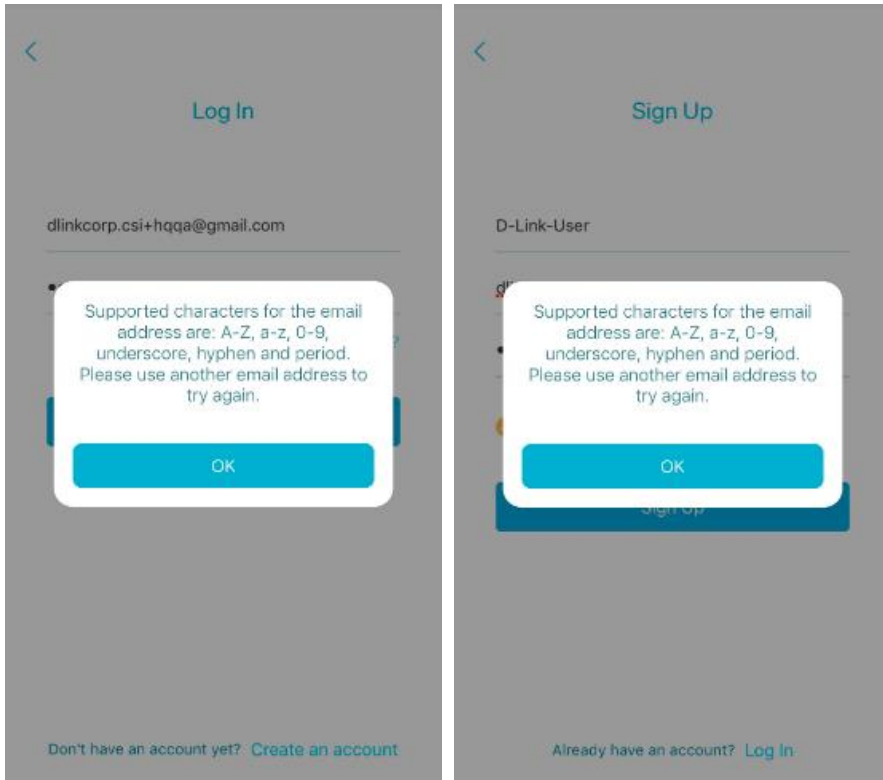
If you don't have a D-Link account, please sign up for one.

If you already have D-Link account, please log in.






Note: There are some characters which are not allowed to be applied in your account. See the chart below.

Special Characters			
@@	..	;	?
:\\	//	((\$
))	xp_	<	
>	%	=	[
--	::	=/]
0x	*	+	(
)			

The supported characters for the email address are A-Z, a-z, 0-9, underscore, hyphen and period. Make sure that you use the characters in your account.




Step 14: Enable D-Link defend service.

Cloud Service	D-Link defend	D-Link defend
D-Link Account Registered >	 Powered by McAfee We want to keep protecting your home and family.	 Powered by McAfee We want to keep protecting your home and family.
Parental Control  D-Link defend >	<ul style="list-style-type: none">Secure connected and smart home devicesControl who can access your Wi-FiHelp your kids stay safe onlineProtect devices from viruses <p><input type="checkbox"/> I understand and agree with the Terms of Service and Privacy Notice. I am also aware that D-Link will share my email address and device information with McAfee.</p> <p>KEEP PROTECTING ME</p>	<ul style="list-style-type: none">Secure connected and smart home devicesControl who can access your Wi-FiHelp your kids stay safe onlineProtect devices from viruses <p>Disable Service</p>
3rd Party Service  Amazon Alexa >  The Google Assistant >		

Step 15: Place the remaining Covr Point(s) to the area where you would like to extend your whole home Wi-Fi to:

Place your Covr Point(s)




Place the remaining **Covr Point(s)** where you think you'll need Wi-Fi the most.

NEXT


Step 16: Power on the remaining Covr Point(s), and wait until the COVR LED starts blinking orange then tap **NEXT** to start syncing up:

Power On the Covr Point(s)



Power on the remaining Covr Points. Wait until the COVR LED starts **blinking orange**, then tap **NEXT**.

NEXT



Syncing up the Covr Points. This might take a few minutes ...

Step 17: After the LED becomes **solid white**, it's ready to use:

Success!

The COVR LED should now light up **solid white**. Your Covr whole home Wi-Fi system is now successfully formed and ready to use.



If the LED does not turn solid white, [tap here](#) for more information.

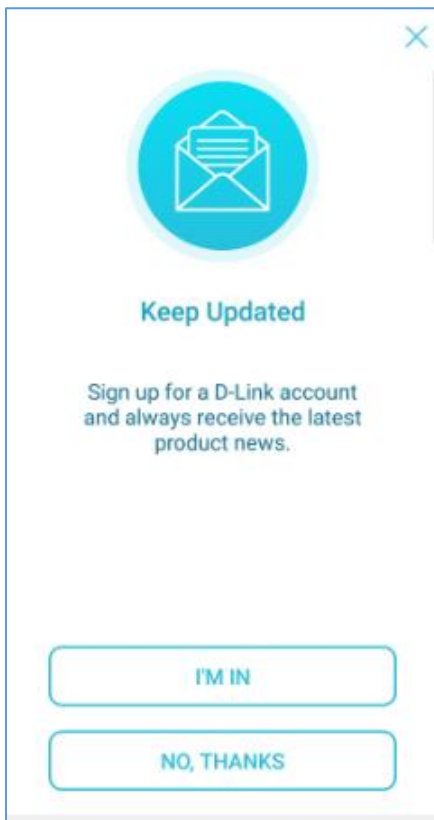
NEXT

Note: Check the LED indicator on your Covr Point(s) to ensure a good connection.

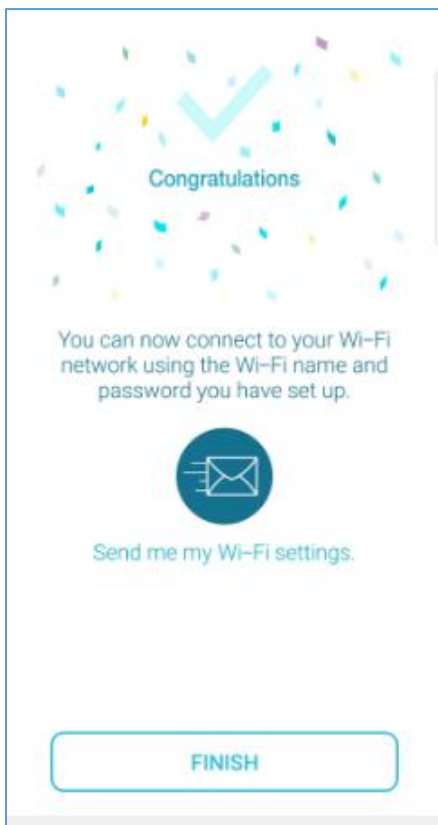
- **Solid white:** Strong signal.
- **Blinking white:** Weak signal. Move your Covr Point(s) closer to the Covr Point A until the LED turns solid white.
- **Blinking orange:** Covr Point(s) can't receive signal. Move your Covr Point(s) closer to the Covr Point A until the LED turns solid white.

*Please check [Q14](#) for detailed description of LED behavior.

Step 18: You'll be asked if you'd like to obtain the latest D-Link product news via registering D-Link account. Select the option which fits your need (Selecting "I'M IN" is highly recommended):

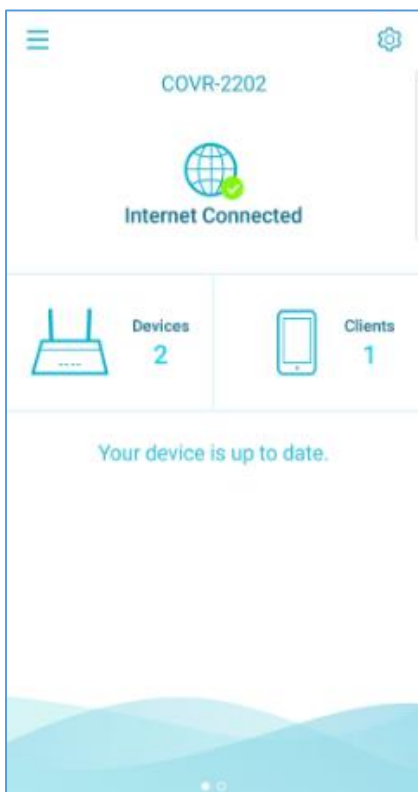


Step 19: Your setup is completed. Tap **FINISH** to finish the process:



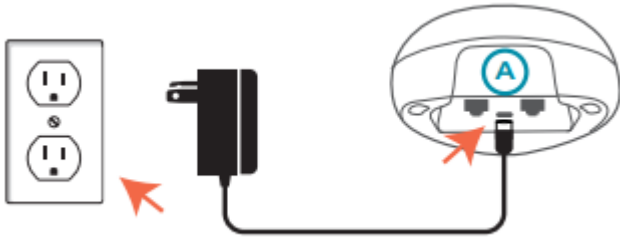
Note: If using iOS mobile device, there will be "<" sign in each step on top-left side which can let you go back to the previous step.

Step 20: Then the information of **Devices** and **Clients** will be shown:



Method 2: Using the web UI

Step 1: Connect the power adapter and plug in the Covr Point labeled **A** (Covr Router):



Step 2: Wait for the device to boot up. When the Covr LED starts blinking orange, connect your PC or laptop to the Wi-Fi name (SSID) printed on the back of the device, or on the included Wi-Fi Configuration Card:




Step 3: Type [http://covr.local./](http://covr.local/) into a web browser and follow the on-screen instructions to complete the setup:



Step 4: The first time you log in, the wizard will automatically start. Power up the COVR Router, place the remaining Covr Point(s) to the area where you would like to extend your whole home Wi-Fi to, then power it up. Click **Next** to continue:

Welcome ✕



Internet COVR router COVR point Wi-Fi Client

This wizard will guide you through a step-by-step process to configure your COVR Wi-Fi system.

Step 1: Install your device

Step 2: Configure your Network and Wi-Fi settings

Step 3: Set your router password

Step 4: Relocate COVR Point(s)

Language: ▾ Next

Step 5: Plug one end of Ethernet cable into **port 1** on the COVR router (Covr Point A), and plug the other end of the Ethernet cable into your modem or gateway. Click **Next** to continue:

Install

Please plug one end of the Ethernet cable included with your device into the port labeled INTERNET on your device. Plug the other end of this cable into the Ethernet port on your DSL or cable broadband modem, and power cycle the modem.

[Retry](#) [Next](#)

Step 6: Select your connection type:

Configure Your Internet Connection

Please select your Internet connection type below:

- DHCP Connection (Dynamic IP Address)**
Choose this option if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.
- Username/Password Connection (PPPoE)**
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this connection type of connection.
- Static IP Address Connection**
Choose this option if your Internet Service Provider provided you with IP Address information that has to be manually configured.

[Back](#) [Next](#)

Step 7: If you are using PPPoE (connecting behind modem), enter your PPPoE user name and password. Click **Next** to continue.

PPPoE

Internet COVR router COVR point Wi-Fi Client

To setup this Internet connection, you will need to have a User Name from your Internet Service Provider. If you do not have this information, please contact your ISP.

Username:

Password:

Back Next

Step 8: Enter a Wi-Fi network name (SSID) and a Wi-Fi password. This name and password will be assigned to both the 2.4GHz and 5GHz bands on all Covr Points. Click **Next** to continue.

Wi-Fi Settings

Internet COVR router COVR point Wi-Fi Client

To setup a Wi-Fi network you will need to give your Wi-Fi network a name(SSID) and password.


COVR Wi-Fi Network Name:

COVR Wi-Fi Password:

Back Next

Step 9: Enter an admin password for your COVR devices. This password will be used to access the web UI and the D-Link Wi-Fi app. Write it down and then click **Next** to continue.

Device Admin Password ✕




Internet COVR router COVR point Wi-Fi Client

By default, your new D-Link device does not have a password configured for administrator access to the Web-based configuration utility. To secure your new device, please create a password below.

Device Admin Password:

Step 10: You'll be asked if you would like to allow D-Link to automatically download and install updates. Select the item which fits your need:

Install Updates Automatically ✕




Always Update provides latest protection and new feature over the air, gives your device fresh and sound firmware.

Keep my device to be up to date automatically.
 I want to manage the device updates myself.

Step 11: A summary page will display your settings. You can also select if you'd like to have automatic firmware upgrade. If you want to make changes, click **Back**, otherwise, click **Next** to continue.

Summary ✕



Internet COVR router COVR point Wi-Fi Client

Below is a summary of your Wi-Fi security and device password settings. Please make a note of your settings and click "Next".

Connection Type:	PPPoE
COVR Wi-Fi Network Name:	COVR-2202
COVR Wi-Fi Password:	12345678
Device Admin Password:	11111111

[Back](#) [Next](#)

Step 12: Click **Finish** to save your settings.

Now you can plug in the remaining COVR Point(s) and place them anywhere within the coverage you want to extend your whole home Wi-Fi to.

The remaining Covr Points will automatically synchronize with COVR Point A and obtain its configuration settings.

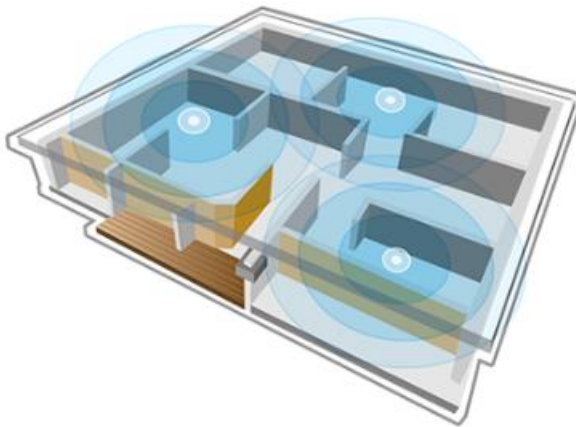
Check the LED indicator on your Covr Points to ensure a good connection.

- **Solid white:** Strong signal.
- **Blinking white:** Weak signal. Move your Covr Point(s) closer to the Covr Point A until the LED turns solid white.
- **Blinking Orange:** Covr Point(s) can't receive signal. Move your Covr Point(s) closer to the Covr Point A until the LED turns solid white.

COVR Point(s) Placement



You may now plug the COVR Point(s) and place it in a location between your COVR Router and the Wi-Fi weak area or deadzone. Once placed, verify that the COVR LEDs are solid white. If the COVR LEDs are not solid white, move the COVR Point(s) closer to the COVR Router until they are.



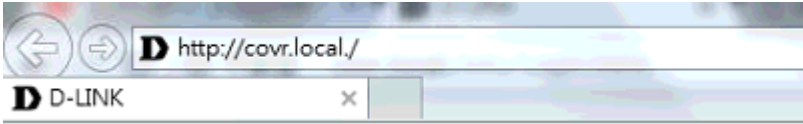
NOTE: Do not place the COVR Extender in a Wi-Fi weak spot or deadzone. The COVR Extender needs a strong signal from the COVR Router to work properly.

Finish

1-2: How do I log in to my Covr Router?

Verify that your computer or laptop is connected to the Covr router either via an Ethernet cable or wirelessly, then follow the steps below:

Step 1: Open your web browser and enter the address of the router into the address bar. The default URL is "**http://covr.local/**"



Step 2: Log into web user interface using your login and password. By default, the username is admin and no password.

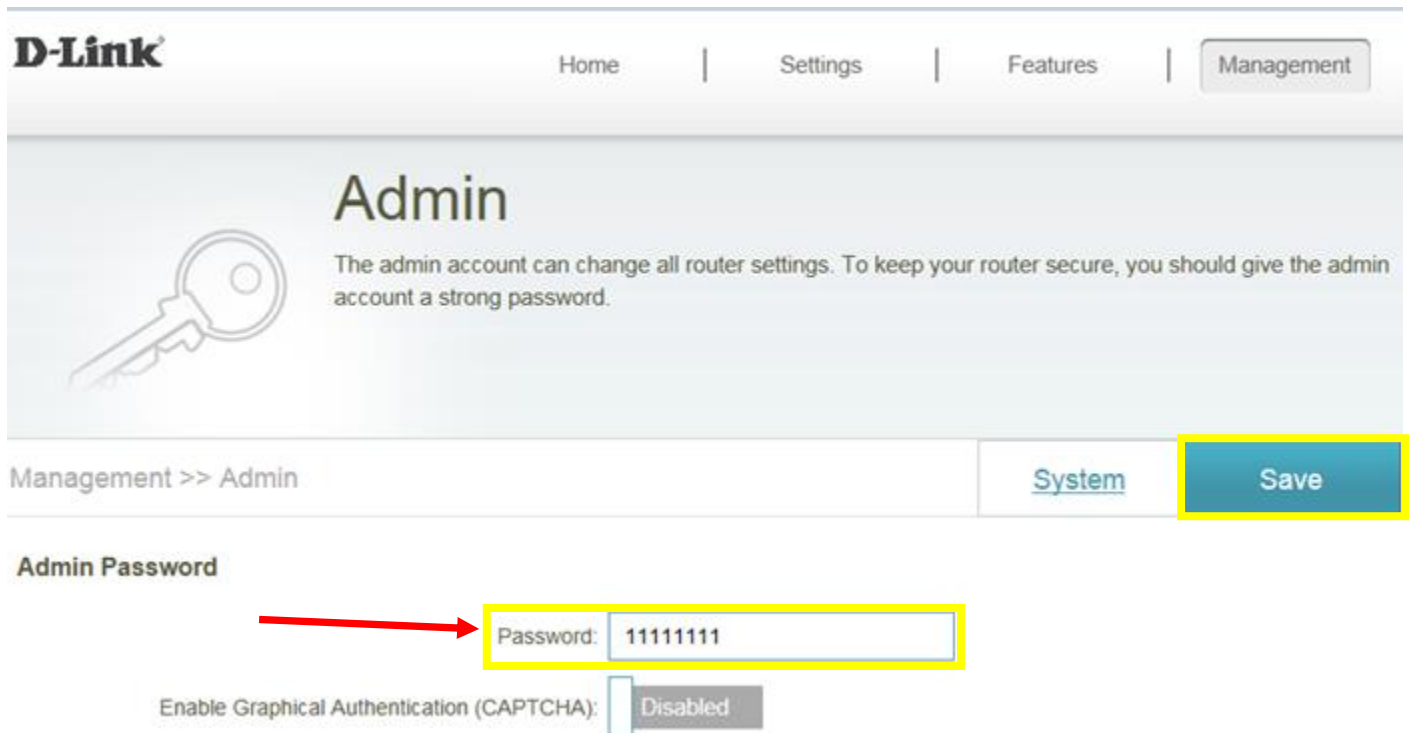
Note: If this is the first time setting up the COVR-2202 system, you can only set up the system wirelessly. Setting up first time using Ethernet is not supported.

1-3: How do I change the admin password on my router?

Please launch your browser and enter [http://covr.local./](http://covr.local/) into the address bar. Then login and follow the steps below:

Step 1: Click **Management** -> **System Admin**

Step 2: Enter a new admin password and click **Save**. Next time you want to access the web user interface, use your new password to log in:



The screenshot shows the D-Link router's web interface. At the top left is the D-Link logo. To the right are navigation links: Home, Settings, Features, and Management (highlighted with a grey background). Below the navigation is a large section titled "Admin" with a key icon and the text: "The admin account can change all router settings. To keep your router secure, you should give the admin account a strong password." Below this is a breadcrumb trail: "Management >> Admin". To the right of the breadcrumb are two buttons: "System" and "Save" (highlighted with a yellow border). Below the breadcrumb is the "Admin Password" section. It contains a "Password:" label and a text input field containing "11111111", which is highlighted with a yellow border. A red arrow points to this input field. Below the password field is a checkbox labeled "Enable Graphical Authentication (CAPTCHA):" which is currently "Disabled".

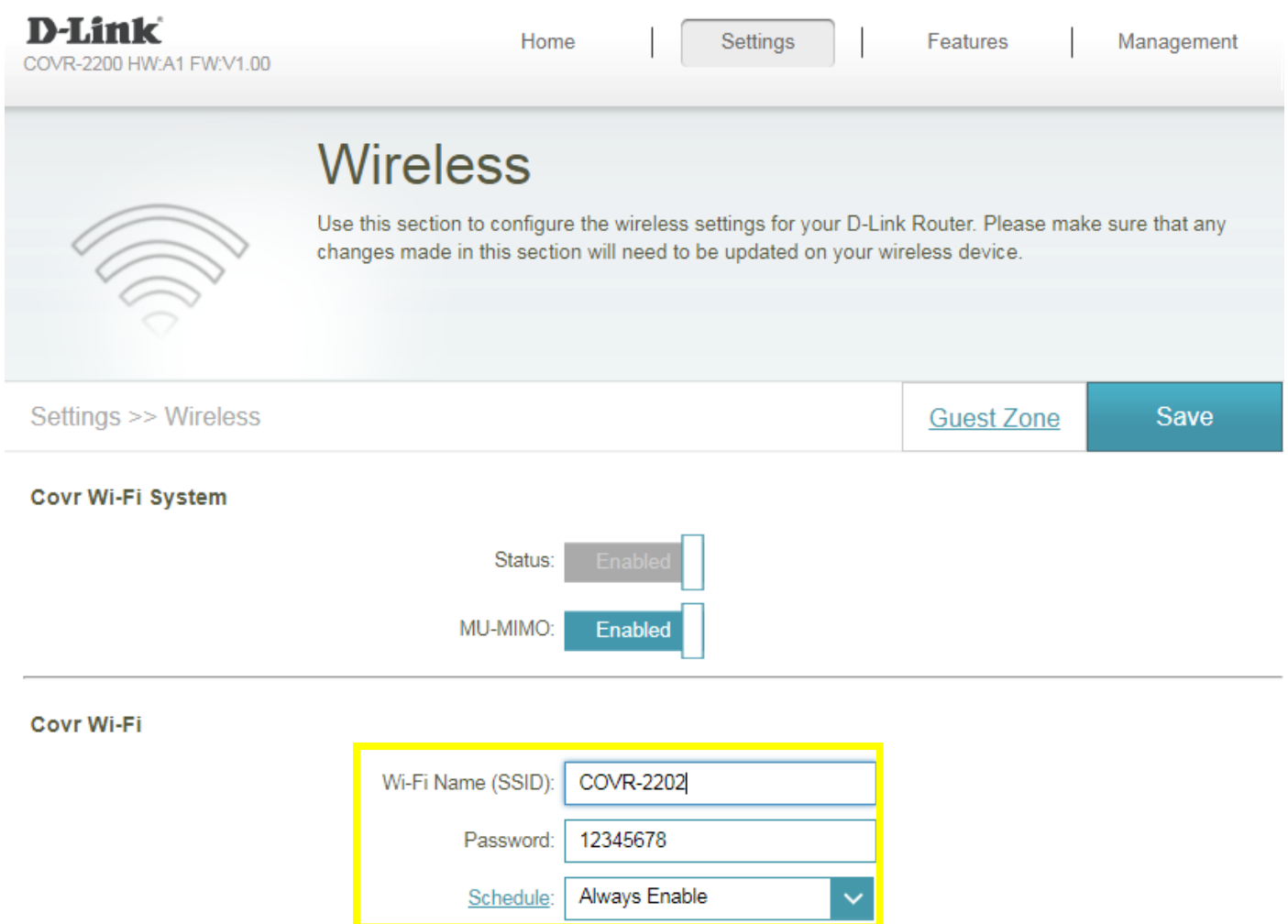
1-4: How do I change the wireless settings?

Please launch your browser and enter [http://covr.local./](http://covr.local/) into the address bar. Then login and follow the steps below:

Step 1: Click **Settings** -> **Wireless**

Step 2: In the **Wi-Fi name (SSID)** field, enter a unique wireless network name. (This is the name you will see when scanning for wireless networks on your computer/wireless device).

In the password field, enter a new password of at least 8 characters long. Click **Save** when you're done. You will need to connect to your new Wi-Fi network using your new password.



D-Link
COVR-2200 HW:A1 FW:V1.00

Home | Settings | Features | Management

Wireless

Use this section to configure the wireless settings for your D-Link Router. Please make sure that any changes made in this section will need to be updated on your wireless device.

Settings >> Wireless [Guest Zone](#) [Save](#)

Covr Wi-Fi System

Status:

MU-MIMO:

Covr Wi-Fi

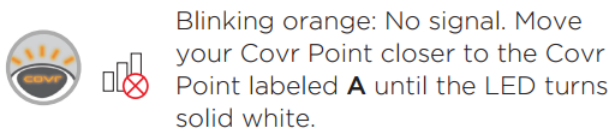
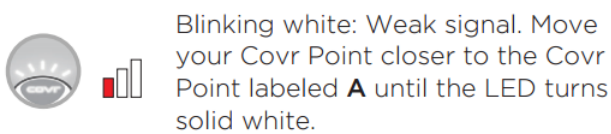
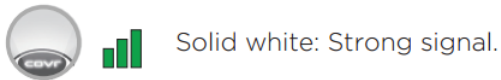
Wi-Fi Name (SSID):

Password:

Schedule:

1-5: Why does my Covr Point keep losing connection?

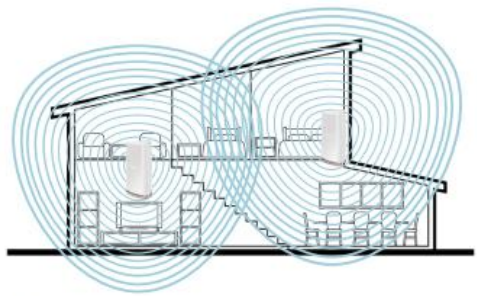
1. Ensure the Covr Point is in a well-ventilated and open area. Do not put the Covr Points in a cabinet or enclosed area.
2. Check and change the location of your Covr Points – Even a subtle change (2-3 feet) can make a big difference.
 - Make sure that you place your Covr Points in an area with a strong uplink connection. Check the LED indicator on your Covr Points to ensure a good connection.



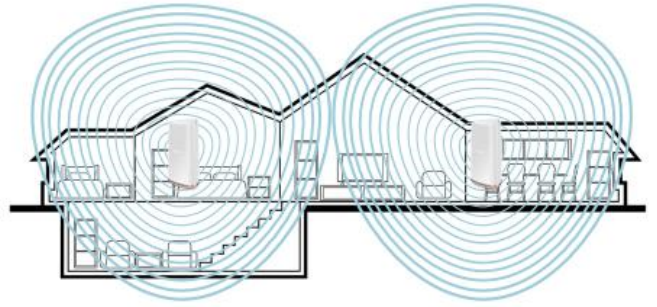
3. Other devices that use 2.4GHz/5GHz wireless band may interfere with your wireless network, including microwaves, wireless cameras, baby monitors...etc. To prevent signal interference, place your Covr Points away from such devices.
4. **Ensure that your router is running the latest firmware version.** Please follow this link for instructions on how to upgrade the firmware- [How to upgrade firmware for router?](#)

Note: COVR-2202 is flexible enough to cover almost every housing type, from 1-story apartment to entire mansions, and basements to back decks. Here are examples you could put your COVR Points:





CONTEMPORARY



BUNGALOW

1-6: Which Ethernet port can be used as WAN port?

The device will automatically configure port 1 or 2 as the WAN port.

Once configured, you cannot change the WAN port. To change configuration, you need to reset your Covr Router to factory default settings and reinstall the device using the other port.



1-7: How many Covr Points will work on my Covr-2202 Wi-Fi system?

The maximum quantity is 4 COVR-Points including 1 COVR-Point A.

The combination:

(1) COVR-2202 + 2 * COVR-2200

(2) 4 * COVR-2200

1-8: How large is the coverage range of COVR-2202?

Please see the chart below:

Part Number	Description	Range
COVR-2200	Tri-band Whole Home Wi-Fi System(Single pack)	325 square meters/3500 square feet
COVR-2202	Tri-Band Whole Home Wi-Fi System(Two Pack)	550 square meters/6000 square feet

1-9: If I don't have ISP service at home, can I still create a LAN environment using COVR-2202?

No, you need to have an active subscription with an Internet Service Provider (ISP) in order to set up the COVR-2202 Whole Home Wi-Fi System.

1-10: Does COVR-2202 support Alexa/Google Assistant?

Yes, COVR-2202 supports Amazon Alexa & Google Assistant for below functions:

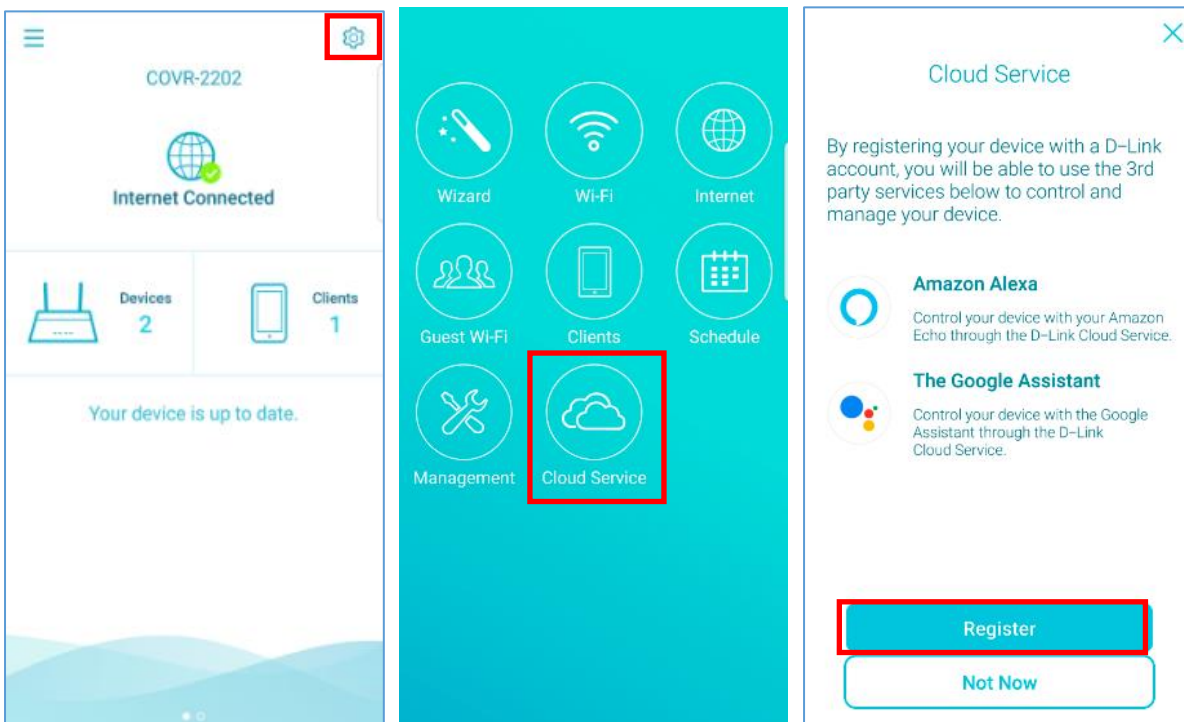
- **Enable/disable Guest Wi-Fi**
- **Find out Guest Wi-Fi credentials**
- **Reboot router**
- **Firmware upgrade**

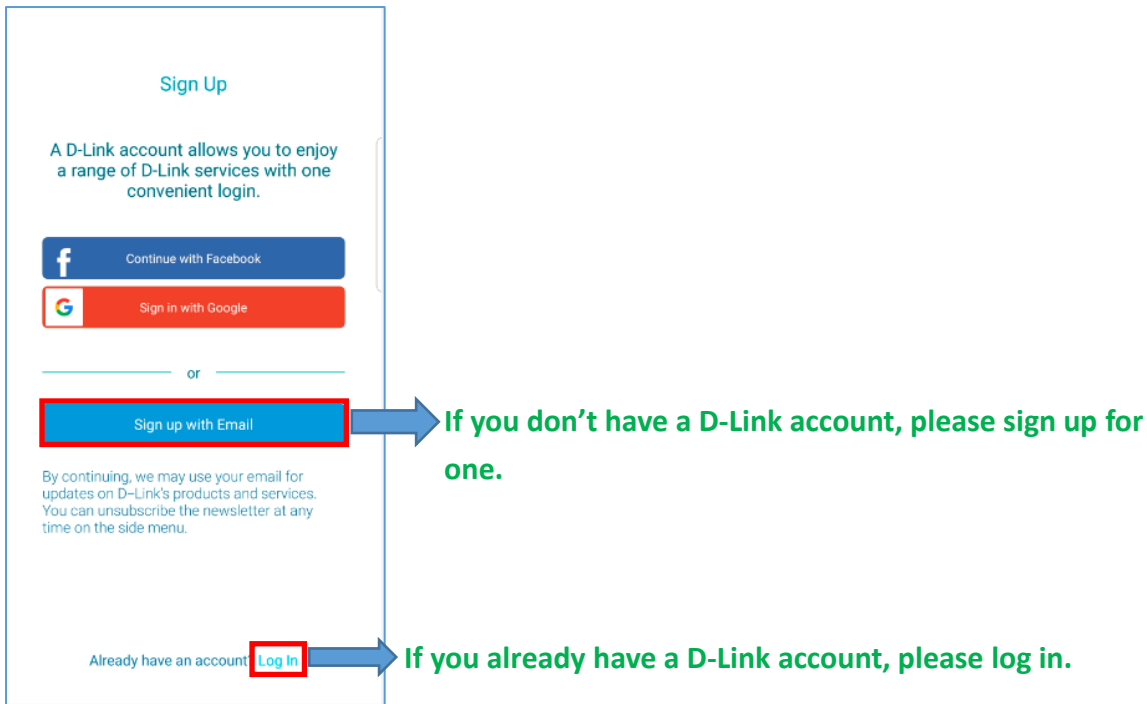
Note: The firmware version must be 1.01 or above.

Google Assistant

Note: You can apply Google Assistant app to carry out the voice control if you don't own Google Assistant device.

Step 1: Register a D-Link account to your COVR-2202 via D-Link Wi-Fi app:



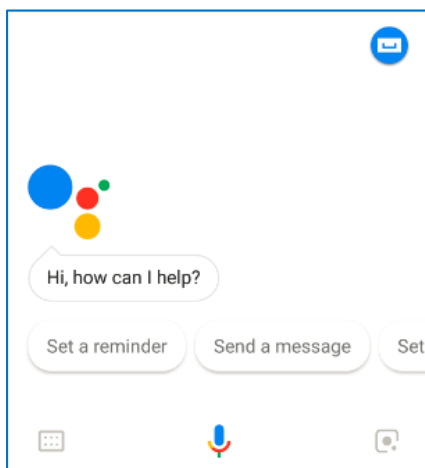


Step 2:

- (1) For Android devices, login **Google app** as your own Google account.
- (2) For iOS devices, please download **Google Assistant app** from App Store, and then login your own Google account.
- (3) If using Google Assistant device, see (3) in Step 3.

Step 3:

- (1) For Android devices, press Home key for 2 seconds to launch Google Assistant, and speak **"talk to D-Link Wi-Fi"** to Google Assistant:



- (2) For iOS devices, please launch **"Google Assistant"**, and speak **"talk to D-Link Wi-Fi"** to Google Assistant app.
- (3) If you use Google Assistant devices, directly speak **"talk to D-Link Wi-Fi"** to start voice control.

Step 4: Follow the command table as below:

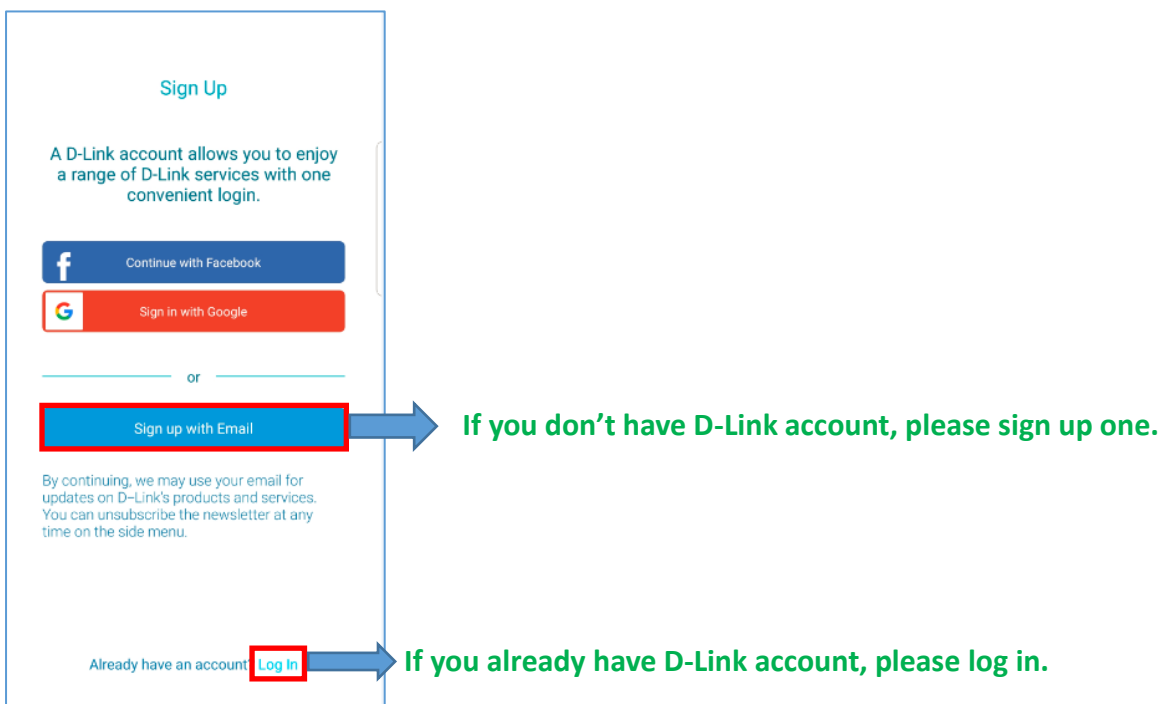
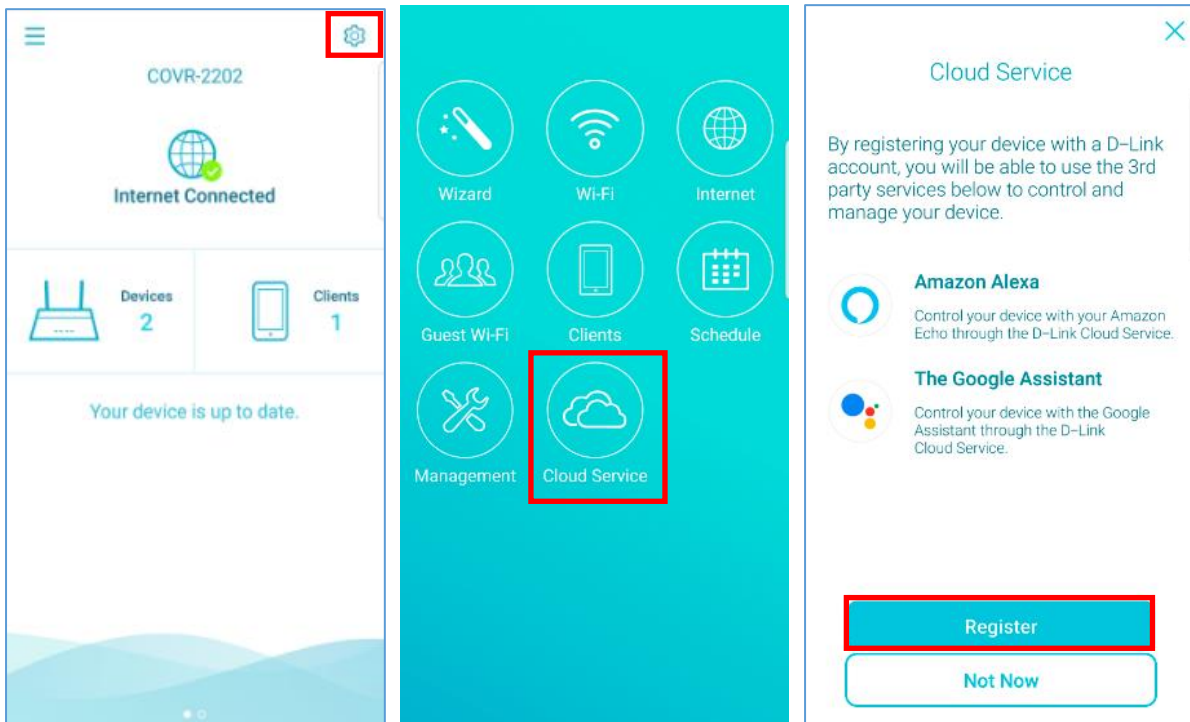
Control	First Command	Second Commands	Supported Google Assistant Devices			
			Google Home Mini	Google Home	Google Home Max	Others
Help	Talk to D-Link Wi-Fi	Help	V	V	V	V
Reboot		Reboot my router	V	V	V	V
Upgrade firmware		Upgrade my router	V	V	V	V
Check Guest Wi-Fi SSID/Password		What are my guest network credentials?	V	V	V	V
Guest Wi-Fi		Enable my guest zone	V	V	V	V
		Disable my guest zone	V	V	V	V

Note: When a round of conversation ends, speak "talk to D-Link Wi-Fi" again to Google Assistant to activate a new round of conversation.

Amazon Alexa

Note: You can apply Amazon Alexa app to carry out the voice control if you don't own Amazon Alexa device.

Step 1: Register D-Link account to your COVR-2202 via D-Link Wi-Fi app:



Step 2: So far, Amazon Alexa supports English only. Make sure that the language of your mobile device is set as English.

Step 3: Download **Amazon Alexa** app from App Store/Google Play, then login with your Amazon account.

Note: You must have US App Store/Google Play account because Amazon Alexa is available for US only.

Step 4: Open Alexa app, then follow the instruction below:

- Go to the menu from top-left side, and select "**Skills**".
- Search for **D-Link Wi-Fi** and tap it to open the Skill details page.
- Tap the **Enable Skill** button.
- Log in with your D-Link Wi-Fi account and tap **Authorize** to link your account to Alexa.

You can now control your router with Amazon Alexa app or any Amazon Alexa Echo device.

Step 5: Start to control your router via talking to Amazon Alexa app or Amazon Alexa Echo device followed by the command chart below:

Control	First Commands	Second Commands	Alexa devices			
			Echo Dot	Echo with improved sound	Echo Show	Echo Spot
Help	Open to D-Link Wi-Fi	Help	V	V	V	V
Reboot		Reboot my router	V	V	V	V
Upgrade firmware		Upgrade my router	V	V	V	V
Check Guest Wi-Fi SSID/Password		What are my guest network credentials?	V	V	V	V
Guest Wi-Fi		Enable my guest zone	V	V	V	V
		Disable my guest zone	V	V	V	V

Note: When a round of conversation ends, D-Link Wi-Fi will leave the conversation. If you'd like to use Amazon Alexa app or Amazon Alexa Echo device to control D-Link Wi-Fi again, please speak "**Open D-Link Wi-Fi**" again to Amazon Alexa app or Amazon Alexa Echo device to activate a new round of conversation.

1-11: Does COVR-2200 support VLAN feature?

No, currently COVR-C2202 does not support VLAN functionality.

1-12: Can I adjust the 2.4GHz or 5GHz wireless bands for COVR-2202?

No, the 2.4 GHz and 5 GHz wireless bands cannot be configured separately. Instead, COVR-2202 features a single network with a single Wi-Fi network name (SSID) which uses intelligent band steering to automatically place your devices on the optimal wireless band, either 2.4 GHz or 5 GHz.

1-13: Can I turn off the LED (for both COVR router and COVR point(s)) for COVR-2202?

You can turn off the LED (for both COVR router and COVR point(s)):

Please launch your browser and enter [http://covr.local./](http://covr.local/) into the address bar. Then log in and follow the steps below:

Step 1: Click **Management** -> **System Admin**

Step 2: Toggle **Status LED** to **Disabled**, then click **Save**. A 25 seconds countdown timer will pop up. This will turn off the LED on all Covr Points. Toggle the **Status LED** to **Enabled** to enable the LED:

Management >> Admin [System](#) **Save**

Admin Password

Password:

Enable Graphical Authentication (CAPTCHA): Disabled [Advanced Settings...](#)

LED Control

Status LED: Disabled



1-14: What does the LED behavior on my COVR-2202 system mean?

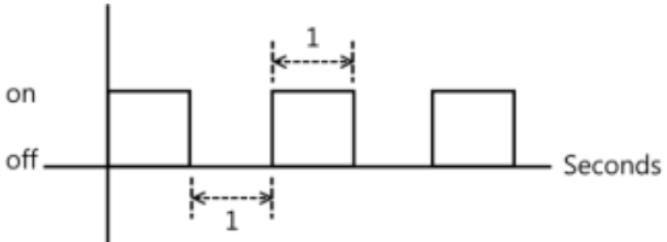
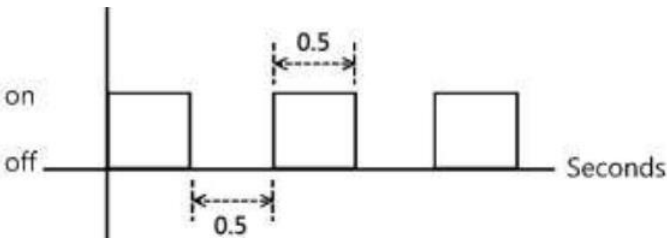
COVR Point A:

Status	Description
Solid Red	During power on process, OR device is malfunctioned.
Blinking Orange (Normal)	Cannot connect to internet.
Blinking Orange (Faster)	The device is upgrading firmware.
Blinking White (Normal)	The device is processing WPS.
Solid White	Internet is established, and IP is provisioned.
Light Off	The device is powered off.

Other COVR Points (Not A):

Status	Description
Solid Red	During power on process, OR device is malfunctioned.
Blinking Orange (Normal)	Cannot sync with COVR Point A. Please move the COVR Point closer to COVR Point A till you get solid white LED status.
Blinking Orange (Faster)	The device is upgrading firmware.
Blinking White (Normal)	The device is processing WPS.
Blinking White (Faster)	Connect to COVR Point A successfully, but signal is weak. Please move the COVR Point closer to COVR Point A till you get solid white LED status.
Solid White	Connect to COVR Point A successfully, and signal is solid.
Light Off	The device is powered off.

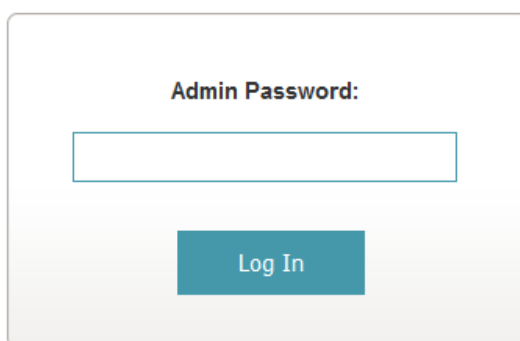
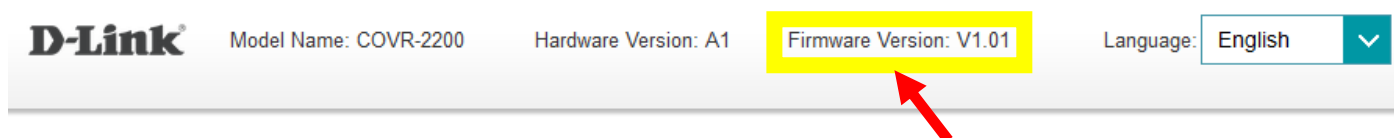
Blinking Speed Definition:

LED Blinking Speed	Description
Normal	<p>Blinking every 1 second.</p> 
Faster	<p>Blinking every 0.5 second.</p> 

Firmware Upgrade/Checking

2-1: How do I check the firmware version of my COVR-2202 system?

Method 1: Please launch your browser and enter `http://covr.local./` into the address bar. The firmware version can be found at the upper right of the page.



The image shows a login form titled 'Admin Password:'. It contains a text input field for the password and a blue 'Log In' button below it.

Note: This version only shows the firmware version of the Covr Router. The other Covr Points may be using a different firmware version. Refer to method 2 to verify the firmware version of each Covr Point.

Method 2: Click **Management** -> **Upgrade**. On this page you can see the firmware version for both the Covr Router and Covr Point(s):

Firmware Information

Master	COVR-2200	Firmware Version: V1.01
COVR Points	COVR-2200	Firmware Version: V1.01

Check for New Firmware

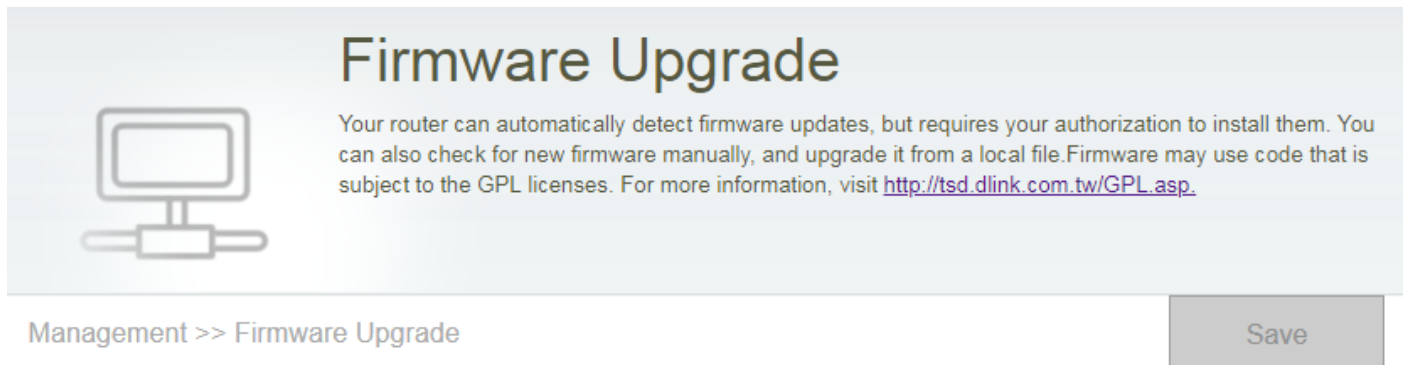
Note: If you need to upgrade the Covr Router or Covr Point(s) individually, please refer to the **Manual Upgrade** section in Q16.

2-2: How do I upgrade the firmware on my Covr-2202?

Please launch your browser and enter <http://covr.local/> into the address bar. Then login and follow the steps below:

Step 1: Click **Management** -> **Upgrade**

Step 2: The current firmware version of your device (including Master and COVR Points) will be displayed. Click **Check for New Firmware** to browse for the firmware:



The screenshot shows the 'Firmware Upgrade' page. On the left is an icon of a computer monitor. The main heading is 'Firmware Upgrade'. Below it is a paragraph of text explaining that the router can automatically detect updates but requires authorization, and that manual updates from local files are also possible. A link to the GPL license is provided. At the bottom left, the breadcrumb 'Management >> Firmware Upgrade' is visible. At the bottom right, there is a 'Save' button.

Firmware Information

Master	COVR-2200		Firmware Version: V1.00
COVR Points	COVR-2200		Firmware Version: V1.00

Check for New Firmware

[Advanced Settings...](#)

If there's new firmware available, system will pop out the notification. Click **Upgrade Firmware** to carry out the upgrade procedure:

Firmware Information

Master	COVR-2200		Firmware Version: V1.01
COVR Points	COVR-2200		Firmware Version: V1.00

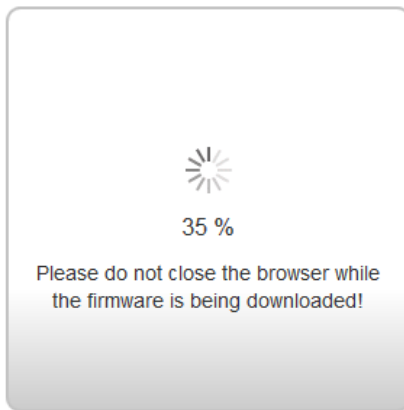
New Firmware Version: V1.01

New Firmware Version: V1.01

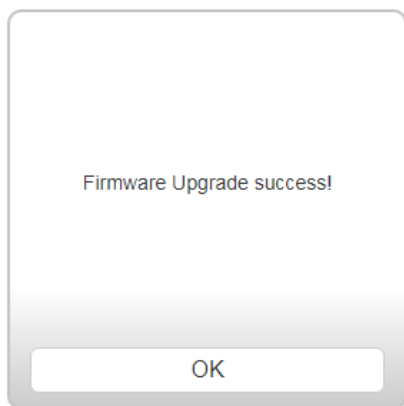
Upgrade Firmware

Step 3: If new firmware is detected, click **Upgrade Firmware** to begin the update process.

A message will appear informing you on the update progress (Do not power off or reboot any of your Covr units while upgrade is in progress):



If the firmware has successfully updated, the following message will appear:



Note:

1. The notification message will pop up if the firmware is the latest version:

Firmware Information

Master	COVR-2200		Firmware Version: V1.01	New Firmware Version: unknown
COVR Points	COVR-2200		Firmware Version: V1.01	New Firmware Version: unknown

This firmware is the latest version.

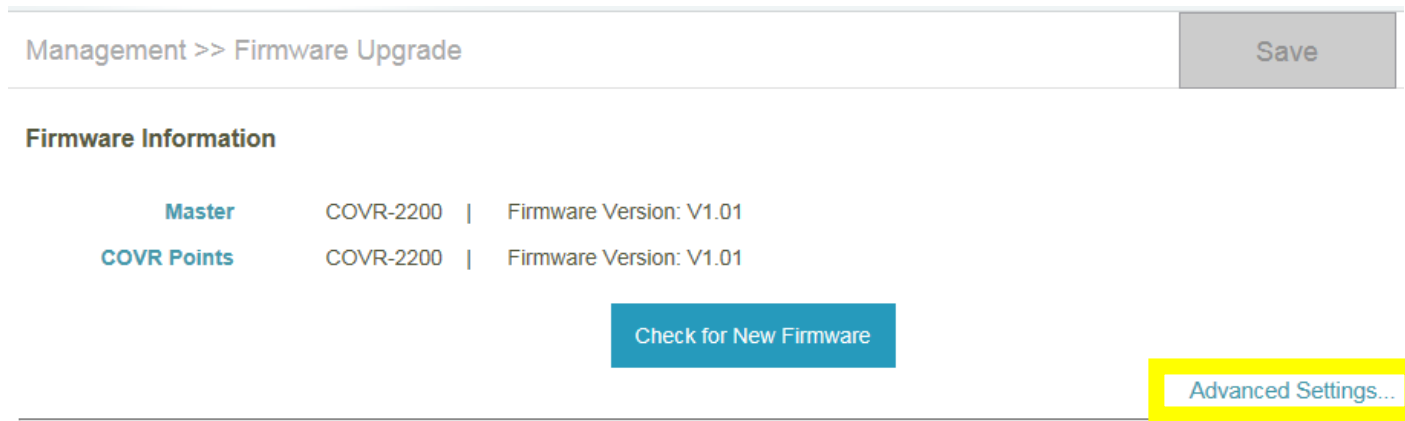
2. Manual Upgrade:

You can also manually upgrade the device firmware if you have downloaded the firmware file from the D-Link support website:

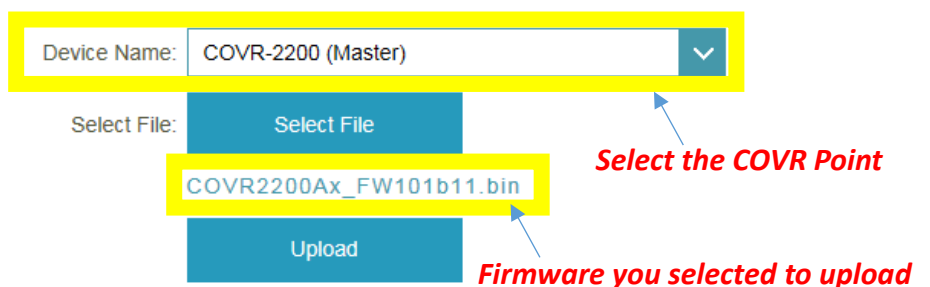
Step 1: On the firmware page, click **Advanced Settings**.

Step 2: From the **Device Name** drop-down menu, select the Covr Point you would like to upgrade firmware for.

Step 3: Click **Select File** and navigate to the firmware file you downloaded earlier, then click **Upload** to begin the upgrade process.



Upgrade Manually



3. Automatic Firmware Upgrade:

You can also configure auto upgrade firmware time to make your system automatically upgrade the latest firmware if any updated version is available. Device will be automatically upgraded every day at 3:30-4:00AM by default if you don't enable **Choose Upgrade Time** & select a specific time:

Management >> Firmware Upgrade Save

Firmware Information

Master	COVR-2200		Firmware Version: V1.01
COVR Points	COVR-2200		Firmware Version: V1.01

[Check for New Firmware](#)

[Advanced Settings...](#)

Automatic Firmware Upgrade

Automatic Upgrade: Enabled

Update my device automatically every day at 3:30-4:00 AM to always enjoy the latest improvements and features.

Choose Upgrade Time: Enabled

Upgrade Time: :

Configuration Backup/Factory Reset

3-1: How do I backup/restore the configuration settings of my Covr router?

Please launch your browser and enter <http://covr.local/> into the address bar. Then login and follow the steps below:

Step 1: Click **Management** -> **System Admin**

Step 2: Click **System**

Management >> Admin [System](#) Save

Admin Password

Password:

Enable Graphical Authentication (CAPTCHA):

[Advanced Settings...](#)

Step 3: Click **Save** to save a backup of your current configuration settings to your local hard drive:

Management >> System [Admin](#) Save

System

Save Settings To Local Hard Drive:

Load Settings From Local Hard Drive:

Restore To Factory Default Settings:

Step 4: To restore your configuration, click the **Select File** button and select your configuration backup file from your local hard drive. Once selected, click **Restore**.

Management >> System [Admin](#) Save

System

Save Settings To Local Hard Drive:

Load Settings From Local Hard Drive:

Restore To Factory Default Settings:

System

Save Settings To Local Hard Drive:

Save

[configuration file you selected](#)

Load Settings From Local Hard Drive:

Select File

config.bin

Restore

Restore To Factory Default Settings:

Restore



3-2: How do I reset my Covr router to factory default settings?

If you forgot your admin password or your device isn't working properly, you can perform a reset to return the device to its factory default settings.

Resetting your device will:

- (1) Erase all your current settings. This cannot be undone.
- (2) Reset the device admin password back to its default (blank).
- (3) Does NOT reset the firmware to the previous version.

Step 1: While the unit is powered on, use an unfolded paperclip to press the reset button at the bottom of the Covr Router (Covr Point A) until the LED on the front panel turns solid red, indicates that the unit is restarting.

Step 2: The unit will reboot automatically. Once the LED is blinking with orange, the unit has been reset and is ready to use.

Note: You only need to reset the Covr Router. The remaining Covr Point(s) will automatically synchronize and obtain their configuration settings from the Covr Router after finishing the setup process.

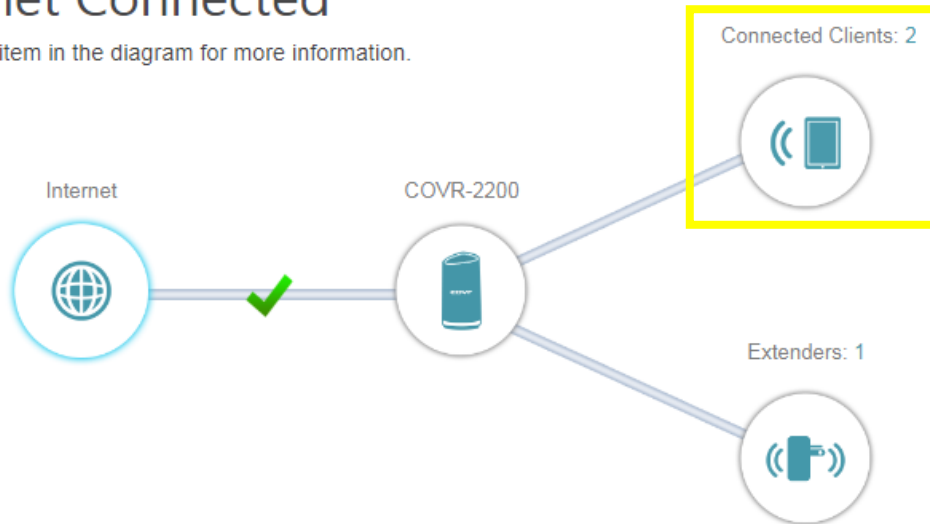
General Setting

4-1: How do I set up parental control features?

Step 1: From the home page, click the **Connected Clients** icon and select the device you'd like to set up parental controls for:

● Internet Connected

Click on any item in the diagram for more information.



Step 2: Click the pencil icon, then enable parental control & select the schedule to set the time frame of blocking the network access:

	android-58df89c3d9a	
	HTC	192.168.0.108
	Parental Control: Disabled	

Edit Rule



Name:

Vendor: HTC

MAC Address: 00:EE:BD:B9:A7:2A

IP Address: 192.168.0.108

Reserve IP: Remaining: 24

Parental Control:

Schedule: ^

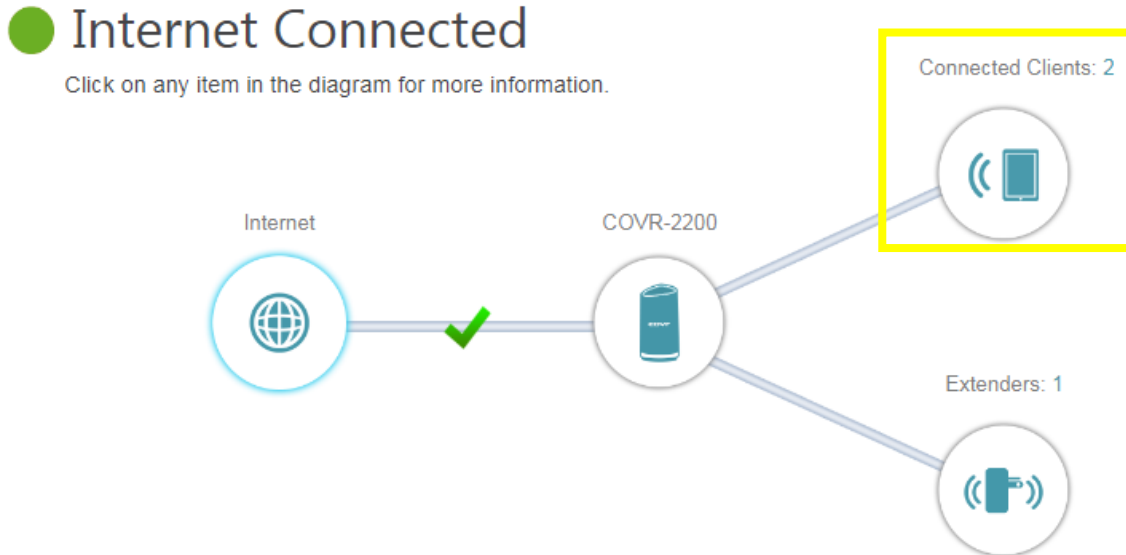
Always Enable
test

Note: For creating the schedule, please refer to [how to create schedule on my router?](#)

4-2: How do I configure DHCP IP reservation settings?

Please launch your browser and enter <http://covr.local/> into the address bar. Then login and follow the steps below:

Step 1: From the home page, click the **Connected Clients** icon:



Step 2: Click the **Pencil Icon** in the box of the client you want to change settings for:

	android-58df89c3d9a	
	HTC	192.168.0.108
	Parental Control: Disabled	

Step 3: Click **Reserve IP** to enable IP reservation. Enter the reserved IP address, then click **Save**. By doing this, the DHCP server will reserve the IP address you entered for this client device.

Edit Rule ✕

Name:

Vendor: HTC

MAC Address: 00:EE:BD:B9:A7:2A

IP Address: 192.168.0.108

Reserve IP: Remaining: 24

IP Address (Reserved):
It will take effect after reconnecting

Parental Control:

4-3: How do I change the router's IP address?

Please launch your browser and enter <http://covr.local/> into the address bar. Then login and follow the steps below:

Step 1: Click **Settings** -> **Network**

Step 2: In the **LAN IP Address** field, enter a new IP address and click **Save**.

Settings >> Network Save

Network

Use this section to configure the network settings for your device. You can enter a name for your device in the management link field, and use the link to access web UI in a web browser. We recommend you change the management link if there are more than one D-Link devices within the network.

Network Settings

LAN IP Address: 192.168.0.2

Subnet Mask: 255.255.255.0

Management Link: http:// covr .local/

Local Domain Name:

Enable DNS Relay: Enabled

[Advanced Settings...](#)

Note: If you have more than one D-Link devices within the network at home, we highly recommend you change the management link.

4-4: How do I enable remote management for my router?

Please launch your browser and enter `http://covr.local/` into the address bar. Then login and follow the steps below:

Step 1: Click **Management** -> **System Admin**

Step 2: Click **Advanced Settings**, and **enable Remote Management**, then click **Save**. The default remote management port: 8080.

Management >> Admin [System](#) **Save**

Admin Password

Password:

Enable Graphical Authentication (CAPTCHA): Disabled **Advanced Settings...**

Administration

Enable HTTPS Server: Enabled

Enable Remote Management: Enabled

Remote Admin Port:

Use HTTPS: Enabled

Note: To access your router remotely, from a web browser enter: <http://<your WAN IP>:8080>.

e.g. <http://220.137.8.23:8080>

You can find your WAN IP by clicking on the **Home** tab. It will be displayed under the Internet Section.

Internet

[IPv4](#) / [IPv6](#)

Cable Status: Connected
Connection Type: PPPoE
Network Status: Connected
Connection Uptime: 0 Day 16 Hour 35 Min 14 Sec

Disconnect

MAC Address: 18:0F:76:91:06:8A
IP Address: 220.137.14.149
Subnet Mask: 255.255.255.255
Default Gateway: 168.95.98.254
Primary DNS Server: 168.95.1.1
Secondary DNS Server: 168.95.192.1

Guest Zone Setting

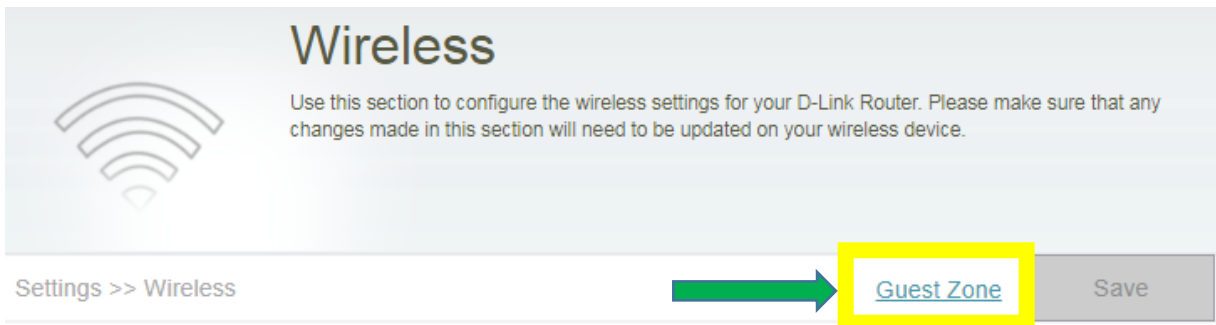
5-1: How do I enable Guest Zone/Guest Access on my Covr router?

The guest zone feature will allow you to create a temporary Wi-Fi zone separate from your main wireless network that can be used by guests to access the Internet.

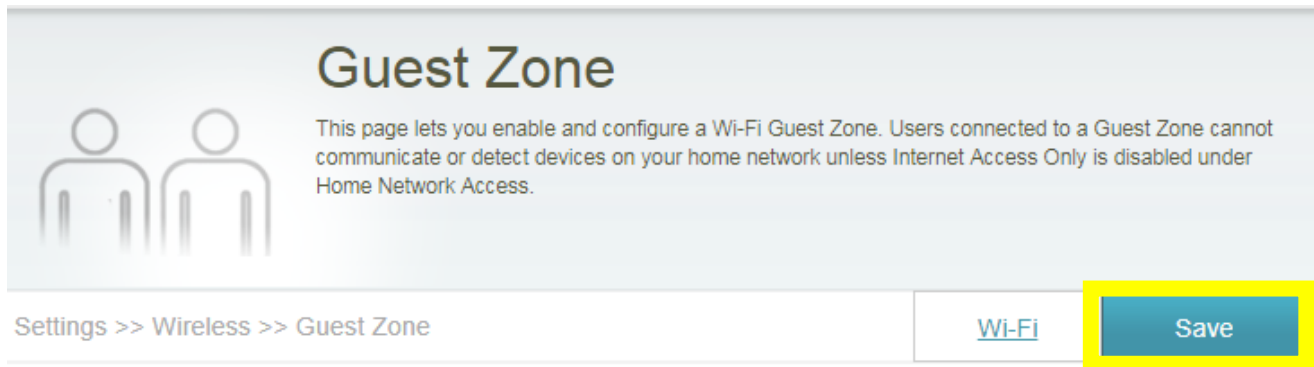
Please launch your browser and enter <http://covr.local/> into the address bar. Then login and follow the steps below:

Step 1: Click **Settings** -> **Wireless**

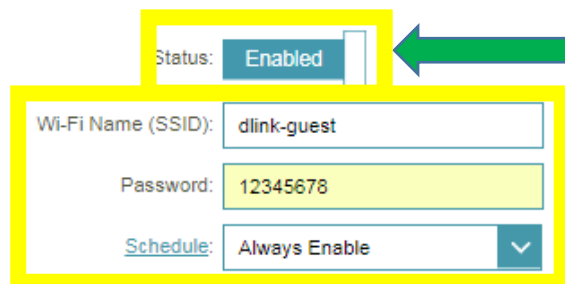
Step 2: Click the **Guest Zone** tab:



Step 3: Set **Status** to Enabled, and configure your Guest Zone Wi-Fi name (SSID) and password then click **Save**:



Covr Wi-Fi System



Note: Guest zone is disabled in default setting. Highly suggest to enable it for the concern of security.

Port Forwarding/Virtual Server Setting

6-1: How do I enable DMZ on my router?

DMZ should only be used if you have a computer/device that cannot run Internet applications properly from behind the router.

Note: By enabling the DMZ (Demilitarized Zone) feature, you are allowing the router to forward all incoming traffic from the internet to the device specified, virtually disabling the router's firewall protection. This may expose the device to a variety of security risks, so only use this option as a last resort.

Please launch your browser and enter `http://covr.local./` into the address bar. Then login and follow the steps below:

Step 1: Click **Features** -> **Firewall**

Step 2: Click **Enable DMZ** to use the DMZ feature, and fill in or select the IP address of the specified device from the drop-down menu, then click **Save**.

The screenshot shows the router's Firewall Settings page. At the top, there are navigation links: "Advanced >> Firewall Settings >> Advanced", "IPv4 Rules", "IPv6 Rules", and a "Save" button. The "Enable DMZ" checkbox is checked and highlighted with a yellow box. Below it, the "DMZ IP Address" field is empty, and a dropdown menu is open, showing a list of computer names and their IP addresses, also highlighted with a yellow box. The list includes: "<< Computer Name", "<< Computer Name", "192.168.0.101 (COVR-2200)", "192.168.0.103 (DCS-8100LH)", "192.168.0.104 (WiFi_2.4G)", "192.168.0.106 (08384NBWIN7)", and "192.168.0.105 (android-7664776b15d)". Below the DMZ settings, there are four other settings, all disabled: "Enable SPI IPv4", "Enable Anti-spoof Checking", "IPv6 Simple Security", and "IPv6 Ingress Filtering".

6-2: How do I open ports on my router?

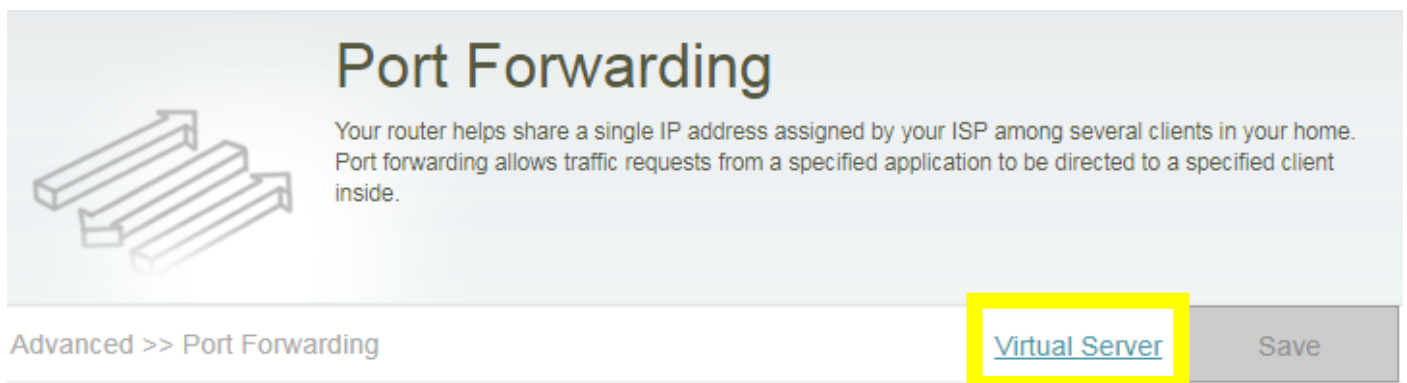
Scenario 1: Single Port:

By default, your router will block all incoming connections (into your network) and allow all outgoing connections to the Internet. In some cases, you may need to allow some connections into your network, for example when using the Remote Desktop application. To use these applications, you must open ports on your router.

Please launch your browser and enter `http://covr.local./` into the address bar. Then login and follow the steps below:

Step 1: Click **Feature** -> **Port Forwarding**

Step 2: Click **Virtual Server** and **Add Rule**

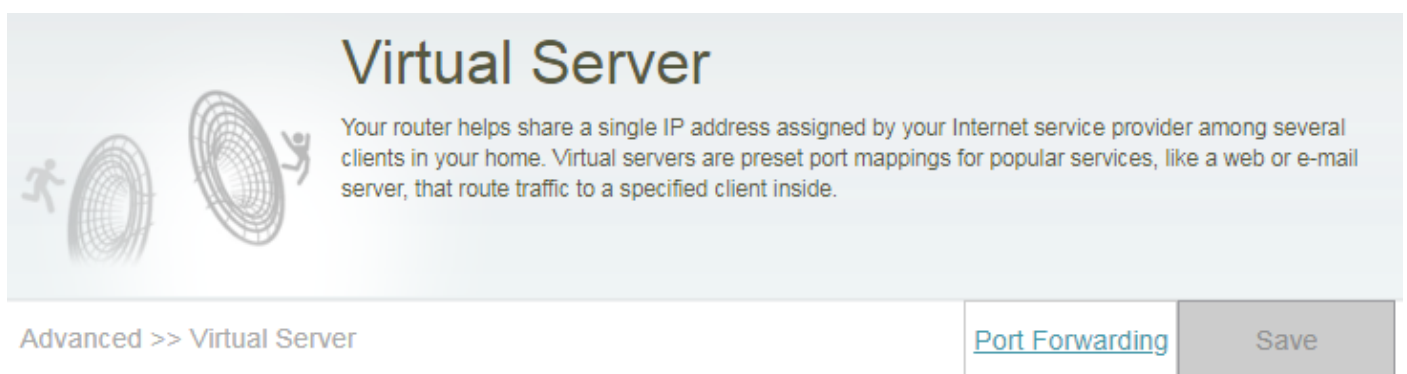


Port Forwarding

Your router helps share a single IP address assigned by your ISP among several clients in your home. Port forwarding allows traffic requests from a specified application to be directed to a specified client inside.

Advanced >> Port Forwarding [Virtual Server](#) Save

Status	Name	Local IP	TCP Port	UDP Port	Schedule	Edit	Delete
Add Rule	Remaining: 15						



Virtual Server

Your router helps share a single IP address assigned by your Internet service provider among several clients in your home. Virtual servers are preset port mappings for popular services, like a web or e-mail server, that route traffic to a specified client inside.

Advanced >> Virtual Server [Port Forwarding](#) Save

Status	Name	Local IP	Protocol	External Port	Internal Port	Schedule	Edit	Delete
Add Rule	Remaining: 15							

Step 3: Enter the necessary information (FTP server as example), then click **Apply**.

- **Name:** Enter a name for the rule (i.e. Web Server 1)
- **Local IP:** Specify the IP address of the device you are opening the port for.
- **Protocol:** Specify the traffic type (TCP or UDP). If you are not sure, choose **BOTH**.
- **External/Internal Port:** Enter the port number you want to open (i.e. 21, for FTP)

Create New Rule ✕

Name: ▼

Local IP: ▼

Protocol: ▼

External Port:

Internal Port:

Schedule: ▼

Apply

Step 4: When you are finished adding your rule(s), click **Save**.

Virtual Server

Your router helps share a single IP address assigned by your Internet service provider among several clients in your home. Virtual servers are preset port mappings for popular services, like a web or e-mail server, that route traffic to a specified client inside.

Advanced >> Virtual Server [Port Forwarding](#) **Save**

Status	Name	Local IP	Protocol	External Port	Internal Port	Schedule	Edit	Delete
<input checked="" type="checkbox"/>	FTP	192.168.0.106	TCP	21	21	Always Enable		


Add Rule Remaining: 14

Scenario 2: Multiple Ports:

Please launch your browser and enter <http://covr.local/> into the address bar. Then login and follow the steps below:

Step 1: Click **Feature** -> **Port Forwarding**

Step 2: Click **Add Rule**



Port Forwarding

Your router helps share a single IP address assigned by your ISP among several clients in your home. Port forwarding allows traffic requests from a specified application to be directed to a specified client inside.

Advanced >> Port Forwarding [Virtual Server](#) Save

Status	Name	Local IP	TCP Port	UDP Port	Schedule	Edit	Delete
--------	------	----------	----------	----------	----------	------	--------

Add Rule

Remaining: 15

Step 3: Enter the necessary information, then click **Apply**:

- **Name:** Enter a name for the rule (i.e. Web Server 1).
- **Local IP:** Specify the IP address of the device you are opening the port for.
- **TCP Port:** Enter the TCP port numbers you want to open.
- **UDP Port-** Enter the UDP port numbers you want to open.

Note: You can enter the ports in multiple different ways- Range (50-100) Individual (80, 68, 888) Mixed (1020-5000, 689).

Create New Rule

Name:

Local IP:

TCP Port:


UDP Port:

Schedule:

Apply



Step 4: When you are finished adding your rule(s), click **Save**.

Port Forwarding



Your router helps share a single IP address assigned by your ISP among several clients in your home. Port forwarding allows traffic requests from a specified application to be directed to a specified client inside.

Advanced >> Port Forwarding [Virtual Server](#) **Save**

Status	Name	Local IP	TCP Port	UDP Port	Schedule	Edit	Delete
<input checked="" type="checkbox"/>	test1	192.168.0.156	22,23,30-40	22,23,30-40	Always Enable		

Add Rule Remaining: 23

Website Filter Setting

7-1: How do I set up a website filter on my router?

Please launch your browser and enter `http://covr.local/` into the address bar. Then login and follow the steps below:

Step 1: Click **Features** -> **Website Filter**

Step 2: If you want to create a list of sites to block, **select DENY clients access to ONLY these sites** from the drop-down menu. All other sites will be accessible.

Website Filter

The website filters feature allows rules to be set that restrict access to a specified web address (URL) or blocks specified keywords in the URL. You can use Website Filter to restrict access to potentially harmful and inappropriate websites.

Advanced >> Website Filter Save

DENY clients access to ONLY these sites
DENY clients access to ONLY these sites
ALLOW clients access to ONLY these sites

Add Rule Remaining: 15 Delete

If you want to specify a list of sites to allow, select **ALLOW clients access to ONLY these sites** from the drop menu. All other sites will be blocked.

Step 3: To add a new site to the list, click **Add Rule** and enter the URL or domain you wish to deny or allow access to in the Website URL/Domain column. When you are finished adding your rule(s), click **Save**.

Advanced >> Website Filter

DENY clients access to ONLY these sites

Website URL/Domain	Delete
www.taipeitimes.com/	

Add Rule Remaining: 14

Note:

1. Up to 15 websites can be added.
2. If you wish to delete a rule, click on its trash can icon in the Delete column. If you wish to edit a rule, simply replace the URL or domain.
3. **The https websites such as Facebook, Youtube, Amazon, etc cannot be blocked by the website filter. To block these, you may need to apply for an OpenDNS paid service.**

The apply for an OpenDNS account, please visit <https://www.opendns.com/setupguide/>. A 15 day free trial is available. Sign up for new account and follow the setup guide on how to establish the service.

Note: Please confirm if DNS relay is enabled. By default, this should be enabled.

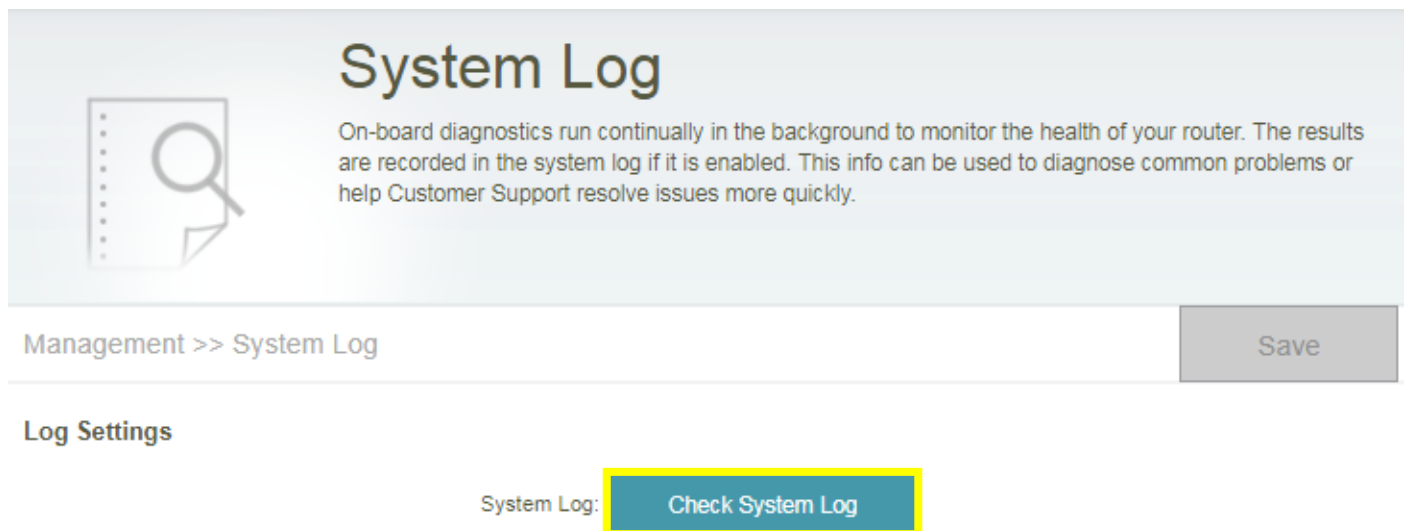
System Log & Statistics

8-1: How do I check the system log of my router?

Select **Management** -> **System Log**, and follow the methods as below:

One-time Syslog:

Step 1: Click **Check System Log** button, and download the file "messages" to your local hard drive.

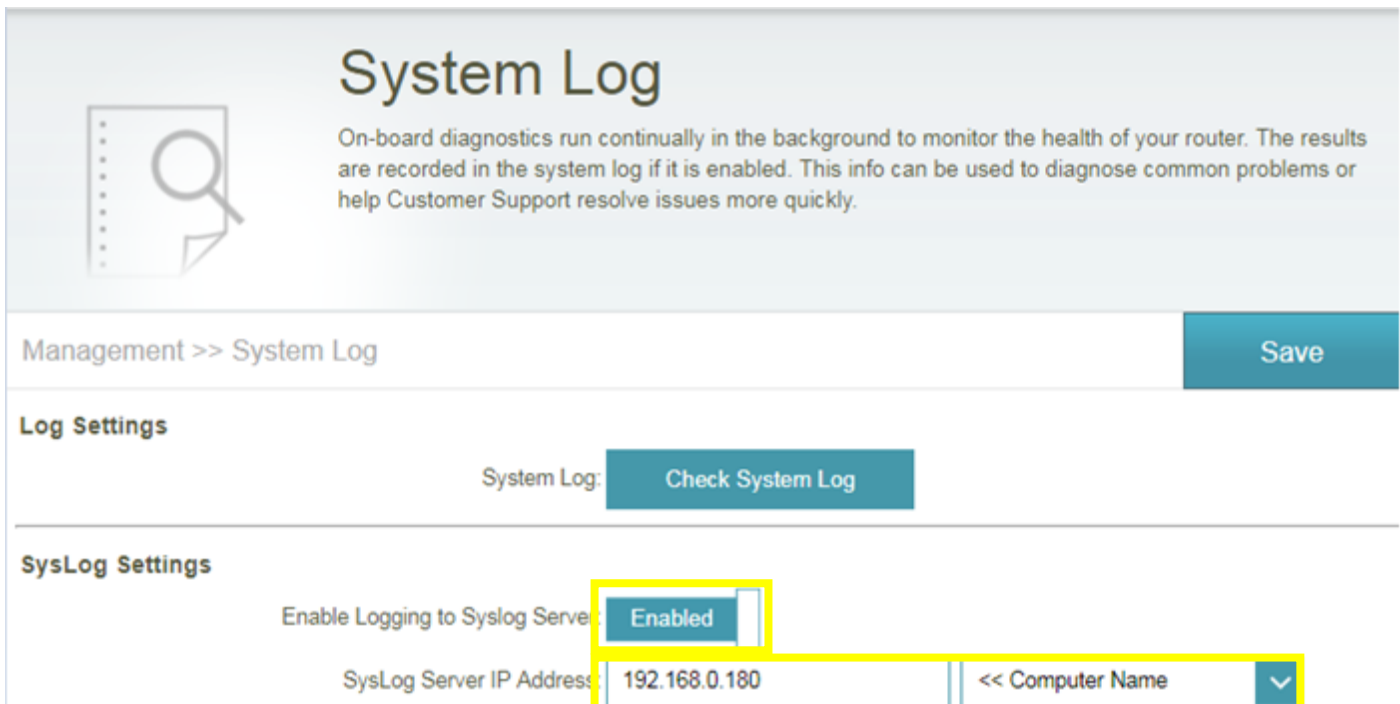


Step 2: Open the messages using a text editor such as WordPad or NotePad to the check system log.

```
Feb 20 23:37:13 prog-cgi[2215]: security.c:AUTH_CheckSessionHandler:1593:--  
AUTH_CheckSessionHandler:Success--  
Feb 20 23:37:13 prog-cgi[2215]: security.c:portal:1977:wp->method = POST  
Feb 20 23:37:13 prog-cgi[2215]: security.c:isNoCheckUrl:2105:wp->url:/HNAP1/  
Feb 20 23:37:13 prog-cgi[2215]:  
security.c:isNoCheckUrl:2106:soapaction:"http://purenetworks.com/HNAP1/GetWanStatus"  
Feb 20 23:37:13 prog-cgi[2215]: security.c:isPostMethod:1607:method:POST,wp->url:/HNAP1/  
Feb 20 23:37:13 prog-cgi[2215]:  
security.c:AUTH_CheckHandler:1241:hnap_auth:361AE464C481B06133DC077E0578F112,  
1519141038644,soapaction:"http://purenetworks.com/HNAP1/GetWanStatus"  
Feb 20 23:37:13 prog-cgi[2215]:  
security.c:AUTH_CheckHandler:1283:auth_code_md5:361AE464C481B06133DC077E0578F112,  
auth_code:361AE464C481B06133DC077E0578F112  
Feb 20 23:37:13 prog-cgi[2215]: security.c:AUTH_CheckHandler:1289:AUTH_CheckHandler:  
time : 1519141038644, timestamp : 1519141037645, webstime : 1519141038644  
Feb 20 23:37:13 prog-cgi[2215]: security.c:timestampFaultRate:1191:webstime - timestamp =  
faultlen : (1519141038644 - 1519141037645) = 999  
Feb 20 23:37:13 prog-cgi[2215]: security.c:timestampFaultRate:1195:tmTime : 1519141038644  
,tmTimeLast : 1519141037645  
Feb 20 23:37:13 prog-cgi[2215]:  
security.c:AUTH_CheckHandler:1292:AUTH_CheckHandler:Success  
Feb 20 23:37:13 prog-cgi[2215]: security.c:websSecurityHandler:3109:mRet:0,urlPrefix:/,webDir:  
Feb 20 23:37:13 prog-cgi[2215]:  
form.c:websFormHandler:57:fn:0x436f38,formName:GetWanStatus  
Feb 20 23:37:13 prog-cgi[2215]: modules/Internet.c:GetWanStatus:244:ret=3  
Feb 20 23:37:13 prog-cgi[2215]:
```

Real-time Syslog:

Step 1: Enable “**Enable Logging to Syslog Server**”, and fill in the IP address of the PC which you’d like to set as syslog server:

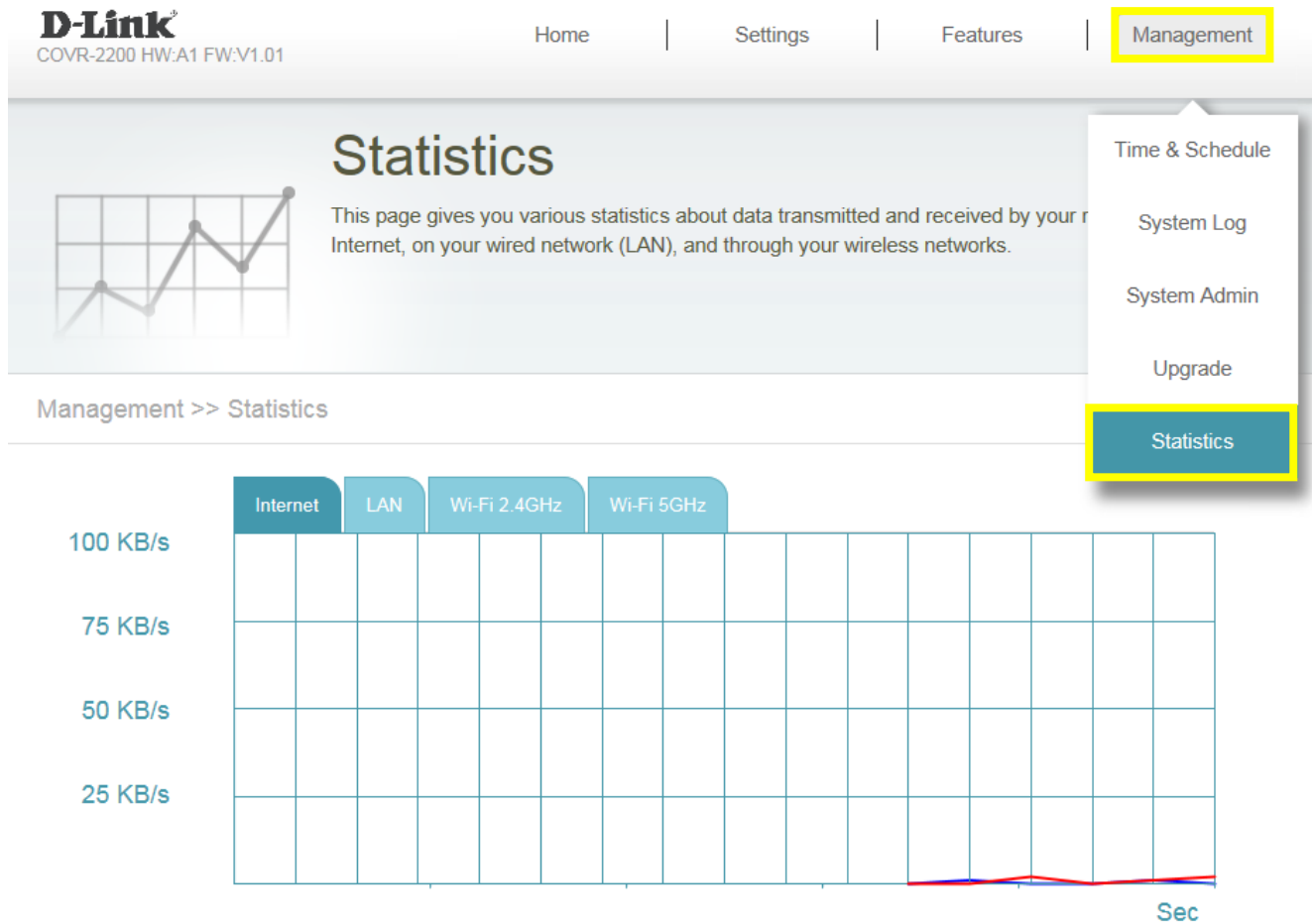


The screenshot shows the 'System Log' configuration page. At the top, there is a header with the title 'System Log' and a brief description: 'On-board diagnostics run continually in the background to monitor the health of your router. The results are recorded in the system log if it is enabled. This info can be used to diagnose common problems or help Customer Support resolve issues more quickly.' Below the header, there is a breadcrumb trail 'Management >> System Log' and a 'Save' button. The 'Log Settings' section includes a 'System Log:' label and a 'Check System Log' button. The 'SysLog Settings' section contains two main fields: 'Enable Logging to Syslog Server' with a dropdown menu set to 'Enabled', and 'SysLog Server IP Address' with a text input field containing '192.168.0.180' and a dropdown menu set to '<< Computer Name'. A yellow highlight box encompasses the 'Enabled' dropdown, the IP address input field, and the '<< Computer Name' dropdown.

Step 2: Download a system log server application you prefer to use, and configure the required setting to it.

8-2: How do I check network statistics for my router?

Click **Management** -> **Statistics**. An interactive diagram of all the transmitted and received packets (via Internet, LAN or the 2.4G/5G Wi-Fi bands) will be displayed:



DNS/DDNS

9-1: How do I configure Dynamic DNS on my router?

Please launch your browser and enter <http://covr.local/> into the address bar. Then login and follow the steps below:

Step 1: Click **Features** -> **Dynamic DNS**

Step 2: Enable **Dynamic DNS**, and enter your Dynamic DNS account information, then click **Save**:

Advanced >> Dynamic DNS Save

Enable Dynamic DNS: Enabled

Status: Disconnected

Server Address:

Host Name:

User Name:

Password:

Time Out: hours

Step 3: Your DDNS is successfully established after **Status** shows **Connected**:

Advanced >> Dynamic DNS Save

Enable Dynamic DNS: Enabled

Status: Connected

Server Address:

Host Name:



User Name:

Password:

Time Out: hours

Note:

1. To register for the dlinkddns service, please visit: <https://www.dlinkddns.com/signin/>, then fill in the required information.

HOME	UPGRADE ACCOUNT	CHANGE EMAIL	CHANGE PASSWORD	SUPPORT
 Reminder: This service is for D-Link customers only. If you are not a D-Link user and you're looking for a way to remotely access your router, computer, etc.; then Dyn would love to offer you an exclusive 25% off our Remote Access (DynDNS Pro) service . You'll gain access to up to 30 hostnames per account and will never have to worry about your account expiring!				HOW TO
<h2>New Account</h2> <p>Username <input type="text"/></p> <p>Password <input type="password"/></p> <p>Confirm Password <input type="password"/></p> <p>Email <input type="text"/></p> <p>Serial Number <input type="text"/> ?</p> <p>MAC Address <input type="text"/> ? Ex: 1A:2B:3C:4D:5E:6F</p> <div data-bbox="145 831 647 1025"><p>Type the text <input type="text"/></p><p>Privacy & Terms</p></div>				FAQ
				CONTACT
				LOST PASSWORD

2. If need to access your router remotely, please follow below steps:
 - (1) Make sure if remote management is enabled. [How to enable remote management?](#)
 - (2) If using a PC connecting to the remote network, type in <http://<HostName>:PortNum>, then you could access your router. (For this case, type in <http://kobebrarian.dlinkddns.com:8080>)

QoS Setting

10-1: How do I configure QoS on my router?

Please launch your browser and enter <http://covr.local/> into the address bar. Then login and follow the steps below:

Step 1: Click **Features** -> **QoS Engine**

Step 2: Set the **Management Type** to **Manage By Device**. To assign a priority level to a device, drag the device card from the **Connected Clients** list to an empty slot and release the mouse button. The card will move to the priority slot. If you want to remove a priority assignment from a device and return it to the Connected Clients list, click the cross icon in the top-right of the device card.

- A maximum of one device can be assigned **Highest** priority.
- A maximum of one device can be assigned **High** priority.
- A maximum of two devices can be assigned **Medium** priority.

Advanced >> QoS Engine Save

Management Type: Manage By Device

Download Speed (Mbps): ⓘ

Upload Speed (Mbps):

Connected Clients

◀ 07136NBWIN10
INTEL
192.168.0.100 COVR-2200
UNKNOWN VENDOR
192.168.0.101 WiFi_2.4G
D-LINK
192.168.0.104 DCS-8100LH
D-LINK
192.168.0.103 ▶

Drag the device cards into the priority boxes below.

Highest High Medium

Step 3: Click **Save** to apply your settings.

Time/Schedule

11-1: How do I configure the time on my router?

Please launch your browser and enter <http://covr.local/> into the address bar. Then login and follow the steps below:

Step 1: Click on the **Maintenance -> Time & Schedule**

Step 2: By default, the **D-Link NTP server** is enabled. Select a time zone from the drop-down menu to synchronize the time with the selected region. Click **Save** when you are done.

Time

Your router's internal clock is used for data logging and schedules for features. The date and time can be synchronized with a public time server on the Internet, or set manually.

Management >> System Time [Schedule](#) **Save**

Time Configuration

Time Zone: Asia/ Taipei

Time: 2018/07/18 03:30:43 PM

Automatic Time Configuration

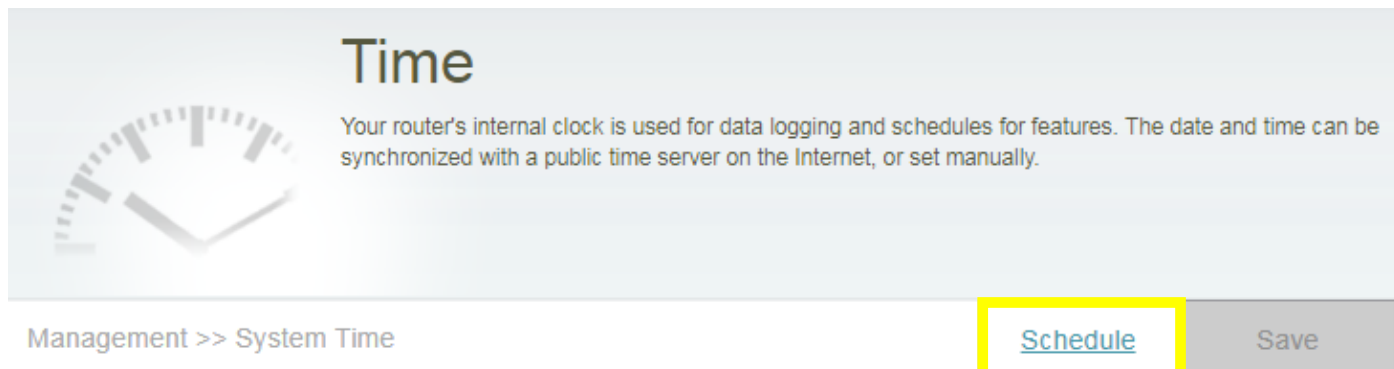
NTP Server: D-Link NTP Server

11-2: How do I create a schedule on my router?

Please launch your browser and enter <http://covr.local/> into the address bar. Then login and follow the steps below:

Step 1: Click on the **Maintenance -> Time & Schedule**

Step 2: Click **Schedule**:




Time

Your router's internal clock is used for data logging and schedules for features. The date and time can be synchronized with a public time server on the Internet, or set manually.

Management >> System Time [Schedule](#) Save

Step 3: Click Add Rule:



Schedule

Some features, such as the firewall and website filters, can be turned on or off based on a schedule. One common use of schedules is to control access to the Internet by a specified device during specified time periods.

Management >> Schedule
[Time](#)
Save

Name	Schedule	Edit	Delete
Add Rule	Remaining: 10		

Step 4: Create your Schedule and click **Apply**. The example below shows the scheduled time from 22:00-24:00 at night, and 00:00-06:00 in the midnight. You can select up to one time period per day, for each day of the week.

Name: ✕

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon	0:00 - 6:00					✕																		✕
Tue	0:00 - 6:00					✕																		✕
Wed	0:00 - 6:00					✕																		✕
Thu	0:00 - 6:00					✕																		✕
Fri	0:00 - 6:00					✕																		✕
Sat	0:00 - 6:00					✕																		✕
Sun	0:00 - 6:00					✕																		✕

Apply

After setup is completed, you'll see your configuration as below:

Name	Schedule	Edit	Delete
test	Mon : 0:00 - 6:00, 22:00 - 24:00 Tue : 0:00 - 6:00, 22:00 - 24:00 Wed : 0:00 - 6:00, 22:00 - 24:00 Thu : 0:00 - 6:00, 22:00 - 24:00 Fri : 0:00 - 6:00, 22:00 - 24:00 Sat : 0:00 - 6:00, 22:00 - 24:00 Sun : 0:00 - 6:00, 22:00 - 24:00	✎	🗑

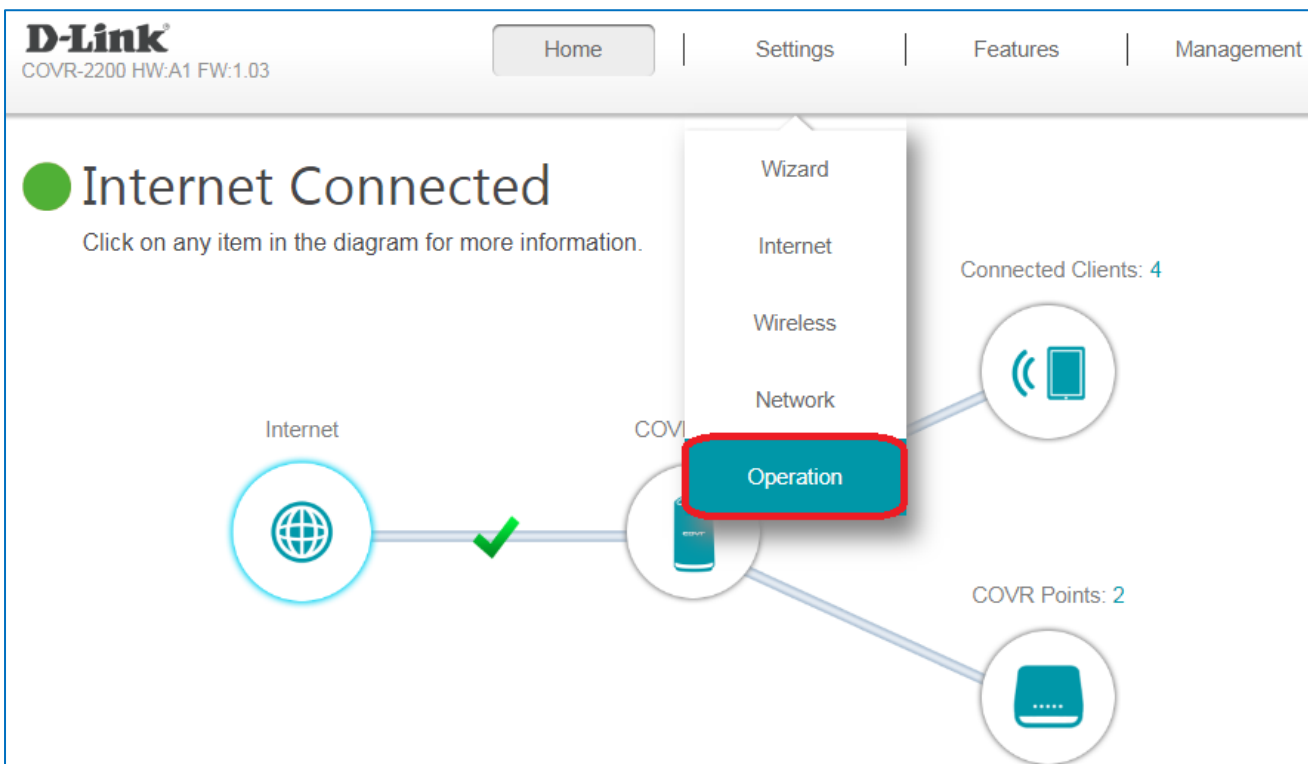
Bridge Mode

12-1: How do I configure my router to bridge mode?

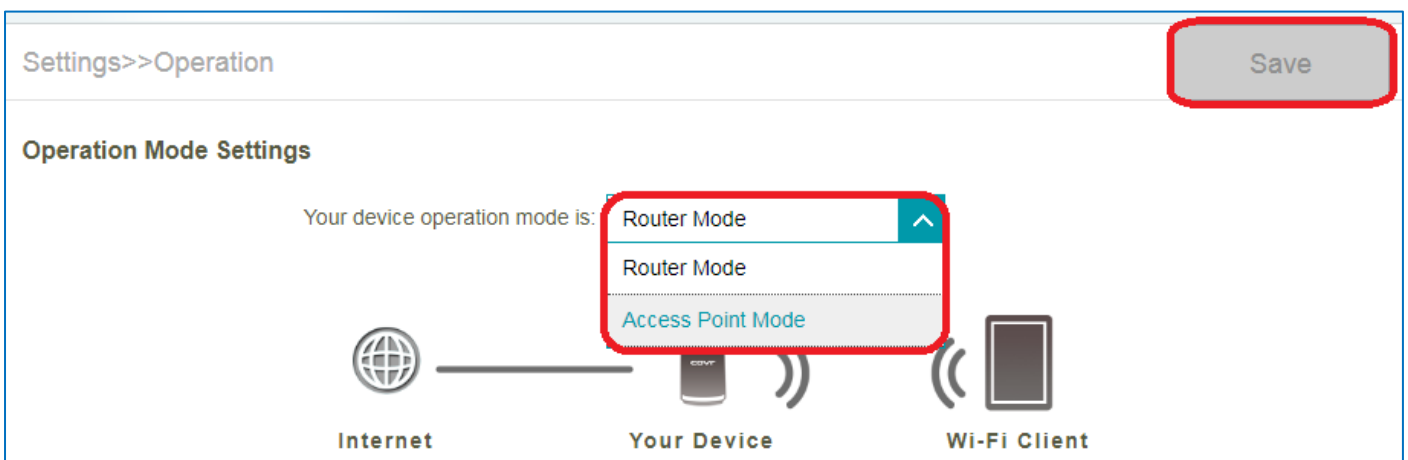
Please note that the firmware must be **v1.03** or above.

Please launch your browser and enter <http://covr.local/> into the address bar. Then login and follow the steps below:

Step 1: Click on the **Settings -> Operation**



Step 2: Switch the operation mode to Access Point Mode from the drop-down menu.



Step 3: After setting up bridge mode, connect your device to the uplink router or the modem with DHCP service with an Ethernet cable. Your device will be dynamically configured by the DHCP server.

Step 4: Your router becomes a bridge since it has no router features, and the uplink router is shown in the home page.

The screenshot displays the D-Link COVR-2200 web interface. At the top left, the D-Link logo and model information (COVR-2200 HW:A1 FW:1.04) are visible. A navigation bar at the top right contains 'Home', 'Settings', and 'Management' buttons, which are highlighted with a red box. A green arrow points from the text 'No router features' to the 'Home' button. The main content area features a green circle and the heading 'Existing Network Connected', with a subtext 'Click on any item in the diagram for more information.' Below this is a network diagram showing an 'Uplink Router' connected to a 'COVR-2200' device, which is in turn connected to two 'COVR Points' (one labeled 'Connected Clients: 2' and another 'COVR Points: 2'). A green checkmark is placed on the connection line between the Uplink Router and the COVR-2200. At the bottom left, a red-bordered box highlights the 'Uplink Router' information panel, which includes: 'Connection Type: Ethernet', 'Network Status: Connected', and 'Connection Uptime: 0 Day, 00 : 07 : 40'. A green arrow points from this panel to the text 'Uplink router info shows in the home page'.

Note: If you need to configure it back to router mode, please reset it to factory default, and run the installation process again.

D-Link defend App for McAfee services


13-1: What is Secure Home Platform?

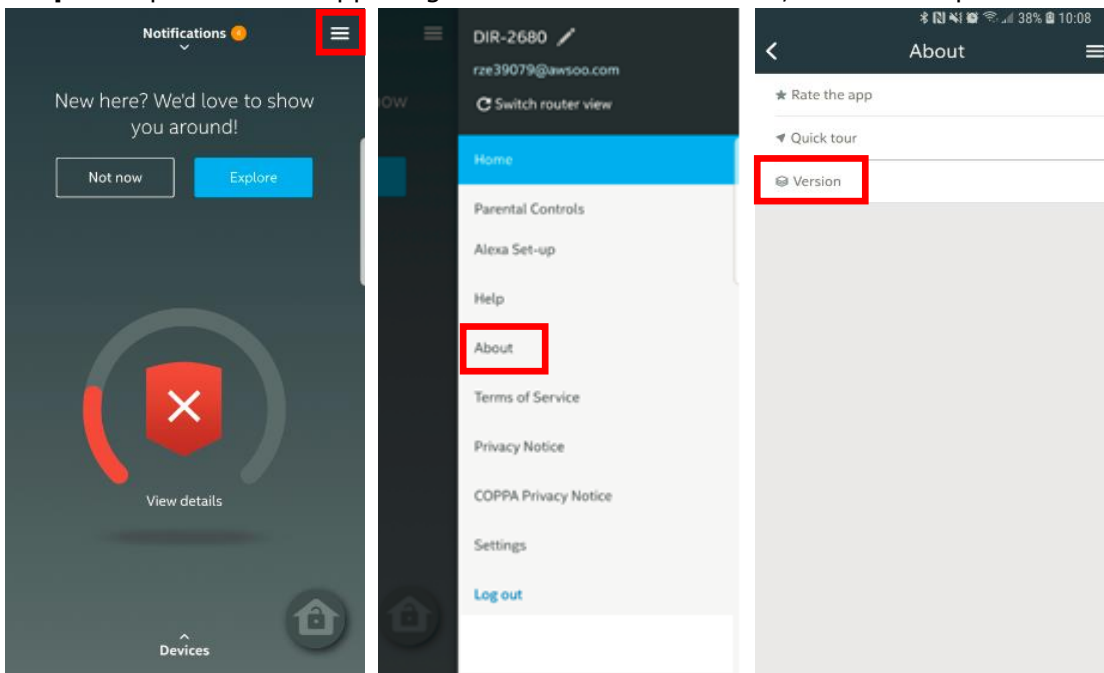
For more information, please visit the McAfee website.

<https://goo.gl/ox518X>

The McAfee SHP service is available in every region except Canada. To use the McAfee SHP service, please upgrade COVR-2202 firmware to v1.04 or above.

13-2: How do I check the SHP and D-Link defend app version?

Step 1: Tap  in the upper right corner. Select **"About"**, and then tap **"Version"**:



Step 2: Both the SHP and D-Link defend App version display.



13-3: What do the security levels mean?

The color is not dependent on the security level applied by the user. It is determined based on the output of an algorithm used by SHP taking few parameters into consideration – some of the parameters include installation of AV, parental controls enabled, device assigned etc. When user takes any action on any of the security card suggestions/recommendations, the score is expected to change. At present, there are 3 possible colors: Red, Amber and Green.



User actions ultimately determine whether the user is in a green, amber, or red zone.

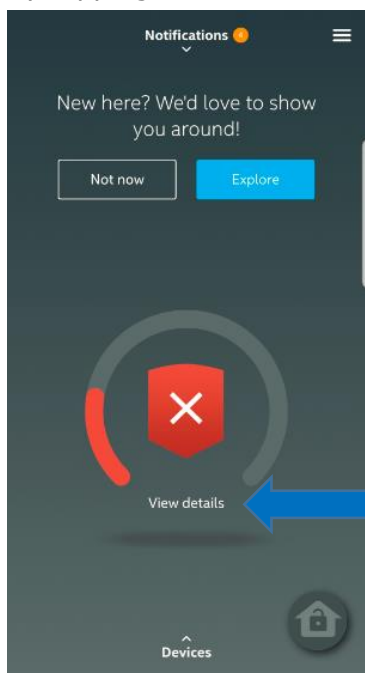
Security level:

- High: Green with a check
- Middle: Yellow with an exclamation point
- Low: Red with an x.

The security level is assessed by whether the below actions are taken out or not:

- Tour walkthrough
- Device update - Edit Device for unidentified devices
- Antivirus installation
- Parental Controls setup
- Time controls setup
- Device assignment to profiles

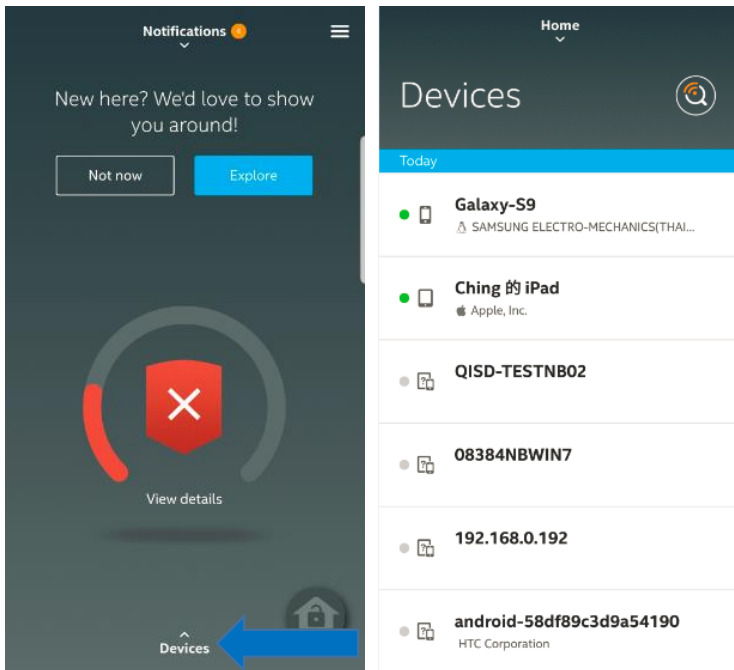
By tapping **View Details**, parents can access tips to increase the security level of their network.



13-4: What information can we check of each client device in the device list?

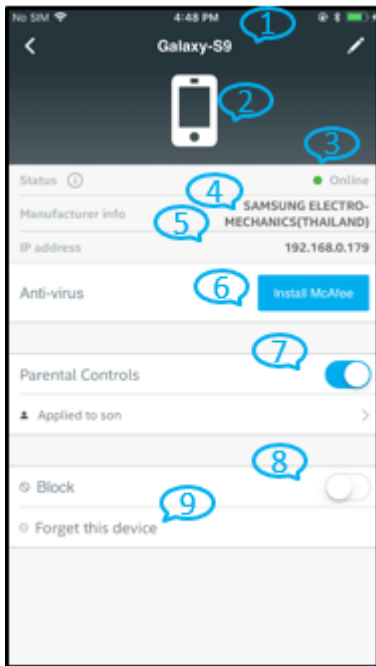
By tapping on **Devices** from the Home page, parents can view all the devices connected to their network.

Step 1: Click on **Devices** from the Home page. Then, select a specific client device:



Step 2: The device information includes:

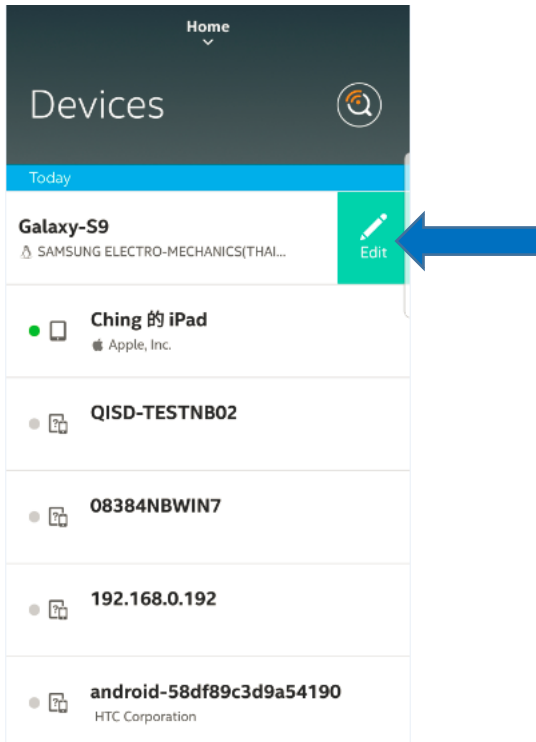
1. Device name
2. Device type
3. Online/offline status
4. IP address
5. Manufacturer
6. Install the McAfee LiveSafe app
7. Parental control status
8. If this device is blocked
9. Forget the device



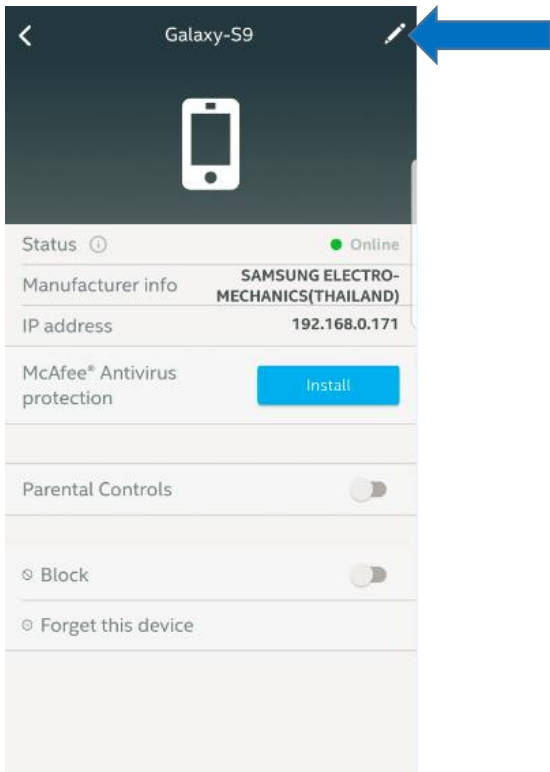
13-5: How do I edit a device?

There are 2 ways to edit a device: Swiping left in the device list and clicking Edit, or clicking the pencil icon on the device details page.

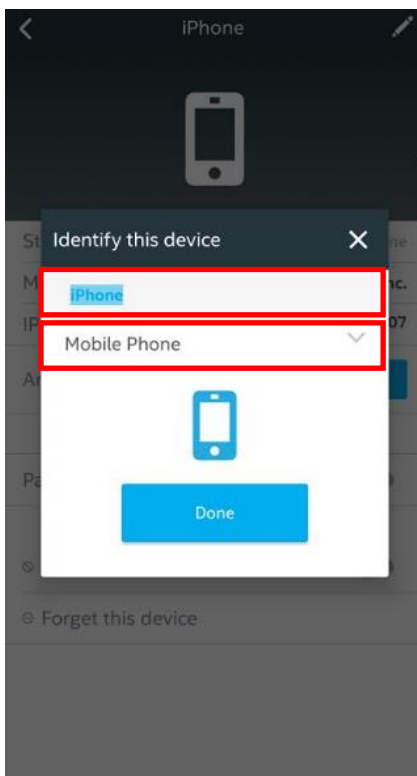
Method 1: Swipe left on a device in the device list, and click **Edit**.



Method 2: Tap the pencil icon on the device page:



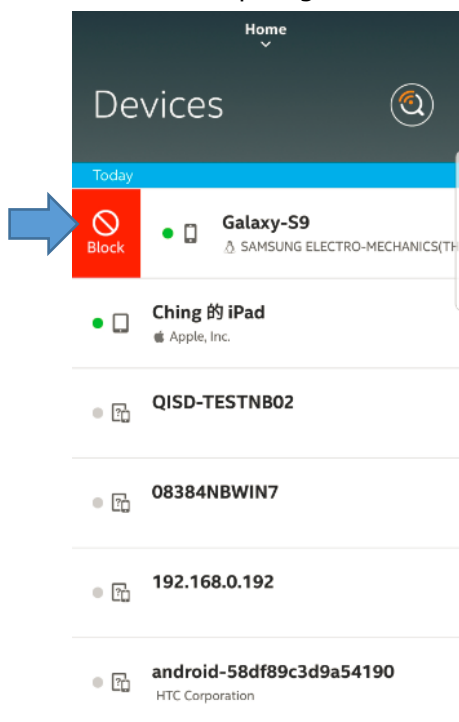
Then you can identify the device by entering a name, and choosing the device type:



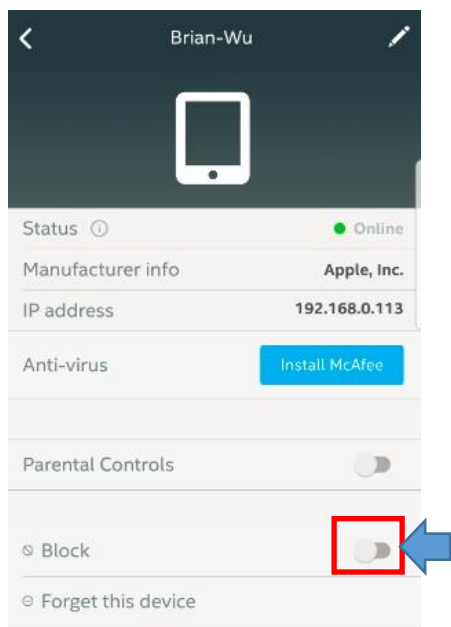
13-6: How do I block a device from the Internet access?

There are 2 ways to block a device.

Method 1: Swipe right on the device list and tap **Block**:



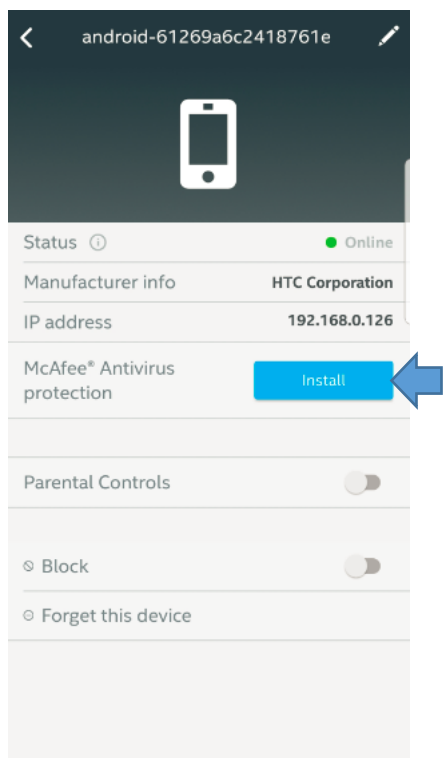
Method 2: Toggle the slider beside Block on the device page.



13-7: How do I install McAfee Antivirus protection on a mobile device or PC?

McAfee LiveSafe (MLS) features antivirus software with identity and privacy protection for all the computing devices (smartphone, PC and laptop) by blocking viruses, malware, ransomware, spyware, unwanted programs, and more malicious online attacks.

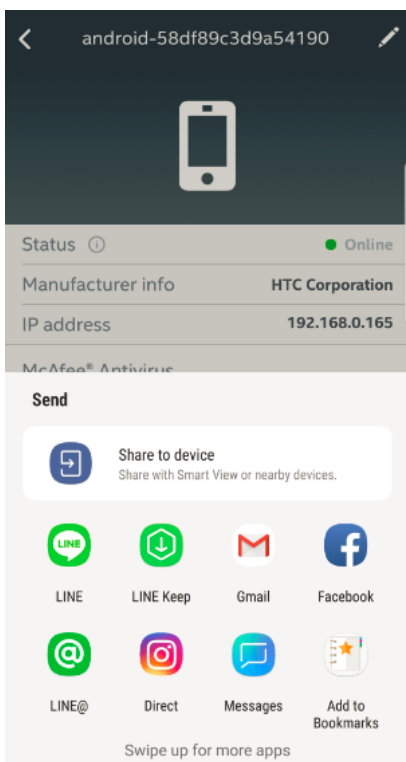
Step 1: Go to a client device, and click **“Install”** to install MLS. Please note that you need to select a non-IoT device.



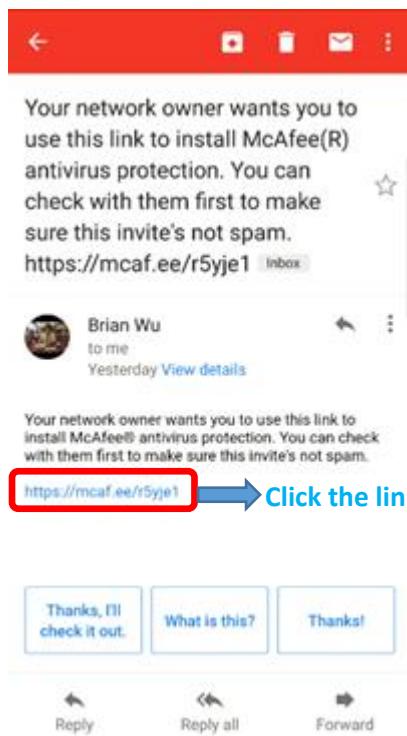
Step 2: Tap "SEND" to send the download link:



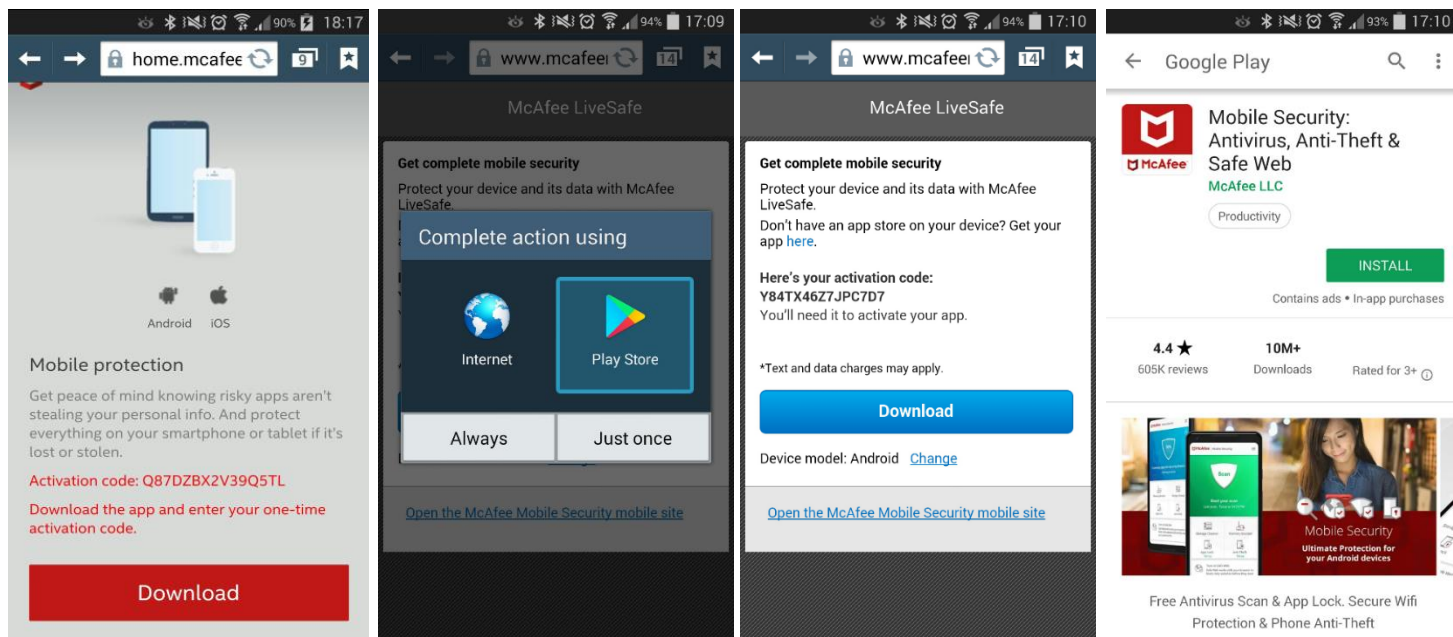
Step 3: Select how you would like to send the download link.



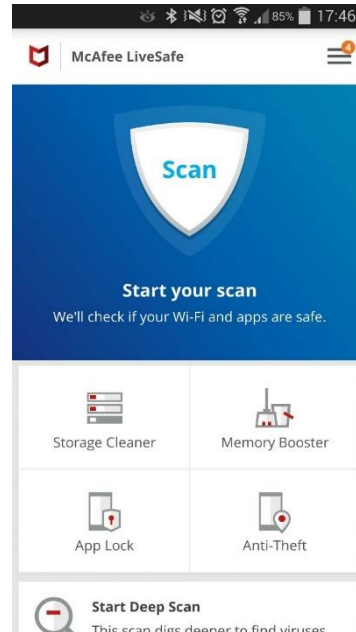
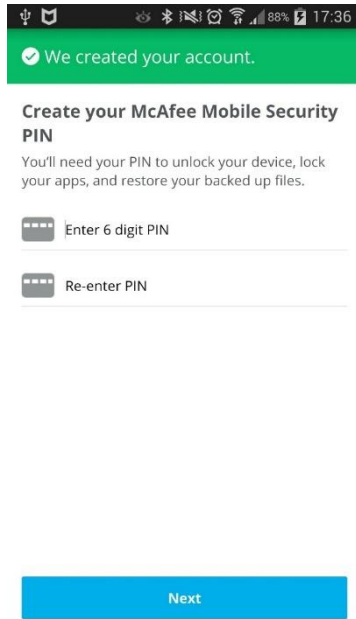
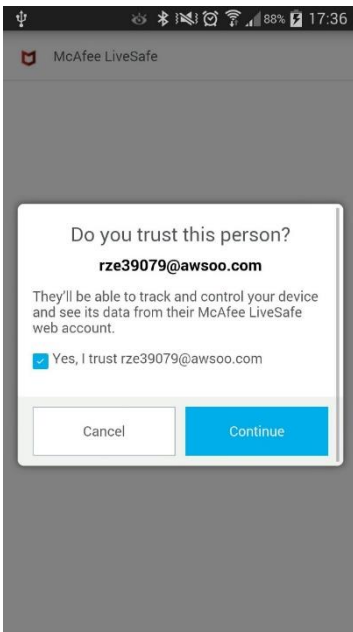
Step 4: Tap the download link to install McAfee antivirus protection.



Step 5: You will receive the activation code of the app. Tap "Download", and then you'll be redirected to the download page of Google Play/App Store:



Step 6: Trust the inviter, and create a password for the app. Then the McAfee antivirus protection is ready to use.



13-8: How do I remove a device which you no longer manage?

Forgetting a device removes the device from the device list.



13-9: If a client device switches from a wired connection to wireless (or from wireless to wired),

will the client device be discovered as a new device?

When a client device switches from a wired connection to wireless (or from wireless to wired), the device is discovered as a new device. This is because SHP identifies a device by its **MAC address**, and the wired and wireless adapters each assign a different MAC address to the device.

Note: You need to set up all the rules again for the device as it is now considered as a new device.

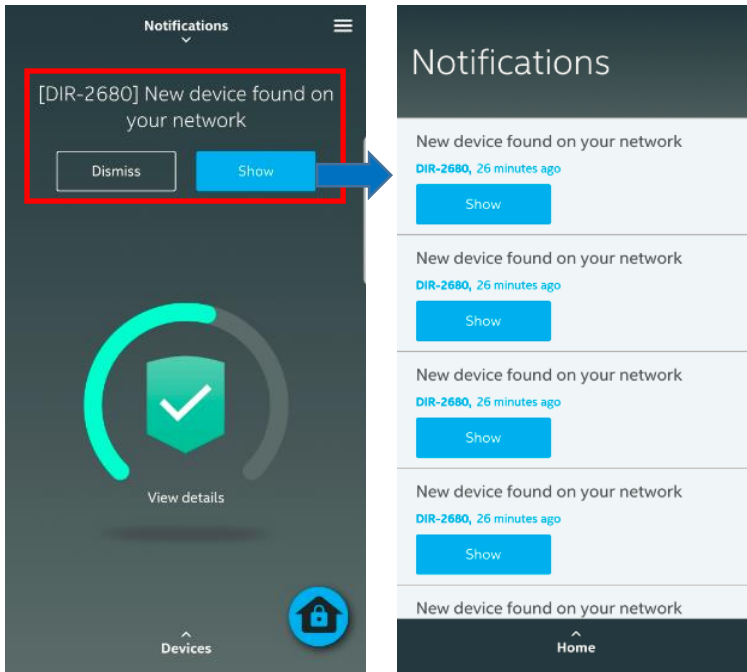
13-10: When a device is disconnected from the network, why does it still appear as online in the

D-Link defend app?


When a device disconnects from the router's network, the device would appear as online for a few minutes. The SHP determines whether the device is offline by waiting for them to miss multiple heartbeats before it can safely conclude that it is offline. This helps SHP to avoid the online devices show as offline.

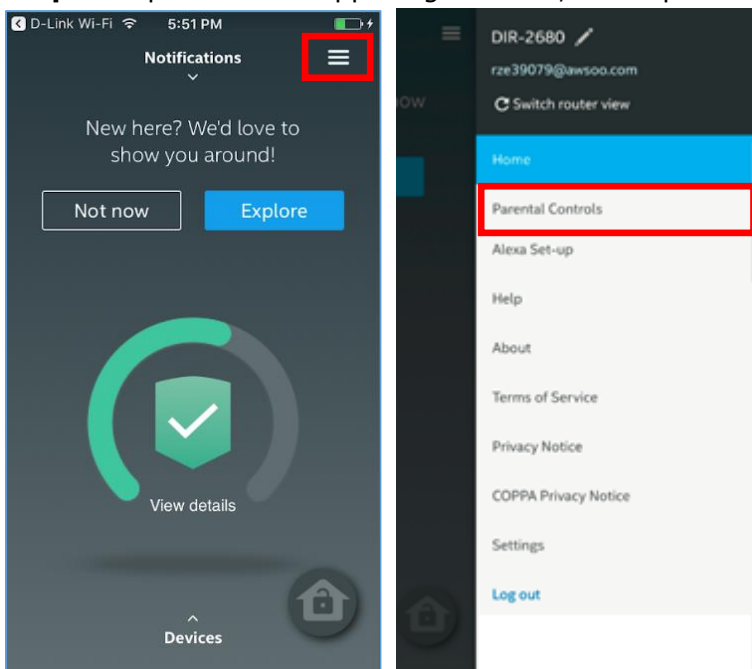
13-11: Can parents be notified if new devices connect to your router?

Yes, parents' device will receive a notification while a new device is found.

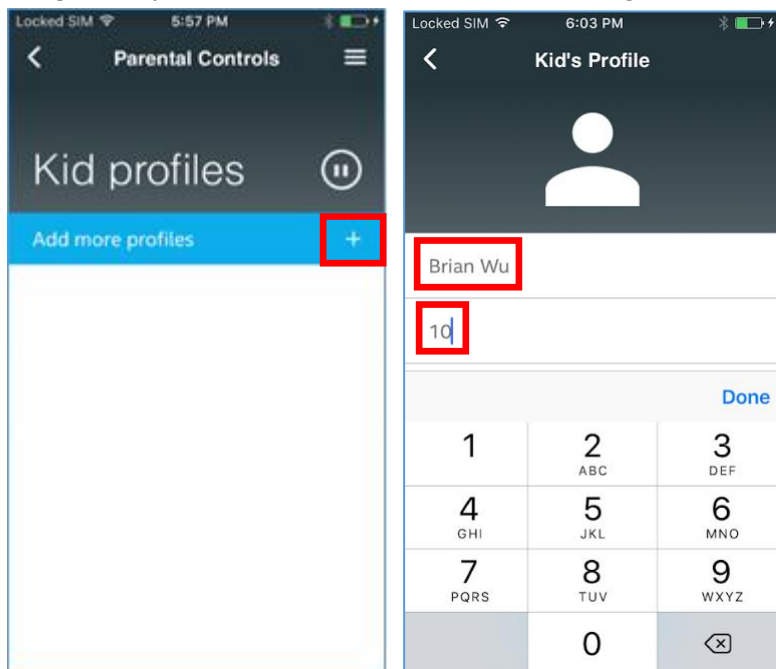


13-12: How do I set up Parental Controls via D-Link defend app?

Step 1: Tap  in the upper right corner, and tap **Parental Controls**.

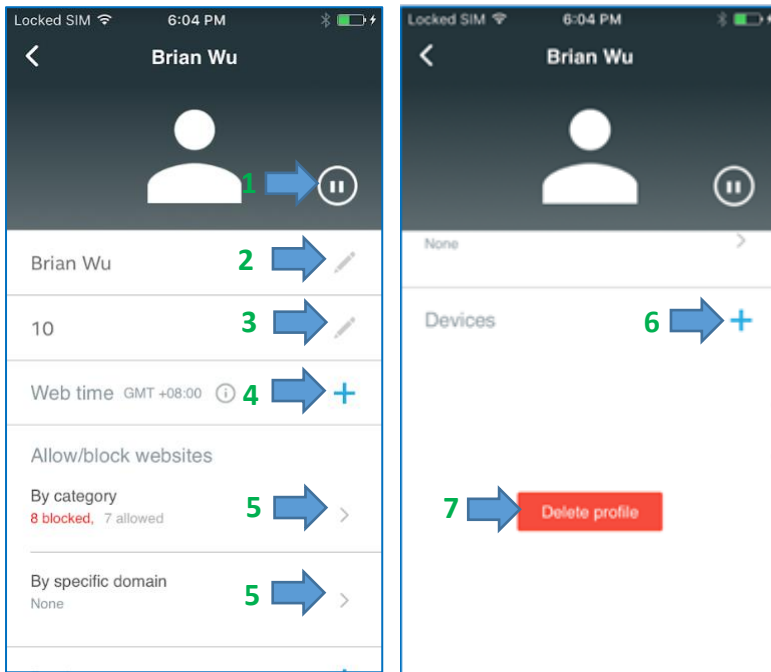


Step 2: Tap '+', and enter a kid's name and age to create a new kid's profile.



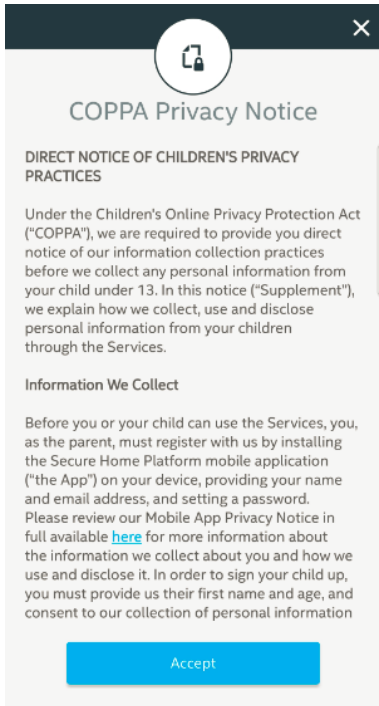
Step 3: A kid profile is created. Parents can manage the profile and set up rules.

1. Pause/resume the internet access of all the devices added to that kid's profile.
2. Edit profile's name
3. Edit profile's age
4. Set the time your kids can access the network.
5. Set what your kids can access on the network and what specific sites are blocked.
6. Add devices to their kid's profile.
7. Delete profile.

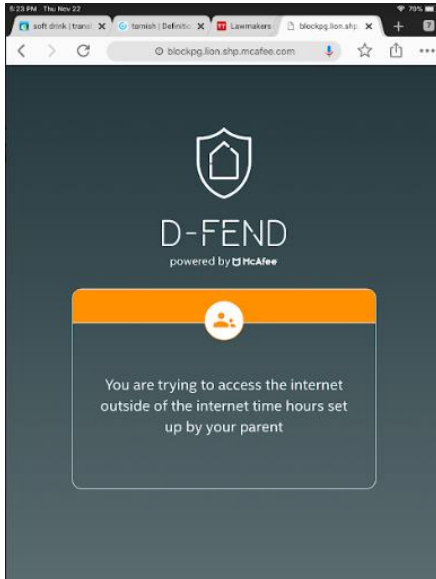


Notes:

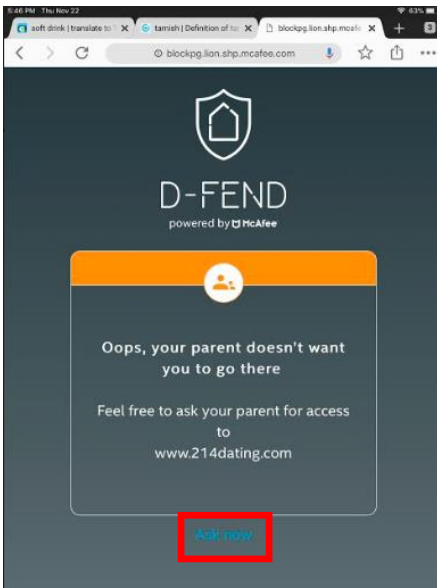
1. If the kid age is less than 13 years, then COPPA (Children’s Online Privacy Policy Protection) notice will be displayed after you add a device to it. Parents must accept the COPPA notice before adding a device.



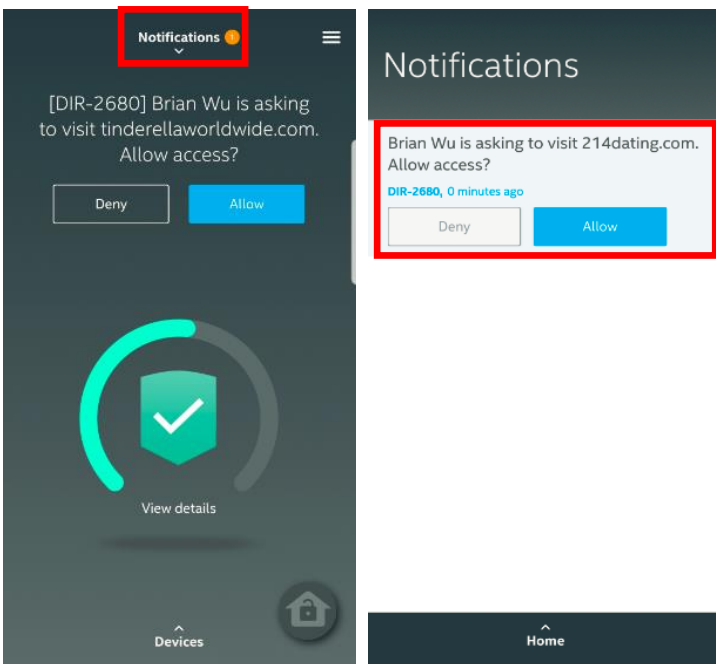
2. If kids are trying to access the internet outside the time set by their parents, they will receive this block page on their browser.



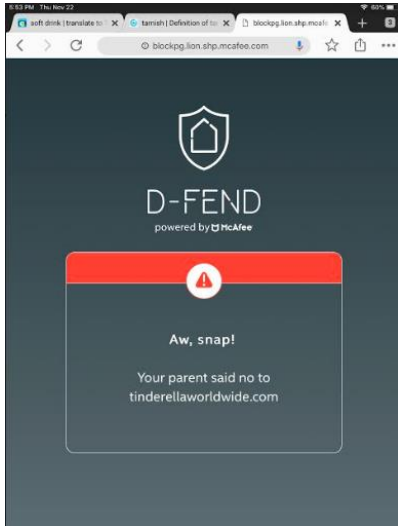
3. If kids are trying to access the website which is categorized as blocked, they will receive the error message below in their browser. They can click **Ask Now** to send a request to their parents to access the site.



Their parents will receive this notification in the D-Link defend app.



- If parents allow the request, their kids will be able to visit the website.
- If parents deny the request, the block page will display on their devices:



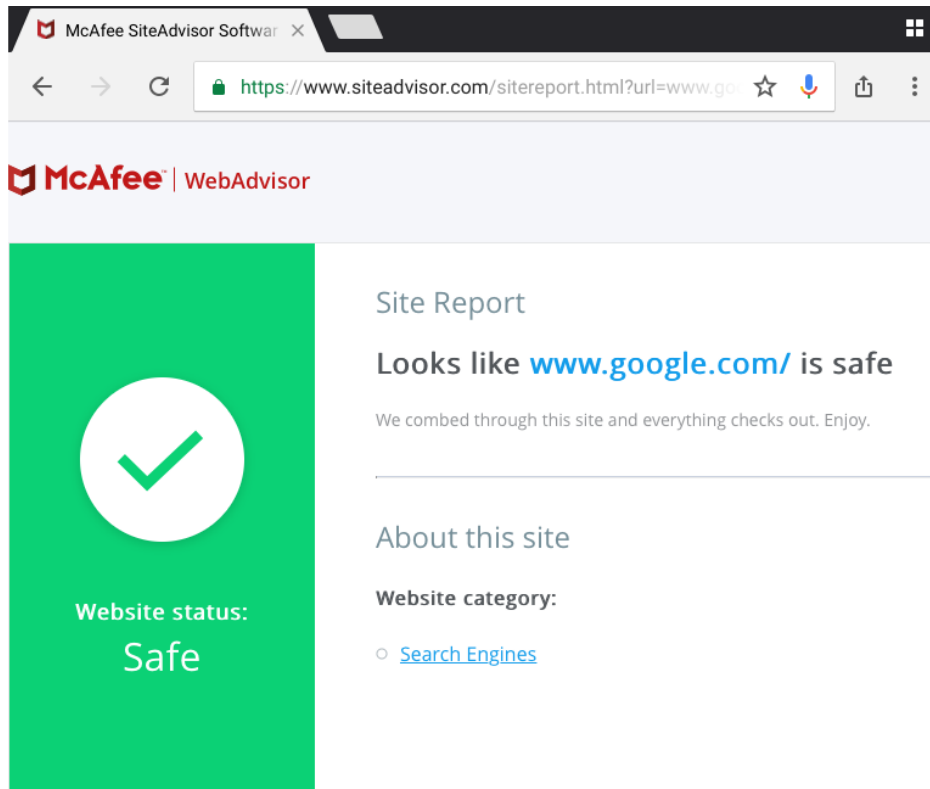
4. Website categories that are allowed or blocked by default depend on kids' age.

Range	Blocked	Allowed
1-7	Dating, Drugs, Alcohol, Tobacco, File transfer and sharing, Gambling Malicious Sites, Parental Control Bypassing, School Cheating, Sexual Content, Social Networking, Uncategorized, Violent Content	Email Entertainment and Streaming Services Games, Search Engines, Shopping and advertising
8-12	Dating, Drugs, Alcohol, Tobacco, Gambling Malicious Sites, Parental Control Bypassing, School Cheating, Sexual Content, Uncategorized, Violent Content	Email Entertainment and Streaming Services Games, Search Engines, Shopping and advertising, File transfer and sharing, Social Networking
Above 12	Dating, Drugs, Alcohol, Tobacco, Gambling Malicious Sites, Parental Control Bypassing, School Cheating, Sexual Content	Email Entertainment and Streaming Services Games, Search Engines, Shopping and advertising, File transfer and sharing, Social Networking, Uncategorized, Violent Content

13-13: How does SHP make sure that a specific website is categorized as blocked or allowed?

You can check the website below to make sure that a browsed website is classified as a blocked category. (Below is for the website www.google.com. If you'd like to check other websites, please change the address)

<https://www.siteadvisor.com/sitereport.html?url=www.google.com/>



13-14: Why does a certificate warning page appear when kids browse a blocked webpage?

If your kid visits the https-based websites that is blocked by parental control policies, certificate warning page will appear. Browsers do this as a security precaution to prevent malicious attacks. SHP will protect you from inappropriate websites (http or https), but because of the browser behavior for https sites it is unable to show you the block page. It shows certificate warning instead.

13-15: Can SHP still prevent a device from visiting malicious sites when VPN is enabled or when proxy is set?

Data through SSL/VPN/proxy connections can't be filtered. Parents must be vigilant if the filtering feasibility of kid's devices is ensured.

13-16: When the Internet is paused, why do some mobile apps, such as Facebook, stay connected to the Internet?

That is because some of these mobile apps cache the DNS requests for a longer time than the browser. Please wait for few more minutes to let the mobile apps finish caching the DNS request.

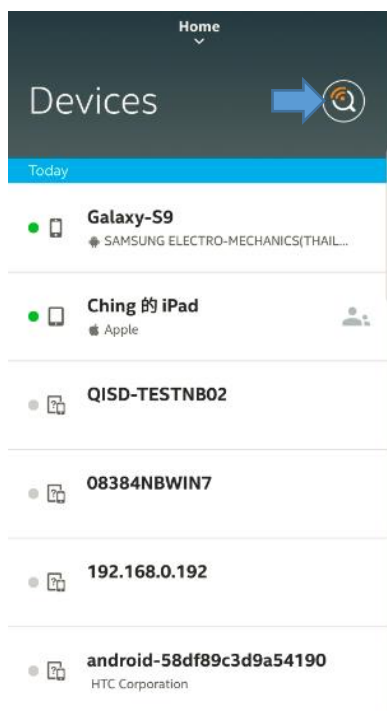
13-17: Why are video streaming still running after pausing the Internet?

DNS requests have already been granted for them. Video streaming will continue until they request for DNS again.

13-18: What does vulnerability scan do?

Vulnerability Scan helps users detect any vulnerabilities found on their network. The Scan ensures that devices have the latest firmware provided by the manufacturer and that they do not retain default credentials for any of their smart devices.

Users can initiate a vulnerability scan from the D-Link defend application by tapping the scan icon on the Devices list:



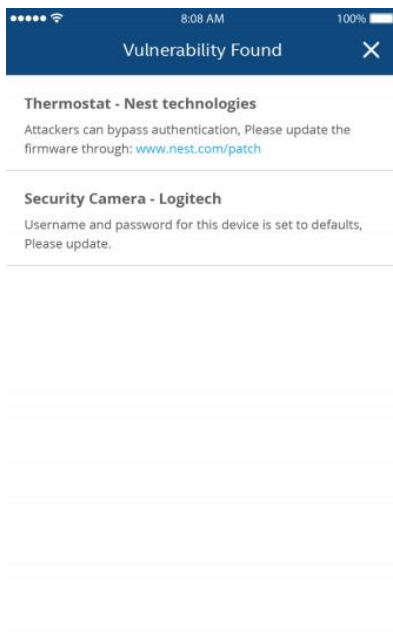
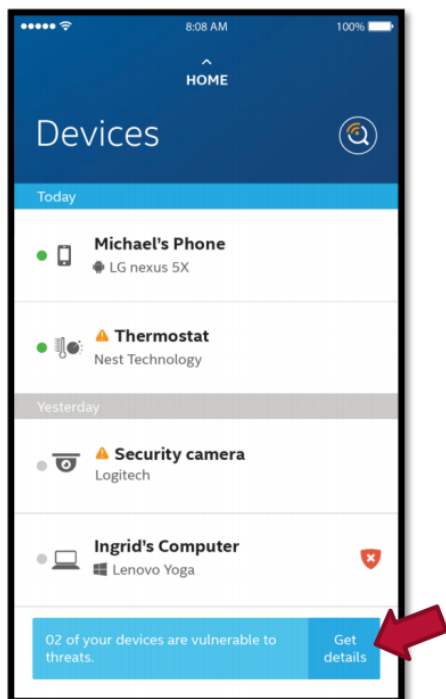
Note: Vulnerabilities will be scanned only if port 22 or 23 is opened, that is, telnet/SSH is enabled.

13-19: What kinds of devices will be scanned when users scan vulnerability?

Devices that are online and identified as IoT devices are scanned:

Device Type	Scanned
Phone	N
Tablet	N
Laptop	N
Mobile Device	N
Desktop	N
Thermostat	Y
Game Console	Y
TV	Y
IP Camera	Y
Multimedia	Y
Smart Lighting	Y
Other IoT Device	Y

If any vulnerabilities are found, a pop-up message displays. To view more details, tap **Get Details**.

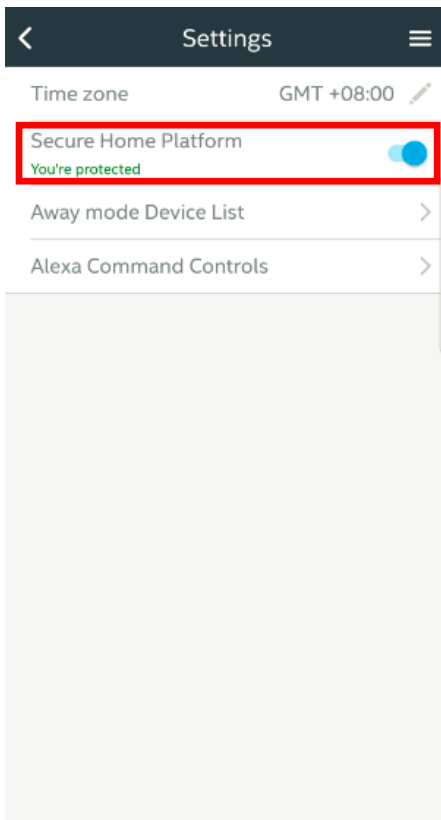


Notes:

1. For now, only two kinds of vulnerabilities are shown:
 - Default user ID password check using CVE (Common Vulnerabilities & Exposures).
 - Update firmware/patch for a device based on information we get from NIST Feed:
<https://nvd.nist.gov/vuln/data-feeds>.
2. For vulnerabilities, users need to contact their device manufacturer.

13-20: How do I check the SHP status in D-Link defend app?

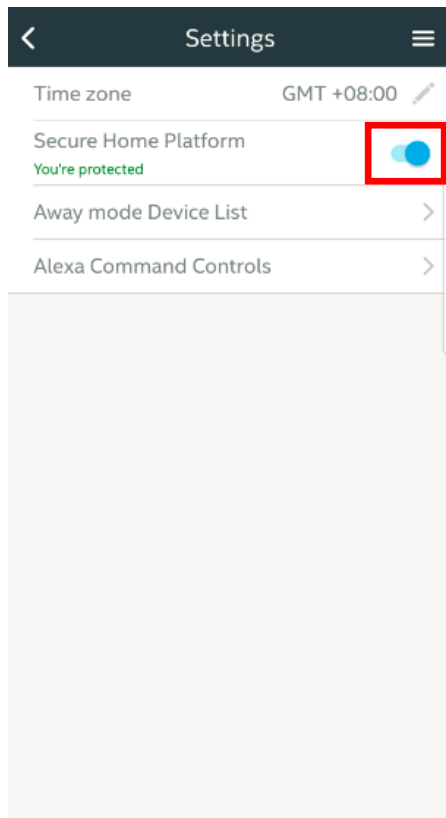
Tap  on the in the upper right corner. Select "**Setting**". Then check the status of "**Secure Home Platform**":



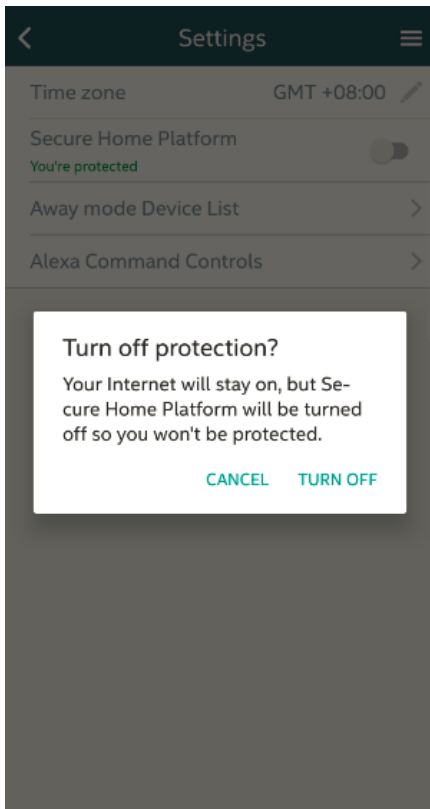
13-21: Can users turn off SHP services in the D-Link defend app?

Yes, users can turn off SHP services in the D-Link defend app anytime. Please note that your internet will stay on, but you won't be protected after you turn off the SHP services.

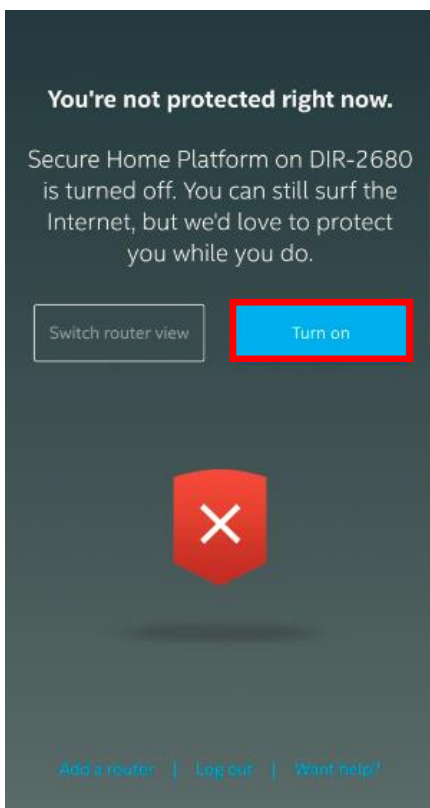
Step 1: Tap  in the upper right corner. Select "Setting". Then toggle the status of "Secure Home Platform":



Step 2: You will be prompted to ensure that you really want to turn off the SHP services. Tap **TURN OFF** to disable the SHP services, or tap **CANCEL** to leave.

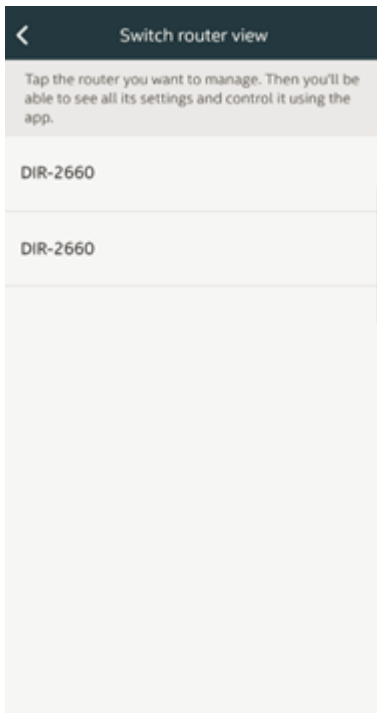


Note: After turning SHP off, users are re-directed to the Home screen, and there is a message showing that SHP services have been turned off. If users want to continue using the app and SHP features, they need to activate SHP by tapping **Turn On**.



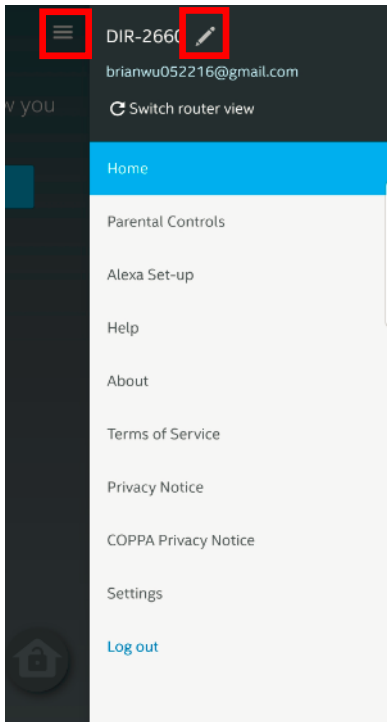
13-22: How do I manage my SHP-enabled routers in the D-Link defend app?

If you have more than 1 SHP-enabled routers in the D-Link defend app, you can manage your router settings by tapping **Switch Router view**.

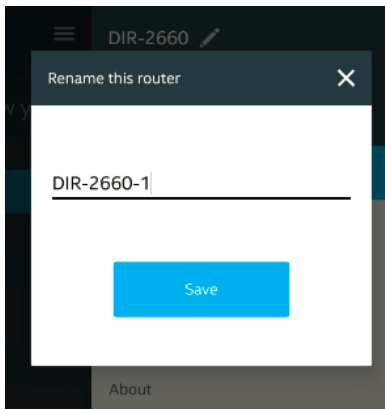


To easily identify your routers, you can change router names by tapping the pencil icon.

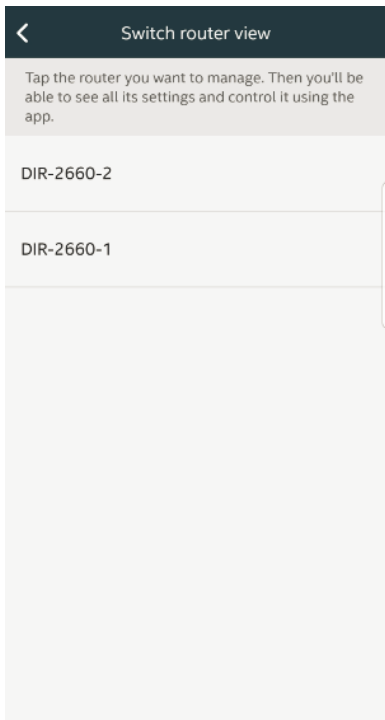
Step 1: Tap the menu in the upper right corner. Then tap the pencil icon :



Step 2: Then you're able to rename each router:



Step 3: The setting is saved.



13-23: How do I use D-Link defend features by Amazon Alexa voice commands?

Step 1: Download **Amazon Alexa** app from App Store/Google Play, and then log in to it with your Amazon account.

Note: Please make sure Amazon Alexa app service is ready in your country.

Step 2: Open Alexa app, and then follow the instruction below:

- Go to the setting menu from top-left side, and select "**Skills**".
- Search for **McAfee** or **D-Link defend** and tap it to open the Skill details page.
- Tap the **Enable Skill** button.
- Log in with your D-Link Wi-Fi account and tap **Authorize** to link your account to Alexa.

You can now use Amazon Alexa voice control service to configure D-LINK DEFEND function.

Step 4: Start to control your router via talking to Amazon Alexa app or Amazon Alexa device by following the command instruction as below:

Control	First Commands	Second Commands	Alexa devices			
			Echo Dot	Echo	Echo show	Others
Check network summery	Open D-Link defend	What's up with my network	V	V	V	V
Find out how many devices are connected to the network		How many devices are online right now?	V	V	V	V
Get the 5 notifications of what's happening on your network		What notifications I have?	V	V	V	V
Scan for vulnerabilities to threats		Initiate/start a vulnerability scan	V	V	V	V

Get the result of vulnerability scan	Open D-Link defend	If there are any vulnerabilities found	V	V	V	V
Block a device from accessing network		Block {device's name}	V	V	V	V
Unblock a device from accessing network		Unblock {device's name}				
Pause the internet for everyone under all parental control policies		Pause the internet for all kids	V	V	V	V
Restart the internet for everyone under all parental control policies		Resume the internet for all kids	V	V	V	V
Pause the internet for everyone under a particular parental control policy		Pause the internet for {policy name}	V	V	V	V
Resume the internet for everyone under a particular parental control policy		Resume the internet for {policy name}	V	V	V	V
Set web time for a particular parental control policy		Assign web time for {policy name}	V	V	V	V
Which router am I connecting to? (If there are 2 or more than 2		Which router am I currently connecting?	V	V	V	V

SHP-enabled routers)						
Switch router (If there are 2 or more than 2 SHP-enabled routers)		Switch to {router name}	V	V	V	V

Note: When a round of conversation ends, D-Link defend will leave the conversation. If you'd like to use Amazon Alexa app or Amazon Alexa Echo device to control D-Link defend again, please speak "**Open D-Link defend**" again to Amazon Alexa app or Amazon Alexa Echo device to activate a new round of conversation.

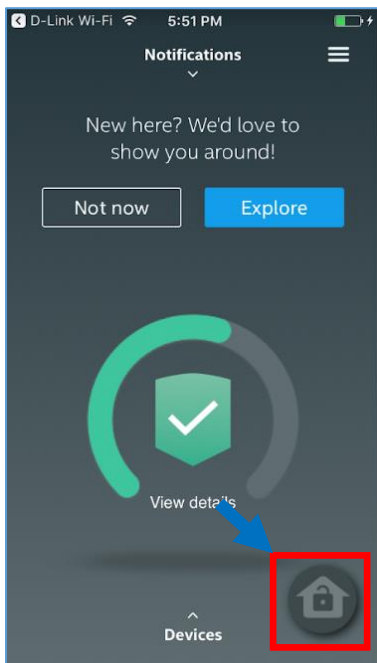
13-24: Does D-Link defend support The Google Assistant?

No, D-Link defend supports Amazon Alexa only.

13-25: How do I set up Away mode?

Away mode allows users to disconnect any devices they want with a single click when they leave home. When Away mode is enabled, no internet is available for devices which are added to the Away device list.

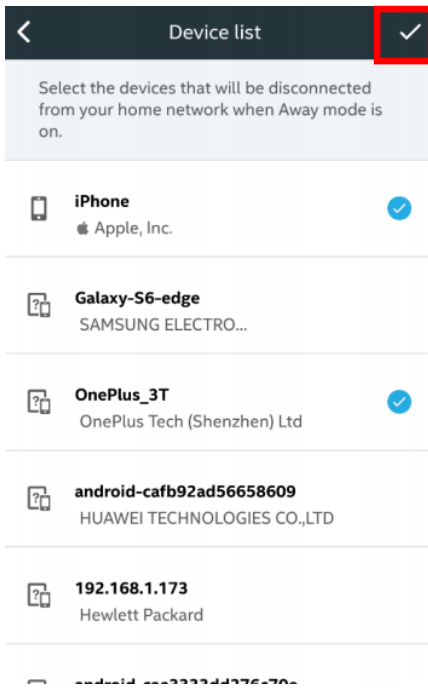
Step 1: Activate Away Mode from the Home screen in the D-Link defend app:



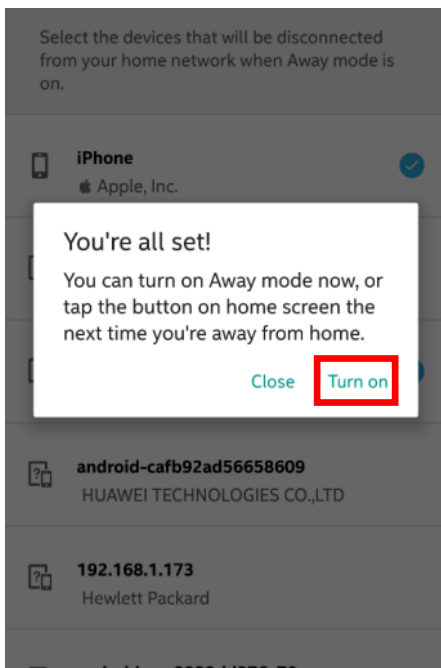
Step 2: Tap **Set up** to choose which devices will be disconnected from the network when Away Mode is enabled:




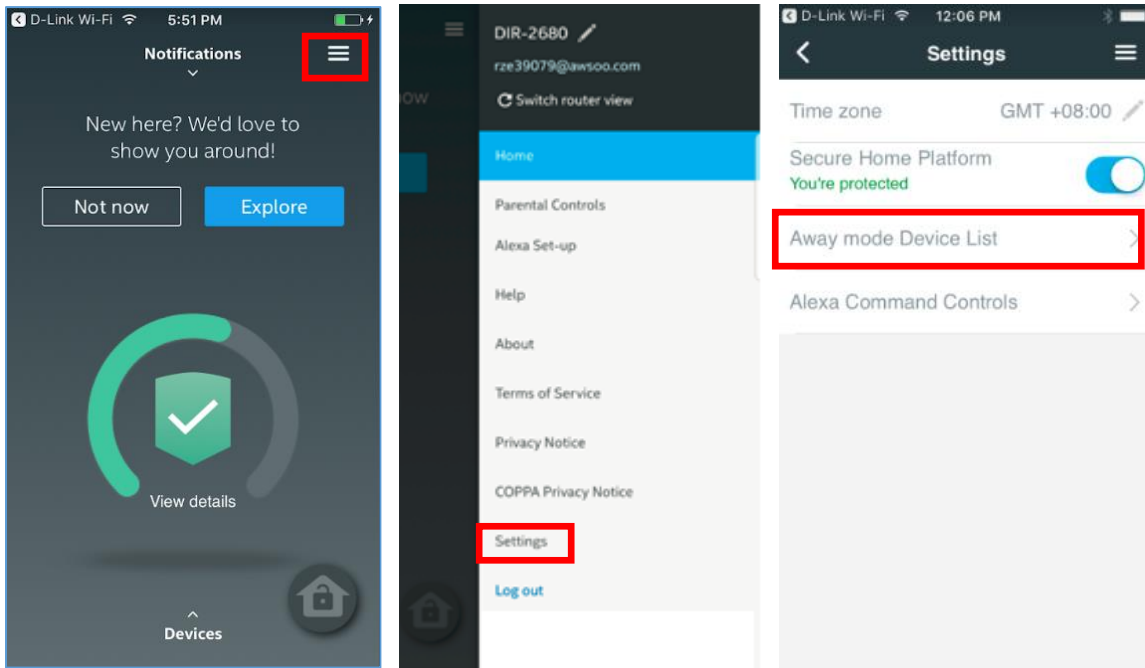
Step 3: Add devices in the Away Mode list and then tap ✓ to continue.



Step 4: If you want to turn on Away mode now, tap **Turn on**. Or tap **Close** to turn it on later.



Step 5: If you want to manage devices from the Away Mode list, tap  in the upper right corner, select **“Settings”**. Then tap **“Away mode Device List”**.



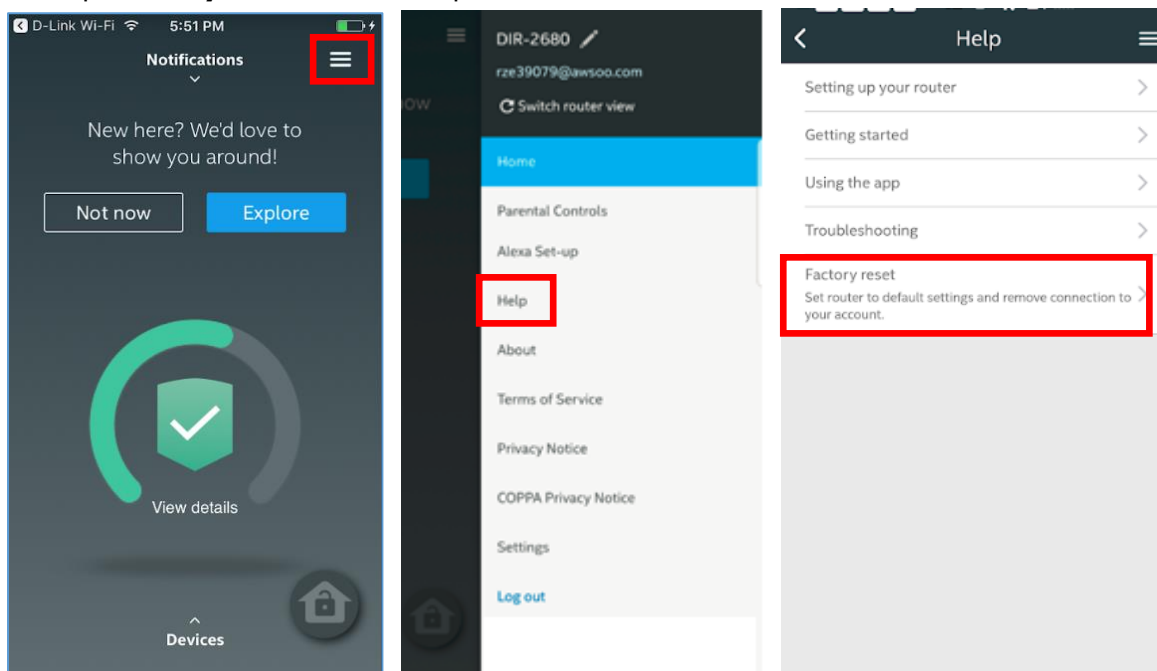
13-26: How do I perform factory reset in the D-Link defend app?

There are 2 ways to carry out factory reset. Please note that performing a factory reset will:

- Remove all SHP settings like devices, kids' profiles, etc. from the router and the McAfee cloud.
- Forces a logout for the parent on the D-Link defend app.

Note: Parents can still use the same email address to re-install their router and enable the McAfee SHP services.

1. Tap **Factory Reset** in the Help Menu.



13-27: What features are available for SHP devices?

This table shows what features are available for SHP devices:

Devices	Block	Forget Device	Parental Controls	Device Status	Detect AV	Block Page on Device	Sends Admin Notifications if Accesses Malicious Site
Mobile Phone	Y	Y	Y	Y	Y	Y	N
Tablet	Y	Y	Y	Y	Y	Y	N
Personal Computer	Y	Y	Y	Y	Y	Y	N
Thermostat	Y	Y	Y	Y	N	N	Y
Game Console	Y	Y	Y	Y	N	N	Y
TV	Y	Y	Y	Y	N	Y	N
Camera	Y	Y	Y	Y	N	N	Y
Media Devices	Y	Y	Y	Y	N	N	Y
Lights	Y	Y	Y	Y	N	N	Y
Switch and Sockets	Y	Y	Y	Y	N	N	Y
Locks	Y	Y	Y	Y	N	N	Y
Other IoT Devices	Y	Y	Y	Y	N	N	Y
Generic	Y	Y	Y	Y	Y	Y	N

Note: AV: Anti-Virus.

13-28: Can I remotely control the D-Link defend app of my SHP-enabled router?

Yes, you can directly launch D-Link defend app when you're outside of your home and have mobile network only. Launching D-Link defend from D-Link Wi-Fi is only required for the 1st time setup. You can remotely manage the D-Link defend app afterwards.

13-29: If your network uses IPv6 only, would SHP work correctly on SHP-enabled router?

Yes, if your network **only** uses IPv6, our security products will still work properly.