Dojo by BullGuard-DL0007

User’s Guide

9 Devonshire Square EC2M 4YF London. United Kingdom
Company website: dojo.bullguard.com
For information, contact: info@dojo-labs.com
For support, contact: helpdesk@dojo-labs.com
May 2017

Table of Contents

Overview

*This manual is addressed for ISPs' consumer base. All sections mentioning Wi-Fi connections are referring to the user's home router.

Congratulations on your Dojo, the smart security and privacy solution for your smart connected home!

Dojo keeps you in control of your home network and privacy by monitoring your home router and alerting you of new devices trying to connect. Dojo provides a security technology that connects to your network and acts as the essential layer between your smart devices and any threats to your security and privacy.

If any suspicious device tries to connect to your home router, Dojo will notify you via the Dojo app (available for Android and iOS) and you can simply block it.

This guide provides instructions for connecting the Dojo system to your home network and using the Dojo app to monitor and control devices in the network.

Dojo Technology

Dojo is a comprehensive and in-depth security system for smart devices and connected homes. It has three main components:

- **Dojo Base Unit**: A local intelligent unit that plugs into your router and takes care of threat detection and prevention alongside network management and control. Dojo constantly analyzes all the network traffic within the home network and enforces the security policy of that specific network.
- **Dojo Cloud Service:** Dojo-Labs runs a cloud-based cybersecurity engine that constantly collects and analyzes the metadata that has been generated by all the deployed Dojos devices. The collected data is then applied to thousands of other smart homes using Dojo, to prevent similar attack from being carried out.
- **Dojo Mobile App:** The Dojo application is the main interface for using the service. It provides an intuitive user interface that provides users with alerts if a security incident is identified, as well as options on what action they can take if required. Using the app does not require any technical knowledge.

The solution is built of technologies that provide comprehensive security and privacy solution for all connected devices:

1. **Automatic Device Discovery:** Dojo automatically discovers all the devices connected to the home router and assigns them to the appropriate security groups. This enables Dojo's Intelligent Platform to tailor a specific profile for each device as well as enforce a security and privacy policy.

2. **Smart Managed Firewall:** Dojo has smart firewall capabilities, keeping the home router and smart connected devices secured from any malicious activity and hacking attempts.

3. **Smart Managed IDPS:** Dojo uses a managed enterprise-grade intrusion detection and prevention system. Its smart IDPS is constantly updated with the latest threat detection packages, specifically tailored to meet IoT related vulnerabilities and threats.

4. **Secure Web Proxy:** Dojo uses a managed secure web proxy capable of interacting with the other components, enabling secure and private web access to all the smart devices connected to the user's home router.

5. **Smart Vulnerability Scanner:** Dojo continuously and actively scans the home route rand connected devices, detecting potential risks and vulnerabilities. The security profile is updated with the outcome of this process and constantly enhances the device protection.

6. **Behavioral Analysis:** Dojo constantly monitors and analyzes the home router and connected devices. The Dojo Cybersecurity Engine is based on cutting-edge Artificial Intelligence and Machine Learning technology using sophisticated algorithms for anomaly detection and behavioral analysis.

Further Information

In addition to this guide, the following resources are available for information:

- A Quick Start Guide is included in the Dojo Pebble kit.
- FAQs on company website at: www.dojo.bullguard.com.

If you experience technical difficulties, contact the support team at: helpdesk@dojo-labs.com

Setup

This chapter describes how to set up the Dojo network, install the Dojo app, register to the Dojo service and discover the devices in your network.

Before You Start

Before you begin to set up the Dojo Pebble, ensure that you have the following:

- Dojo Mobile App for smartphones.
  Download via App Store or Google Play
  Four AA batteries
- Router admin credentials
- Turned on your smartphone's Bluetooth*
  *Bluetooth connection is used only for first-time installation and for Pebble and Base Unit communications.

Unpacking the Dojo Pebble Kit

The Dojo Pebble Kit includes the following items (see Figure 1):

- Dojo Pebble
- Dojo base unit
- Quick Start Guide
- Ethernet cable
- AC adapter

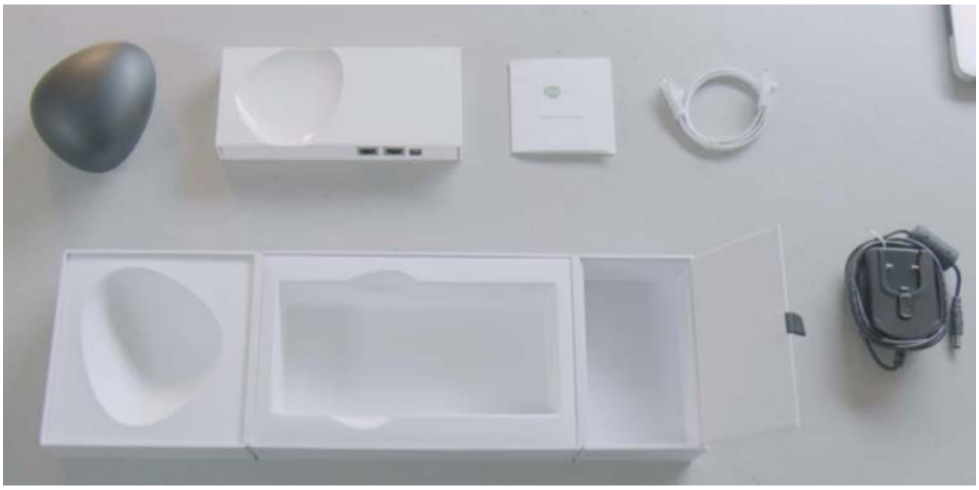


Figure 1: Dojo Pebble kit

Setting Up Dojo

There are four general steps in the setup:

Step 1: Connecting the Dojo Base Unit to the Router
Step 2: Downloading and Installing the Dojo App on your Smartphone
Step 3: Powering on the Dojo Pebble
Note: Please press for 3 seconds on the Pebble power button for it to turn on

Step 4: Registering a New Dojo User and Pairing the Dojo App with the Dojo Base Unit

Step 1: Connecting the Dojo Base Unit to the Router

There are two modes for connecting the Dojo base unit to the router, depending on the way your home network is set up:

- **Router Mode**: When using your service-provider router only. The connections look like this:

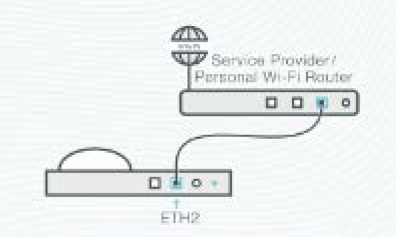
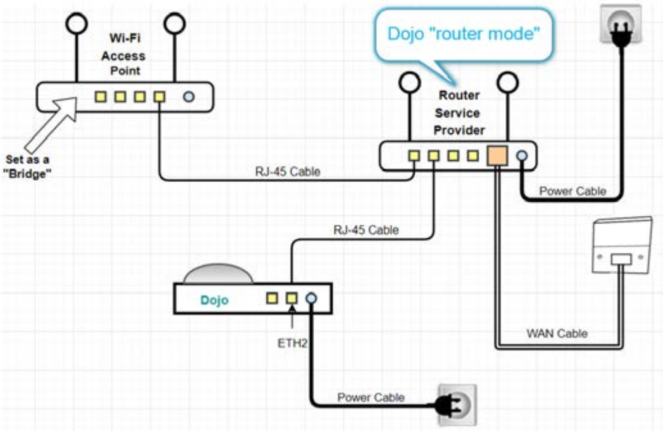


Figure 2: Router setup

- **Bridge Mode**: Currently unavailable.
When using both your service-provider router and an additional home router. The connections look like this:



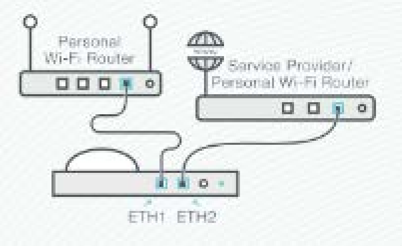


Figure 3: Bridge setup

It is important to understand which setup your network uses, both for the physical setup and software configuration.

Router Mode

1. Plug the AC adapter into the Dojo Base Unit as shown in Figure 4, then connect the adapter to a power outlet.

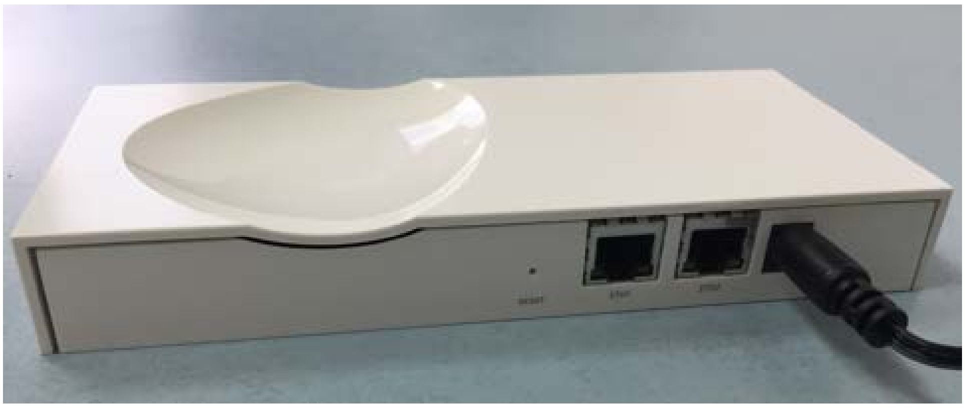


Figure 4: Router mode power connection

2. Plug one end of the Ethernet cable into the **ETH2** port of the Dojo Base Unit, as shown in Figure 5, then plug the other end into an available port in the router.

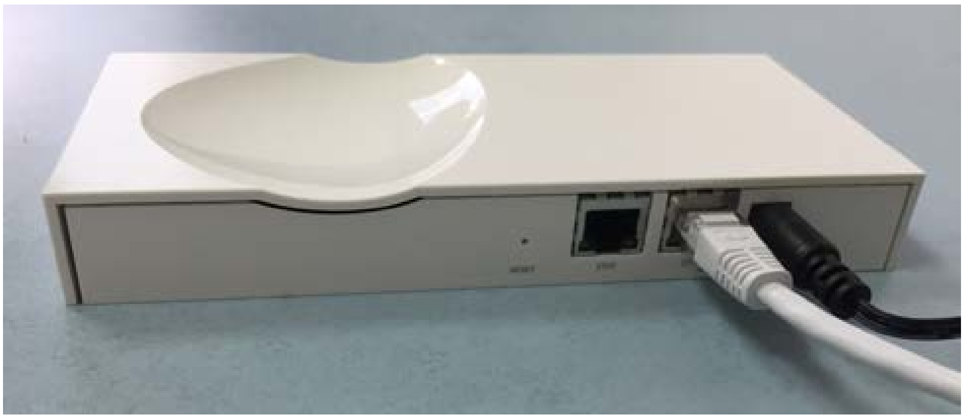


Figure 5: Router mode network connection

Wait a few minutes before you continue with the setup.

Bridge Mode

1. On the home router side, unplug the cable connecting the home router to the service-provider router.
2. Plug one end of the Ethernet cable that was provided in the Dojo kit into the **ETH2** port of the Dojo Base Unit. Plug the other end into the same port of the home router from which you unplugged the cable in step 1. See Figure 6.
3. Plug the AC adapter into the Dojo Base Unit and connect the adapter to a power outlet. See Figure 6.

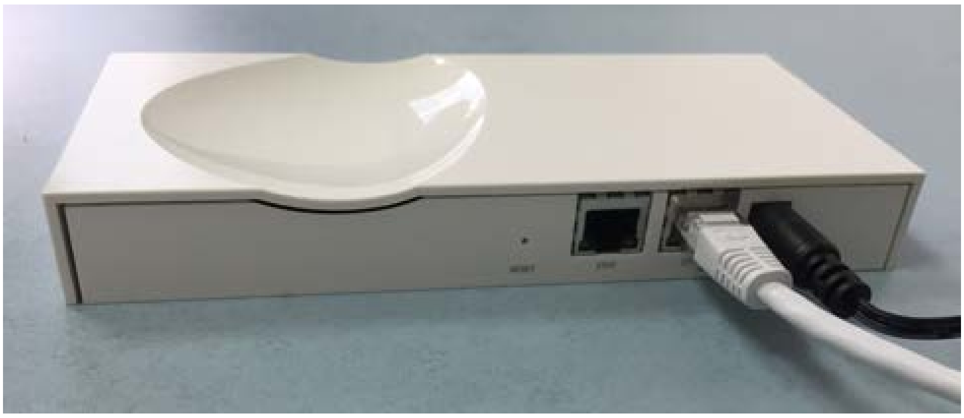


Figure 6: Power and ETH2 connections

4. Plug the Ethernet cable that you unplugged in step 1 into the **ETH1** port.

Wait a few minutes before you continue with the setup.

Step 2: Downloading and Installing the Dojo App on your Smartphone

To download the Dojo app, scan the QR code in the Quick Start Guide. You will be transferred to the Google Play Store or Apple Store, depending on your device.

Step 3: Powering on the Dojo Pebble

1. Turn the Pebble over, so that the Dojo logo is visible.
2. Slide the battery cover off in the direction of the arrows, to expose the battery holder.
3. Insert four AA batteries into the battery holder. Ensure they are aligned properly. Close the battery cover.
4. Turn on the Pebble: Press and hold down the button located next to the Dojo logo for 3 long seconds.

Red, Green, and Blue circles flash to indicate that the Pebble is powering on.

5. Turn the Pebble right-side up.

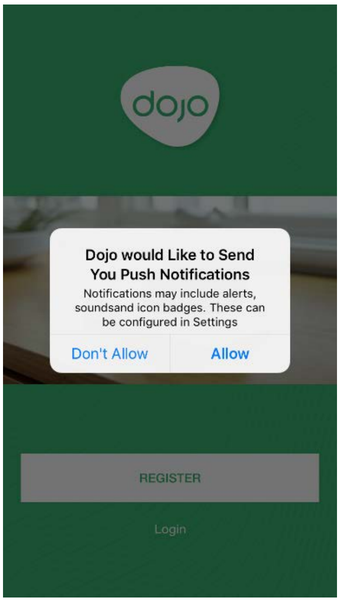
The hollow in the base unit is designed to hold the Pebble. Place it there, or anywhere within five meters of the base unit.

Step 4: Registering a New Dojo User and Pairing the Dojo App with the Dojo Base Unit

Register your username and pair the Dojo app with the Dojo Base Unit.

As you perform the following procedures, make sure you are within five meters of the Dojo Base Unit.

1. Open the Dojo app.



Dojo would Like to Send You Push Notifications

Notifications may include alerts, soundsand icon badges. These can be configured in Settings

Figure 7: Push notifications screen

2. Select **Allow** push notifications to receive alerts from Dojo.
3. Select **Register**.

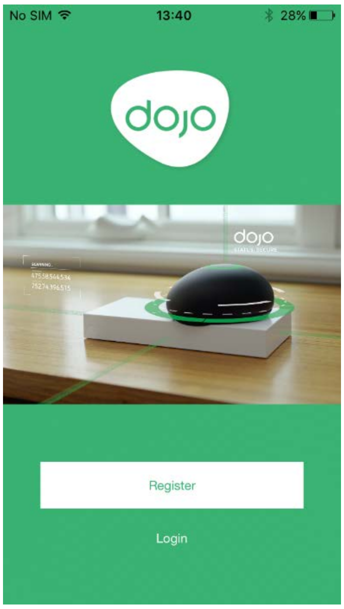
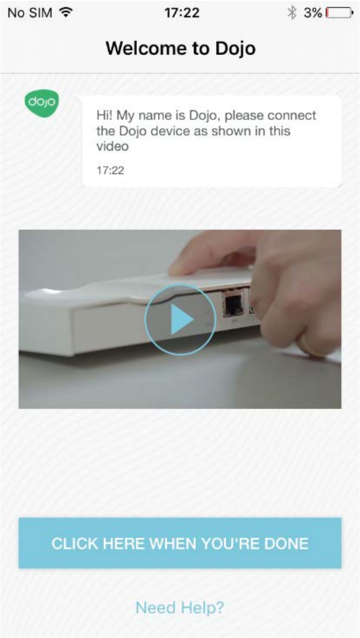


Figure 8: Registration screen

4. Select **Register**.

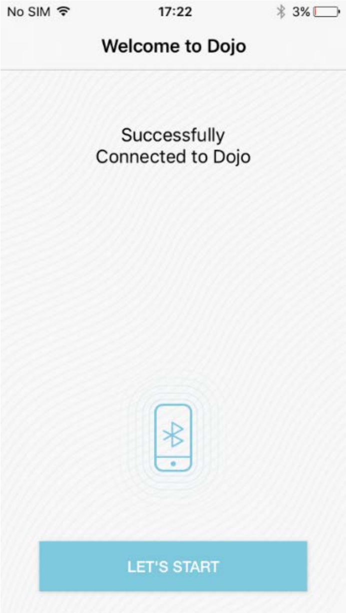


Hi! My name is Dojo, please connect the Dojo device as shown in this video

17:22

Figure 7: Welcome screen

If you have already performed the instructions in the previous step-Connecting the Dojo Base Unit to the Router, on page 6, touch **Click Here When You're Done**. Wait for the app to display **Successfully connected to Dojo**.



Successfully Connected to Dojo

Figure 10: Successful Dojo connection screen

5. Select **Let's Start** to begin registration**.**

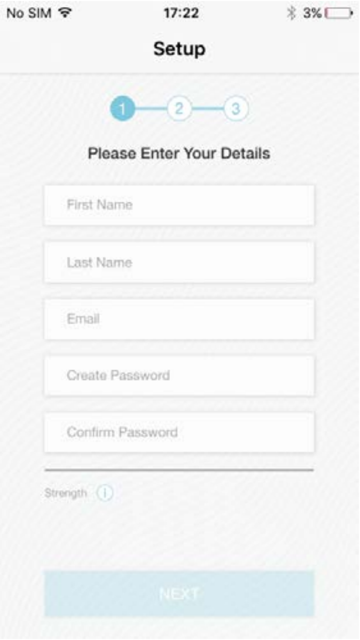
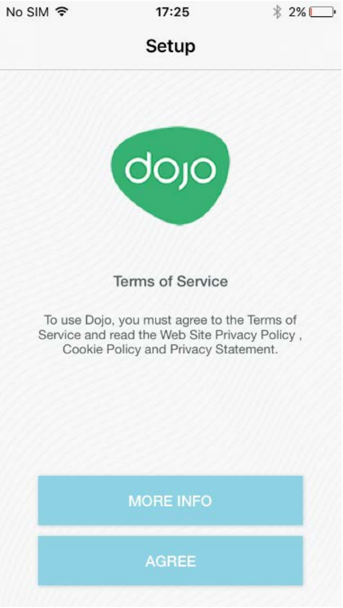


Figure 8: Personal details screen

6. Enter your first name, last name, email, and a password. Enter the password again in the second field.

> **Note**: The email is also used as your username and cannot be changed once the Dojo is registered. Make sure you are satisfied with the email address that you are going to enter.

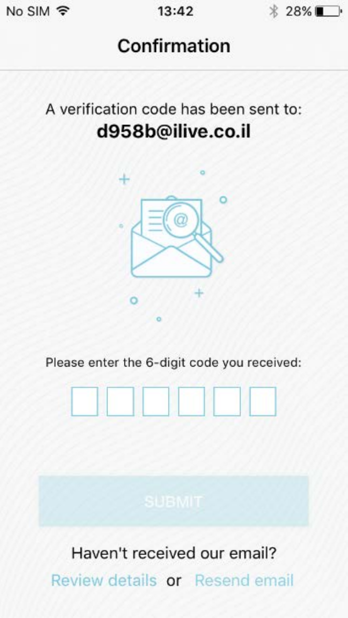
7. iPhone users: To enable sign in with Touch-Id, select the **Allows login with Touch ID** check box.
8. Touch **Next** to proceed.



To use Dojo, you must agree to the Terms of Service and read the Web Site Privacy Policy , Cookie Policy and Privacy Statement.

Figure 9: Terms and policy screen

9. Touch **Agree** to continue with the setup.



A verification code has been sent to:
d958b@ilive.co.il

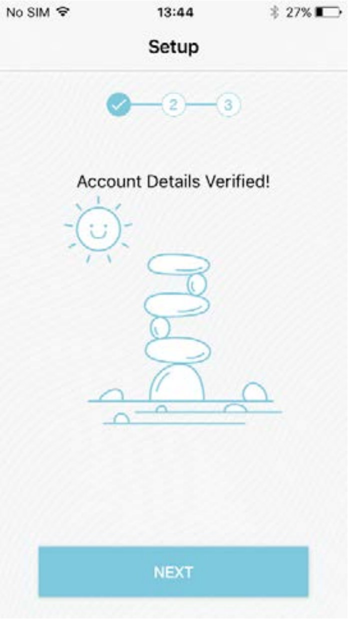
Please enter the 6-digit code you received:

□□□□□□

Haven't received our email?
Review details or Resend email

Figure 10: Confirmation screen

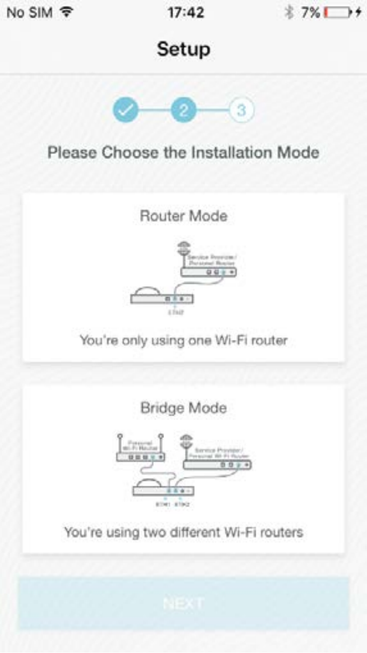
10. Check your email for a message that contains a six-digit PIN code. Enter the PIN code into this screen, then select **Submit**.



Account Details Verified!

Figure 11: Account verification screen

11. Select **Next**.


No SIM
17:42
7%
Setup
1
2
3
Service Provider/ Personal Router
Personal Wi-Fi Router
Service Provider/ Personal Wi-Fi Router
NEXT

Please Choose the Installation Mode

Router Mode

You're only using one Wi-Fi router

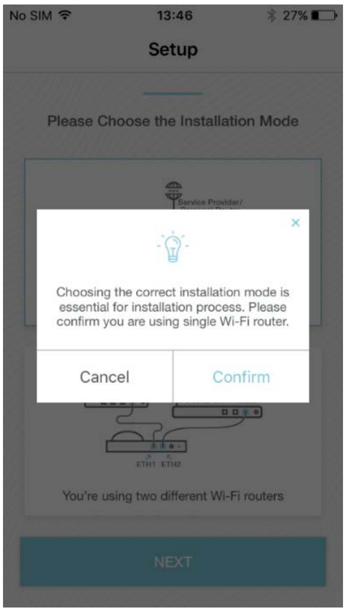
Bridge Mode

You're using two different Wi-Fi routers

Figure 15: Installation mode screen

In this screen, you may select either **Router Mode** or **Bridge Mode**, according to the network configuration you set up earlier:

12. Select a mode, then touch **Next**.



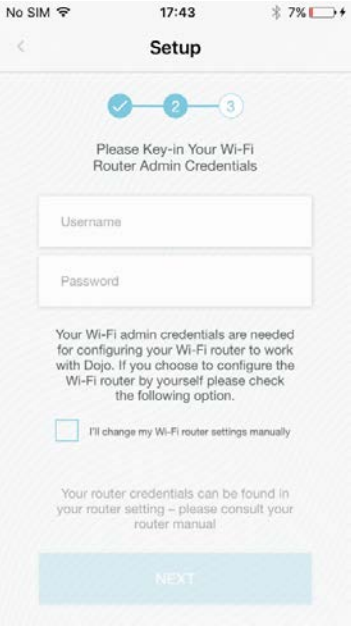
Please Choose the Installation Mode

Choosing the correct installation mode is essential for installation process. Please confirm you are using single Wi-Fi router.

You're using two different Wi-Fi routers

Figure 12: Installation mode confirmation screen

13. Confirm or cancel your selection.



Please Key-in Your Wi-Fi Router Admin Credentials

Your Wi-Fi admin credentials are needed for configuring your Wi-Fi router to work with Dojo. If you choose to configure the Wi-Fi router by yourself please check the following option.

□ I'll change my Wi-Fi router settings manually

Your router credentials can be found in your router setting – please consult your router manual

Figure 13: Home Router admin screen

14. In this screen, you may select one of the following options:

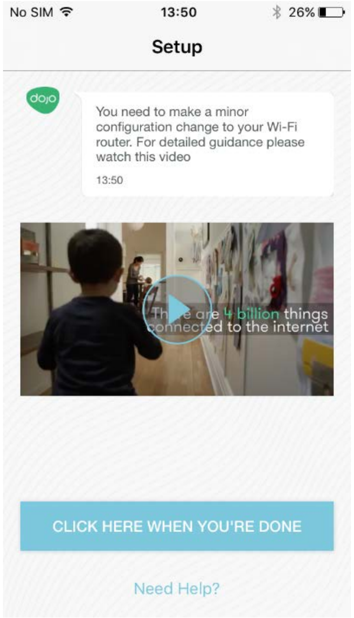
- Let Dojo set your router remotely. In this case, enter your home router admin credentials.

  OR

- Change the home router setting manually, on your own. In this case, you do not enter the credentials, and instead, select the check box next to **I'll change my home router settings manually**.

  > **Note**: If you select this option, you must access your home router to disable the DHCP server manually. You will need to restart it and any Internet switch or bridge that you may have in your home network. For instructions, see Disabling the DHCP Server Manually, on page 16.

15. Select **Next** to complete the setup.
16. If you chose to disable the DHCP manually, you will see the following screen:

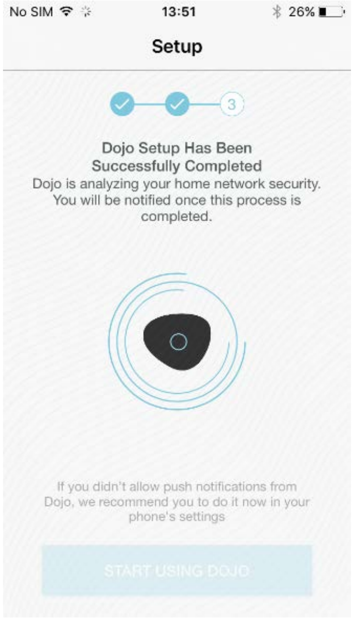


No SIM
13:50
26%
Setup
dojo
There are 4 billion things connected to the internet
CLICK HERE WHEN YOU'RE DONE
Need Help?

You need to make a minor configuration change to your Wi-Fi router. For detailed guidance please watch this video
13:50

Figure 18: DHCP configuration notification screen

Make the necessary configuration in your router, then touch **Click Here When You’re Done** to proceed.

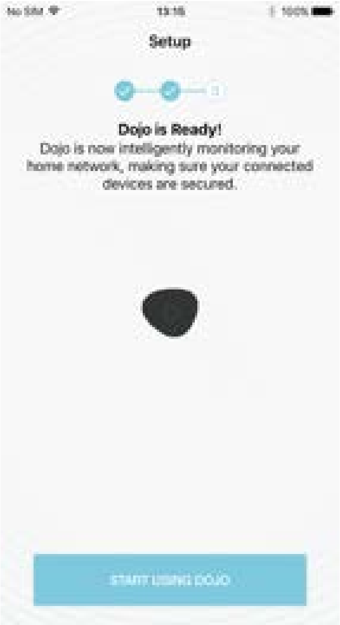


Dojo Setup Has Been Successfully Completed
Dojo is analyzing your home network security. You will be notified once this process is completed.

If you didn't allow push notifications from Dojo, we recommend you to do it now in your phone's settings

Figure 19: Dojo is analyzing network screen

17. Dojo begins to analyze your network. *This process may take several minutes*. When Dojo completes the analysis, a notification will be sent to your smartphone and the following screen is will be displayed.



Dojo is Ready!

Dojo is now intelligently monitoring your home network, making sure your connected devices are secured.

Figure 14: Dojo is ready screen

In addition, the Pebble will blink with a Green light.

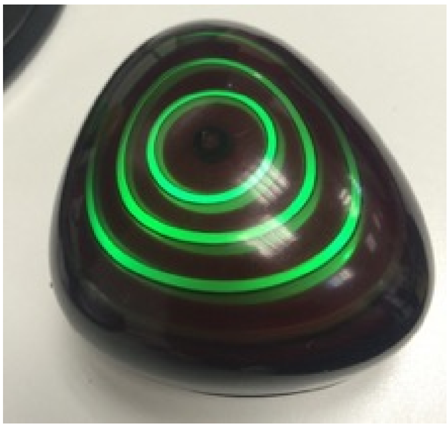


Figure 15: Pebble: ready state

Disabling the DHCP Server Manually

Perform the following procedures only if you chose the option **I'll change my home router settings manually** at the end of the process for registering a New Dojo User and Pairing the Dojo App with the Dojo Base Unit, on page 8.

1. Log into the home router admin page.
2. Disable the DHCP server.
3. Apply the changes.
4. Restart the router.

Discovering Devices in Your Network

Once the Dojo Base Unit is activated and ready, it scans your home network to discover all connected devices.

Note: For Dojo to detect and manage all your devices, ensure that you have restarted the Internet switch, or other home router access points that you may have in your home network.

As devices are discovered, they are displayed in the **My Devices** tab. A push notification about each one is also sent and an event is added to the chat.

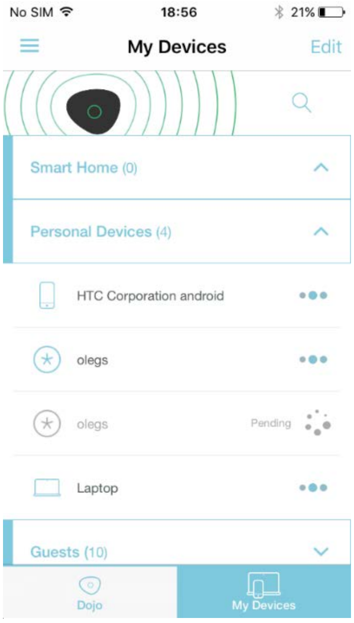


Figure 21: My Devices tab

Note: Dojo places a new device in the Guests group until you move it into another group.

Using the Dojo App

This chapter will guide you on how to use the Dojo app.

Logging In

When you access the app, you are required to log in.

1. Select **Login**.

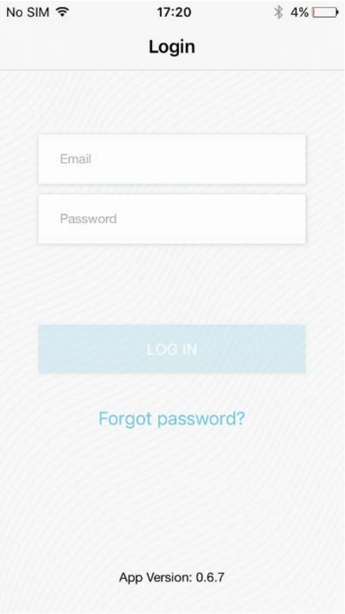


Figure 16: Login screen

2. Enter your username and password.
3. Select **Login**.

The **Dojo** tab is displayed.

Dojo Tab

The Dojo tab is the main screen of the app and shows the recent activity relating to devices in your network. The activity is communicated to you via the Dojo Bot in the form of chat.

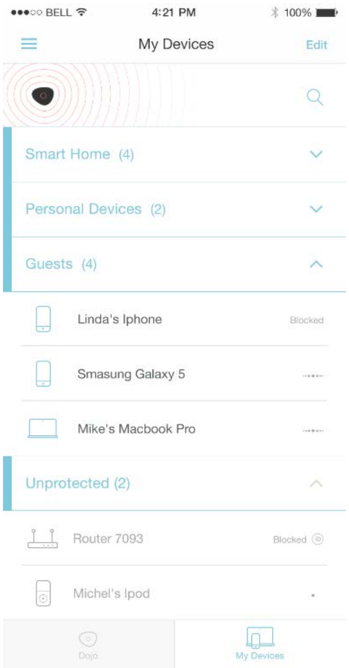
There are three types of messages from Dojo:

- **Red notifications**: Alerts about threats to your network and requires you to take action.
- **Orange notifications**: Signifies that Dojo has handled a threat on your network. You are not required to do anything.
- **Green notifications**: Dojo is continuously monitoring your network, and all well is done.

Your interactions with Dojo previewed as a message in a grey block:

My Devices Tab

In this tab, you can view all the devices that Dojo has identified in your home network.



●●●○○ BELL 4:21 PM 100%

My Devices Edit

Smart Home (4)

Personal Devices (2)

Guests (4)

Linda's Iphone Blocked

Smasung Galaxy 5

Mike's Macbook Pro

Unprotected (2)

Router 7093 Blocked ip

Michel's Ipod

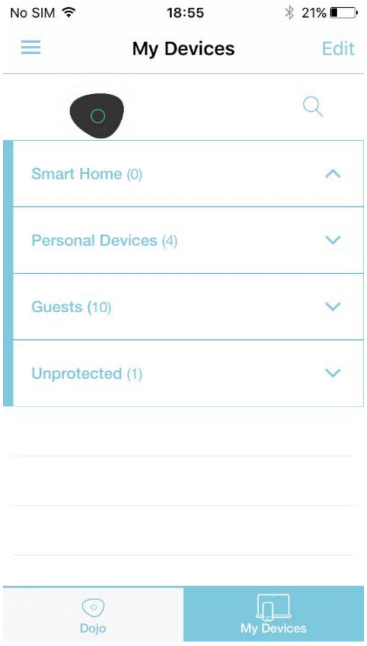
Dojo My Devices

Figure 23: My Devices tab

Each device has the following markings:

- Device name
- Device type. For example, a router has the following icon: .
- Device activity. An active device is marked with three moving dots: ••• ; an inactive device is marked with three static dots.
- A blocked device is marked Blocked .
- A device that uses a static IP is marked ip .

Every detected device is located in one of four groups: Smart Home, Personal Devices, Guests, and Unprotected. You can collapse and expand the devices in a group. In this example, the first three groups are in a collapsed state:



No SIM 18:55 21%

My Devices

Edit

Smart Home (0)

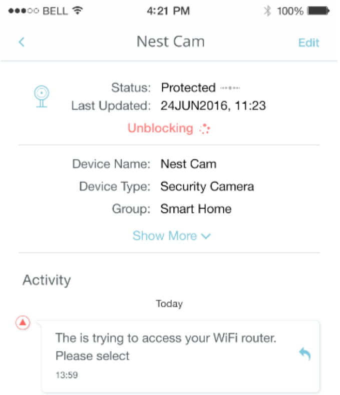
Personal Devices (4)

Guests (10)

Unprotected (1)

Figure 24: Collapsed device group

- By touching a specific device, you can see detailed information about it (at the top of the screen), as well as the recent Dojo monitoring activity relating to the device (at the bottom of the screen).



●●●○○ BELL 4:21 PM 100%

Nest Cam

Edit

Status: Protected
Last Updated: 24JUN2016, 11:23
Unblocking

Device Name: Nest Cam
Device Type: Security Camera
Group: Smart Home

Show More

Activity

Today

The is trying to access your WiFi router. Please select
13:59

Figure 17: Device details

- The **Edit** button lets you edit details of the device so that they are more easily understood or recognized.

Device Groups

Devices that have been discovered by Dojo are sorted into groups.

Each group has particular characteristics and capabilities. By placing a device in a particular group, you define how it interacts with others in that group, how it accesses the Internet, and how the Internet interacts with it.

The following groups are available:

Smart Home Group

The following are the characteristics and behaviors of the devices in the Smart Home group:

- Devices in the Smart Home group ate protected buy the Dojo Base Unit. They are protected against malicious web pages, unauthorized access from other networks, malware, Trojans, and so forth.
- Usually, you would place your smart home devices, such as cameras, door locks, and alarm systems in this group.
- It is possible to open external ports from the Internet to devices in the Personal Devices group, for example, setting port forwarding for remote access to your camera. See Protecting a Device with Remote Access, on page 29.

Personal Devices Group

The following are the characteristics and behaviors of the devices in the Personal Devices group:

- Devices in the Personal Devices group are protected by the Dojo Base Unit. They are protected against malicious web pages, unauthorized access from other network, malware, Trojans, etc.
- Devices in the Personal Devices group are allowed to access and configure the router.
- Usually, you would place your smartphones, mobile devices, tablets, PCs, Mac, laptops, and other advanced devices in this group.
- It is possible to open external ports from the Internet to devices in the Personal Devices network, for example, see Protecting a Device with Remote Access, on page 29.

Guests Group

The following are the characteristics and behaviors of the devices in the Guests group:

- Access to the Internet is unrestricted. Devices in this group can access any website.
- The guest group is not protected from malware, Trojans, malicious websites, and so forth.
- Devices are not allowed to access other devices in the Personal Devices and Smart Home groups.
- Devices are not allowed to configure the router.

Unprotected Group

The following are the characteristics and behaviors of the devices in the unprotected group:

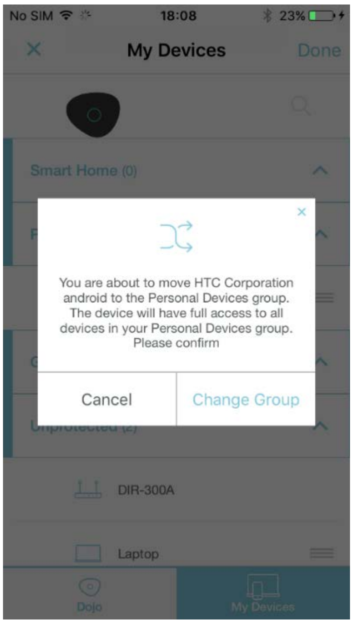
- Devices with static (manual) IP addresses of the router network are placed automatically in this group.
- Once you change the IP address or a device from static (manual) to DHCP-assigned, the device moves into the Guest group.
- Devices in the unprotected group cannot be moved to other groups.
- Access to the Internet is unrestricted, and the devices can access any website.
- Devices in the unprotected group are not protected from malware, Trojans, malicious websites and so forth.
- Devices are not allowed to access other devices in the Personal and Smart Home groups.
- Devices are not allowed to configure the router.
- To enable a device to bypass Dojo entirely, you can move it from its current group to the Unprotected group.

Changing Groups

You can change the group to which a device belongs. There are two ways to do this: by dragging it to a different group, or by editing the device details.

By Dragging a Device

1. Select the **My Devices** tab.
2. Select **Edit**.
3. Drag the required device from one group to the other, by holding down its drag handle.



You are about to move HTC Corporation android to the Personal Devices group. The device will have full access to all devices in your Personal Devices group. Please confirm

Cancel | Change Group

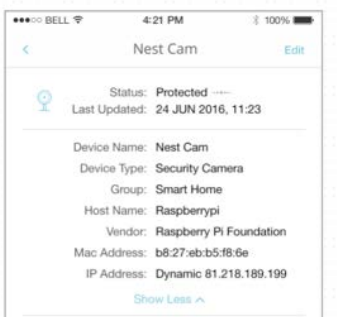
Figure 25: Group move confirmation

4. Select Change Group of Cancel.
5. Select **Done**.

Note: The device will be under pending status until it has been moved successfully to its new group. This may take up to five minutes.

By Editing

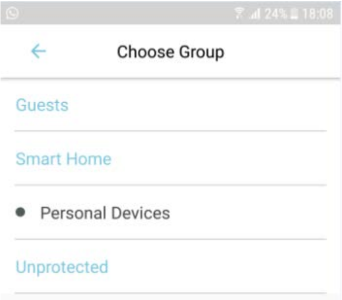
1. Select the device, and its details will be displayed. Select **Edit**.



Status: Protected
Last Updated: 24 JUN 2016, 11:23
Device Name: Nest Cam
Device Type: Security Camera
Group: Smart Home
Host Name: Raspberrypi
Vendor: Raspberry Pi Foundation
Mac Address: b8:27:eb:b5:f8:6e
IP Address: Dynamic 81.218.189.199

Figure 26: Editing device details

2. Select the arrow next to **Group**.



Choose Group

Guests

Smart Home

● Personal Devices

Unprotected

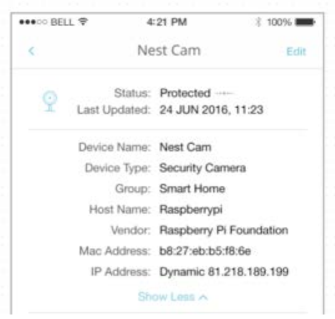
Figure 27: Choose Group screen

3. You will be displayed a list of groups. Select the group to which you want to move the device.
4. Touch **Save** to apply the changes

Editing Device Details

You can modify device details as follows:

1. In the **My Devices** tab, select the device to display its details.
2. Select **Show More** to display more details.
3. Select **Edit** in the top-right corner.



Nest Cam Edit

Status: Protected
Last Updated: 24 JUN 2016, 11:23

Device Name: Nest Cam
Device Type: Security Camera
Group: Smart Home
Host Name: Raspberrypi
Vendor: Raspberry Pi Foundation
Mac Address: b8:27:eb:b5:f8:6e
IP Address: Dynamic 81.218.189.199

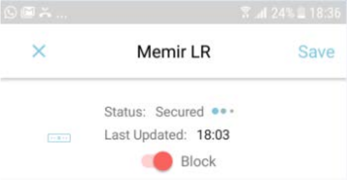
Show Less

Figure 28: Editing device details

4. Edit settings as needed.
5. Select **Save** to apply the changes.

The following are the device details you can edit:

- **Block**: This switch lets you block or unblock the device from the network. A blocked device cannot communicate with other devices and has no access to the Internet.



Memir LR Save

Status: Secured
Last Updated: 18:03

Block

Figure 29: Block switch on

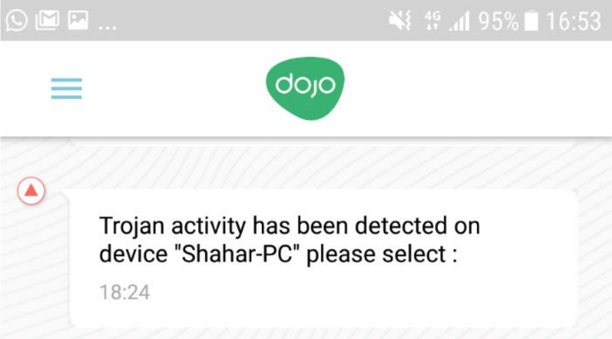
- **Device Name**: Dojo displays the default device name. To change it, select the name and edit as needed.
- **Device Type**: Dojo displays the default device type. To change it, select the arrow next to the device type. Select a different device type from the list displayed.

- **Group**: Dojo places all new devices in the Guests group until you move it into another group. To move it, Select the arrow next to the group name. Select the new group from the list displayed.
- **IP Address**: Dojo displays the current IP address of the device and indicates whether it is static or dynamic. By default, IP addresses are dynamic. If you choose to use a static IP address, Dojo will permanently assign the same IP address to this device. This is important when you need to access the device either remotely or internally by its IP address. To modify the type of IP address, Select **Static** or **Dynamic**.
- **Remote access**: Dojo displays whether remote access is allowed or blocked for the device. To allow, Select **Yes** and to block, Select **No**. When you select **Yes**, you must provide the external IP address, the internal IP address, and network protocol (UDP or TCP) to use. For more instructions, see Protecting a Device with Remote Access, on page 29.

Alerts and Actions

Dojo protects you both from inside and outside your network by alerting you on unusual activity:

- **Red alerts**: These messages require you to act. A Red event typically occurs when an unauthorized device is attempting to access the network or during a malicious attack. In the event of a Red alert, a Red activity message is communicated by the Dojo Bot via the Dojo app, and the Pebble lights up in Red.



Trojan activity has been detected on device "Shahar-PC" please select :

18:24

Figure 30: Alert message

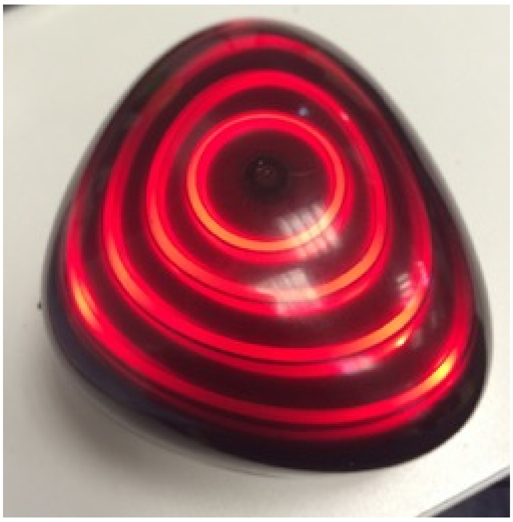


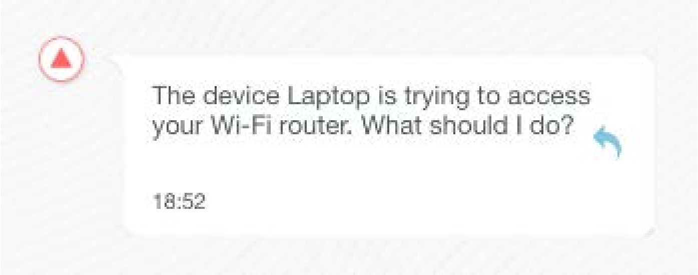
Figure 31: Pebble: alert state

You must respond to every Red alert with a specific action. Once you select an action, it is recorded as an activity in the Dojo Tab.

- **Orange notifications**: These messages merely inform you that the Dojo service has handled the event. In the event of an Orange alert, an orange activity message is communicated by the Dojo Bot via the Dojo app, and the Pebble lights up in Orange.

Example of Alerts and Actions

In the event of an unauthorized attempt of a device to access your network, a Red alert is communicated via the Dojo Bot. This is how it looks on the Dojo app:



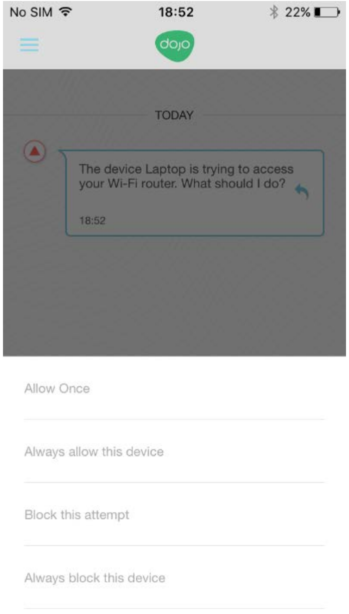
The device Laptop is trying to access your Wi-Fi router. What should I do?

18:52

Figure 32: Alert – example

To handle the alert:

1. Touch the notification. A popup will appear, displaying the following possible actions:



The device Laptop is trying to access your Wi-Fi router. What should I do?

18:52

Allow Once

Always allow this device

Block this attempt

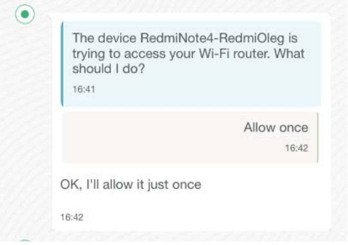
Always block this device

Figure 33: Actions - example

- **Allow once:** This action allows the device temporary access to the home router. If another attempt to gain access is made later, you will be notified again.
- **Always allow this device:** This action allows the device to permanently access the home router. Once the action is allowed, you will not be notified again about the specific device, and it will always be allowed to access the router.
- **Block this attempt:** This action temporarily blocks the device from accessing the home router. If another attempt to gain access is made later, you will be notified again.

- **Always block this device:** This action blocks the device from permanently accessing the home router. Once the action is blocked, you will not be notified again about the specific device, and it will always be blocked from accessing the router.

2. For example, if **Allow Once** is selected, Dojo displays your selection, then follows up with a confirmation:



The device RedmiNote4-RedmiOleg is trying to access your Wi-Fi router. What should I do?
16:41

Allow once
16:42

OK, I'll allow it just once
16:42

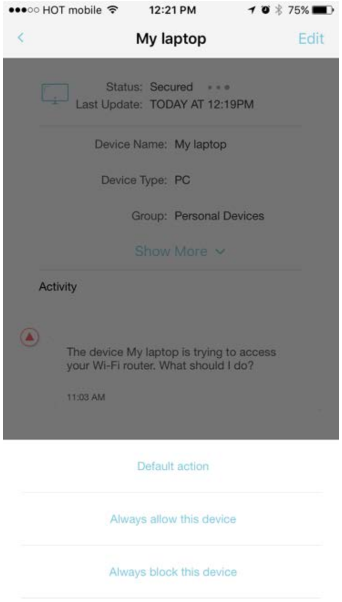
Figure 34: Dojo alert and action messages - example

Removing an Action from a Device

If you apply a permanent action such as **Always block this device** to a particular device, Dojo retains the policy for that device until you change it.

To change the policy for a device:

1. Select the device.
2. Select the action from the list that appears.



Status: Secured
Last Update: TODAY AT 12:19PM
Device Name: My laptop
Device Type: PC
Group: Personal Devices

The device My laptop is trying to access your Wi-Fi router. What should I do?
11:03 AM

Figure 35: Removing an action from a device

Dojo Menu

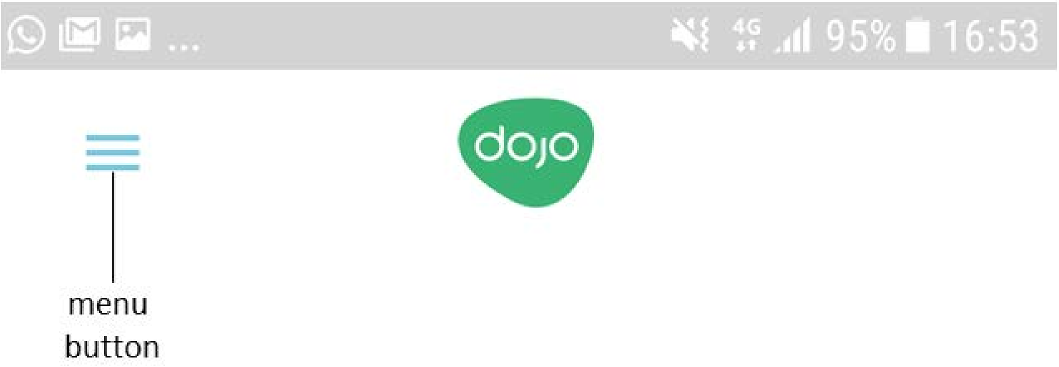


Figure 36: Menu button

Select the **Menu** button in the top left corner of the app to access your Dojo account, Dojo app settings, and online help and support.

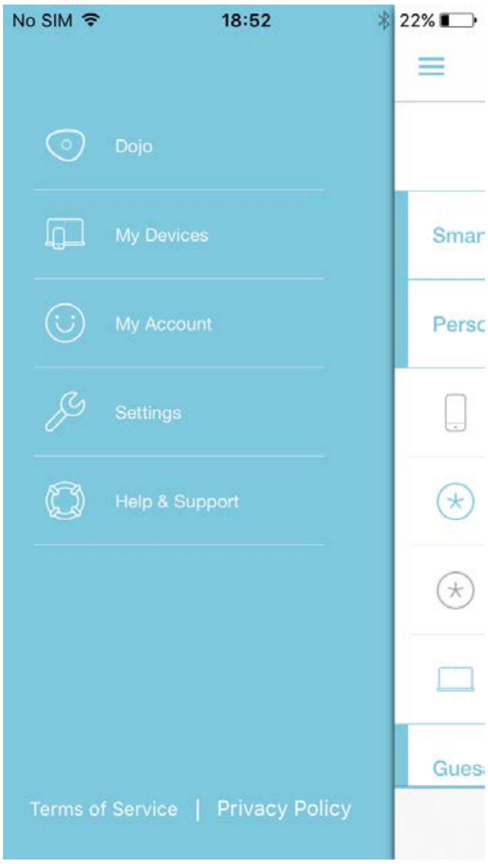
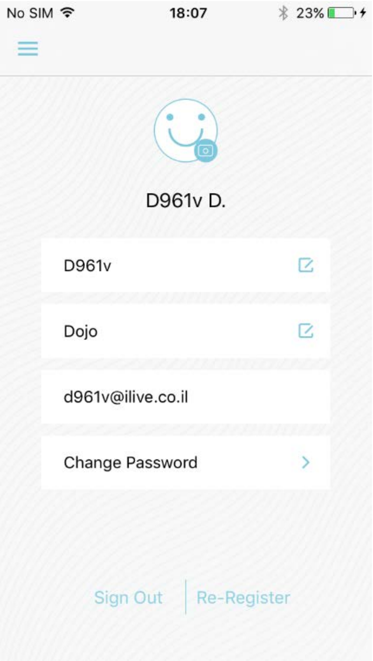


Figure 37: Dojo menu

- Select **Dojo** to display the **Dojo** tab (main screen).
- Select **My Devices** to display the **My Devices** tab.
- Select **My Account** to display details of your Dojo account, where you can also change your username and password.



D961v D.

D961v

Dojo

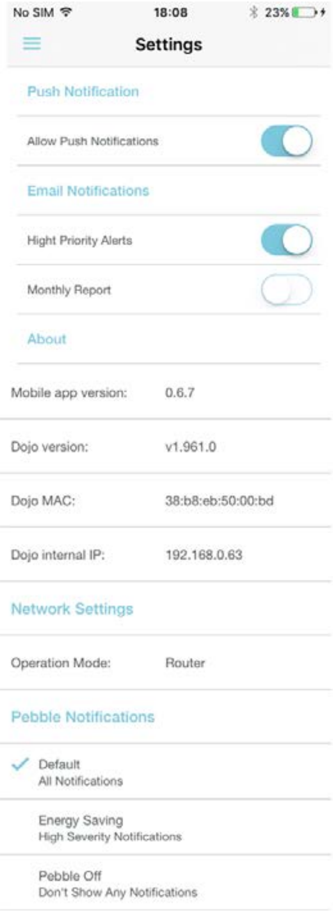
d961v@ilive.co.il

Change Password

Sign Out | Re-Register

Figure 38: My Account screen

- Select **Settings** to display a screen where you can change Dojo app settings.



Settings

Push Notification

Allow Push Notifications ●

Email Notifications

Hight Priority Alerts ●

Monthly Report ○

About

Mobile app version:	0.6.7
Dojo version:	v1.961.0
Dojo MAC:	38:b8:eb:50:00:bd
Dojo internal IP:	192.168.0.63

Network Settings

Operation Mode:	Router

Pebble Notifications

✓ Default
All Notifications

Energy Saving
High Severity Notifications

Pebble Off
Don't Show Any Notifications

Figure 39: Dojo app settings screen

- Select **Help/Support** to display the Dojo Help and Support site.

Protecting a Device with Remote Access

Let’s say that you have set up remote access to a protected camera in your home network so that you can monitor activity from the office. To continue using this setup with Dojo, you must change the settings in the home router and the Dojo app.

Router Settings

The following instructions refer to a generic home router. The settings may vary slightly based on the home router model in your home network.

1. Log in to your home router. Go to the Port Forwarding page.

   > **Note**: Write down the current settings for internal port, external port, and network protocol (UDP or TCP). You will need them later.

2. Change the device IP to which you currently forward traffic to the Dojo internal IP. You can find **Dojo internal IP** in the **About** group, near the bottom of the Dojo app **Settings** screen.
3. Change the internal port to be the same as the external port.
4. Apply the changes you have made.

The home router might restart.

Dojo app settings

1. In the Dojo app, select the device that you want to access remotely. Select **Edit.**
2. Ensure that the setting for the **IP Address** is **Static**.
3. Change **Remote Access** to **Yes**.
4. Options are displayed.
5. For **External Port**, use the same external port setting as you have for the router.
6. For **Internal Port**, use the setting for the internal router port before you made the change in step 3, above.
7. For **Protocol**, select the same protocol that is used by the router, either **UDP** or **TCP**.

Regulatory Compliance Information

Technical Specification

Base Unit

Power Supply: Input 110-240 VAC / Output 12V DC 1.67 A 20 W

Operating temperature: 0 - 35 degrees C / 32 – 95 degrees F

Pebble

Power 4xAA size batteries (not included)

Operating temperature: 0 - 35 degrees C / 32 – 95 degrees F

Model: DL0007R

Pebble

FCC ID: **2ALQXDL0007RV2**

Power 4xAA size batteries (not included)

Operating temperature: 0 - 35 degrees C / 32 – 95 degrees F

Model: DL0007R

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled env ironment. This equipment should be installed and operated with minimum distance 0mm bet ween the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Product Information

FCC ID: **2ALQXDL0007V2**

Model: DL0007v2

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled env ironment. This equipment should be installed and operated with minimum distance 20cm bet ween the radiator and your body.
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications not expressly approved by the party responsible for compliance to this equipment would void the user’s authority to operate this device.

This Device complies with FCC and IC radiation exposure limits.

IC Statement

This device complies with Industry Canada’s licence-exempt RSSs. Operation is subject to the following two conditions:

(1) This device may not cause interference; and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d’Industrie Canada applicables aux appareils radio exempts de licence. L’exploitation est autorisée aux deux conditions suivantes :

1) l’appareil ne doit pas produire de brouillage;

2) l’utilisateur de l’appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d’en compromettre le fonctionnement.

This equipment complies with FCC and ISED (IC) radiation exposure limits set forth for an uncontrolled environment and meets the 47 CFR 2.1091 and RSS-102 of the FCC and ISED (IC) radio frequency (RF) Exposure rules. This equipment should be installed and operated keeping the radiator at least 20 cm or more away from person’s body.

CE

Declaration of Conformity (DoC)

Hereby, BullGuard Israel LTD declares that the radio equipment type [designation of type of radio equipment] is in compliance with Directive 2014/53/EU." Customers can download a copy of the original DoC to our RE products from < exact Internet address where the full text of the EU declaration of conformity can be obtained. >

Parameter	Mode and Conditions	Min.	Typ.	Max.	Unit
Frequency range	-	2402	-	2480	MHz