# Edge Computing COVID-19 Defender Quick Manual

Version 1.2.0

Table of Contents

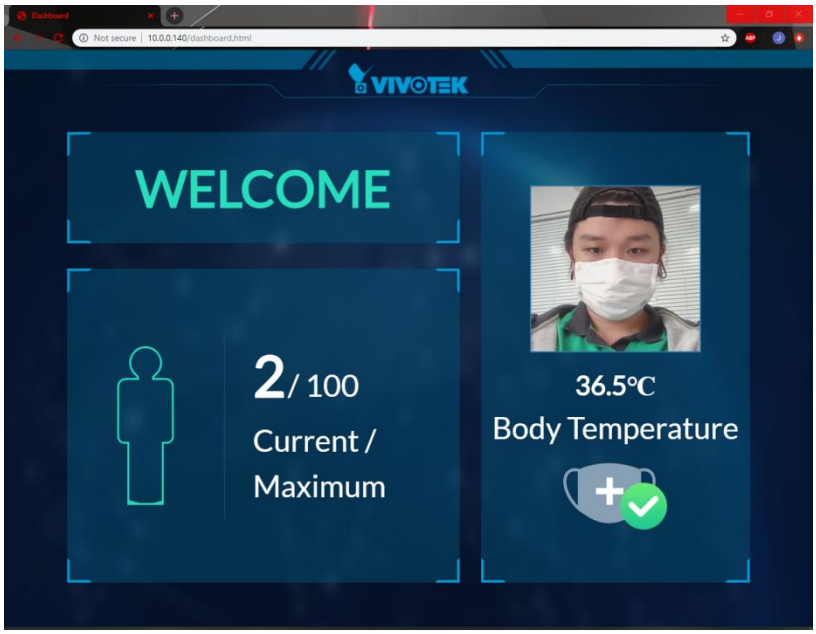
## 1. Introduction

There will be two interfaces for the COVID Defender: Dashboard and the COVID Defender configuration.

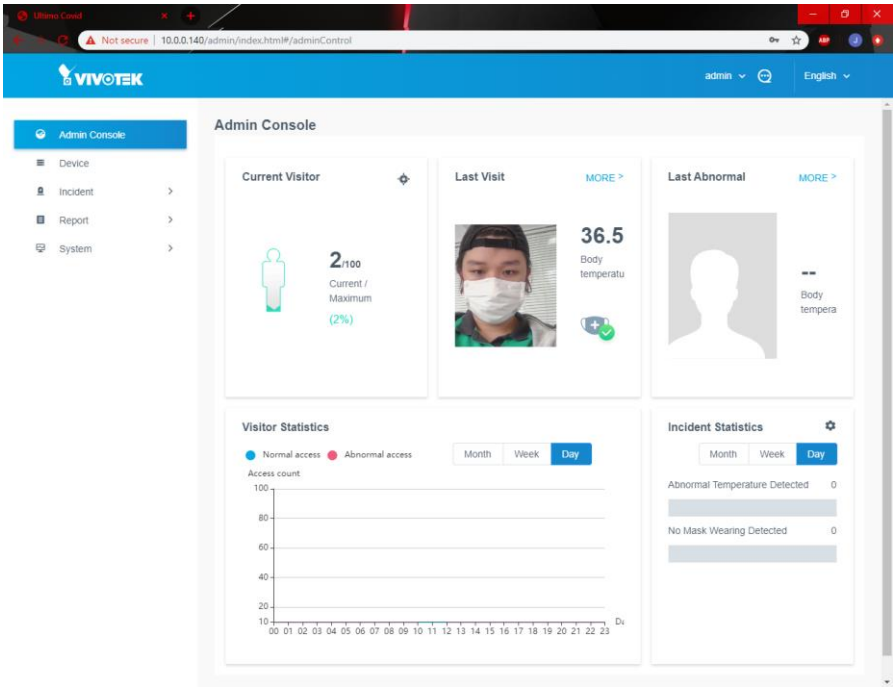
- URL access to Dashboard - http://localhost/dashboard.html
- URL access to COVID Defender configuration - http://localhost/admin/index.html

(If accessing from other PC, change the localhost to AB-101 IP address)

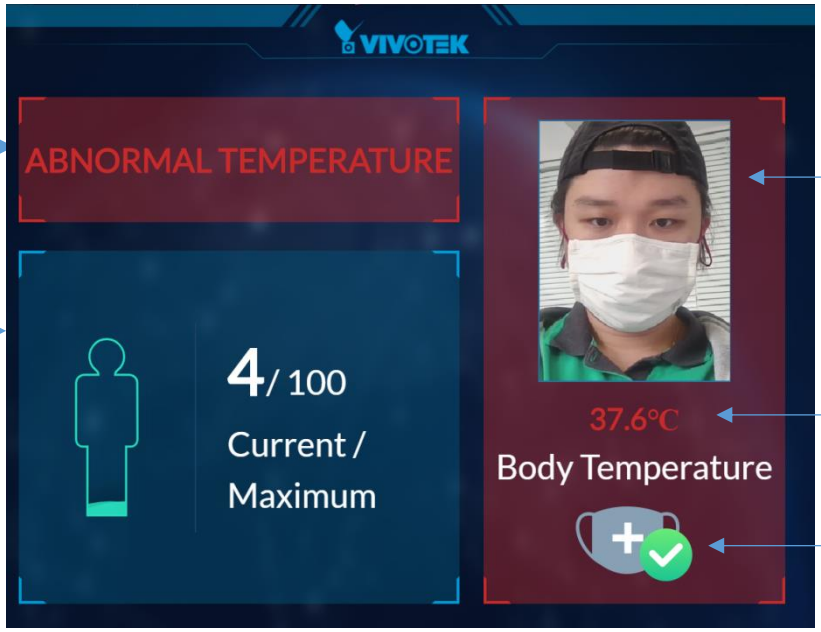
Dashboard




COVID Defender configuration



## 2. Dashboard schematic diagram




Displays current visitors/ maximum number of visitors, once the maximum capacity is reached, it will no longer capture faces and body temperature.

Displays mask detection, Green Tick represents mask on, Red Cross represents no mask.

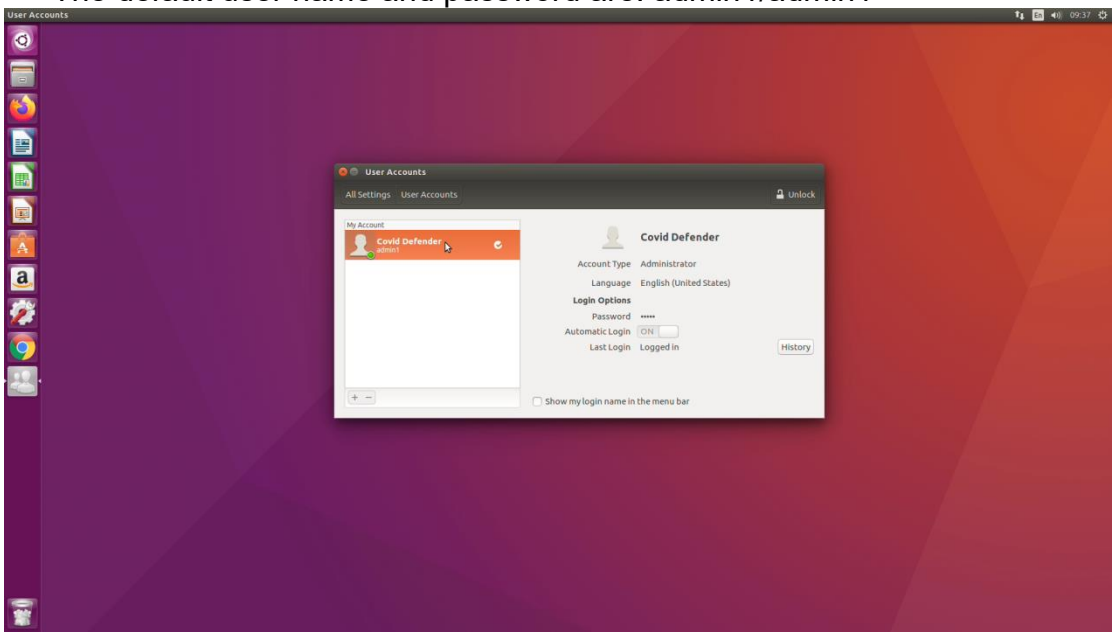
Displays visitor body temperature

Displays visitor temperature and mask detection result. If visitor wear mask and body temperature is normal, it will shows ‘Welcome’. Otherwise, it will display ‘Abnormal temperature’, ‘No mask’ or both.

Displays captured visitor face photo

## 3. Admin Console

1. The IPC comes with a default account. The account name is “Covid Defender.” The default user name and password are: admin1/admin1

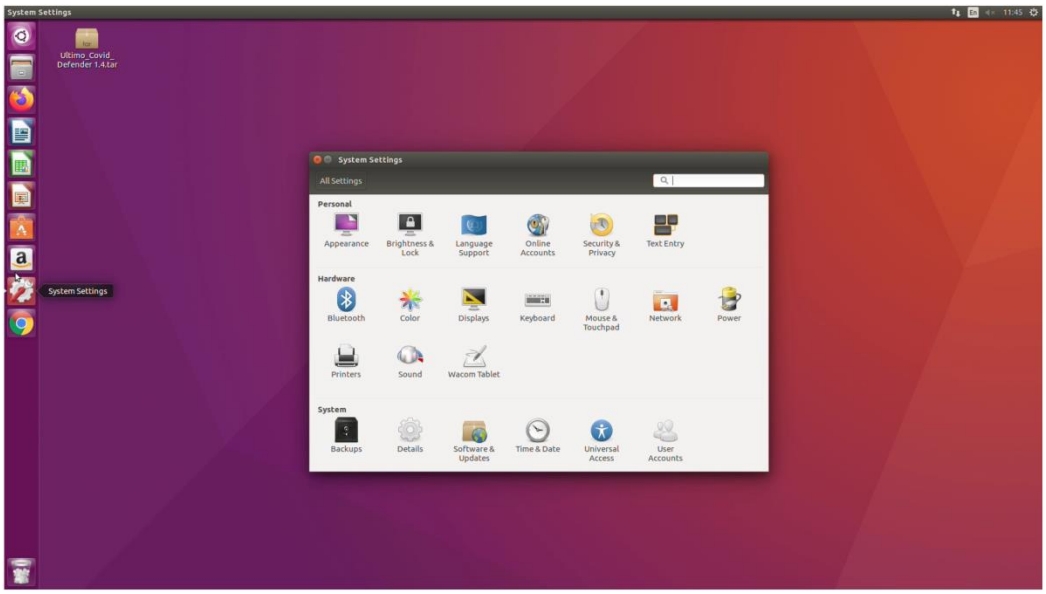



You can also find the password on a name tag of the machine.

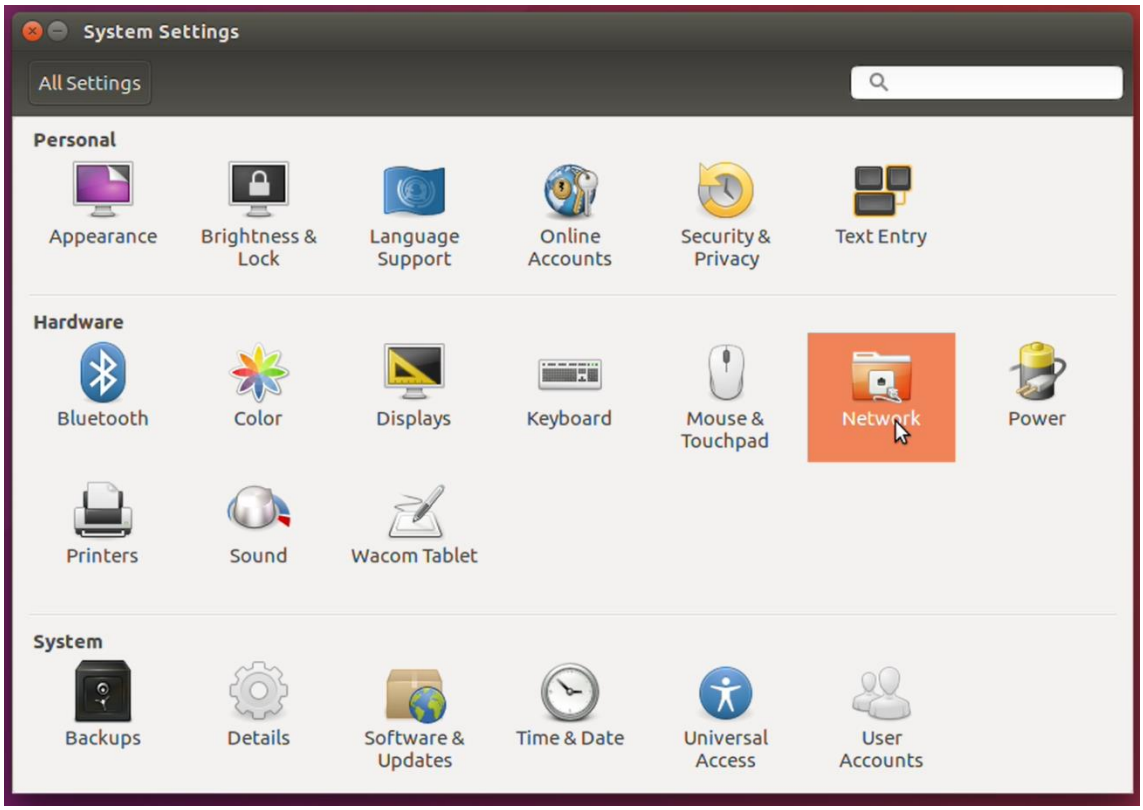
You may need to change the AB-101’s IP address once you power on the machine.

2. Below are the default addresses of the machines in the COVID-19 Defender solution.
   AB-101(IPC): 10.0.0.140
   AF-101(FR reader): 10.0.0.141
   SC8131: Listening to DHCP server.
   Configure the IP addresses of these machines to be in the same subnet.

2-1. On the left pane, click to open **System settings**.

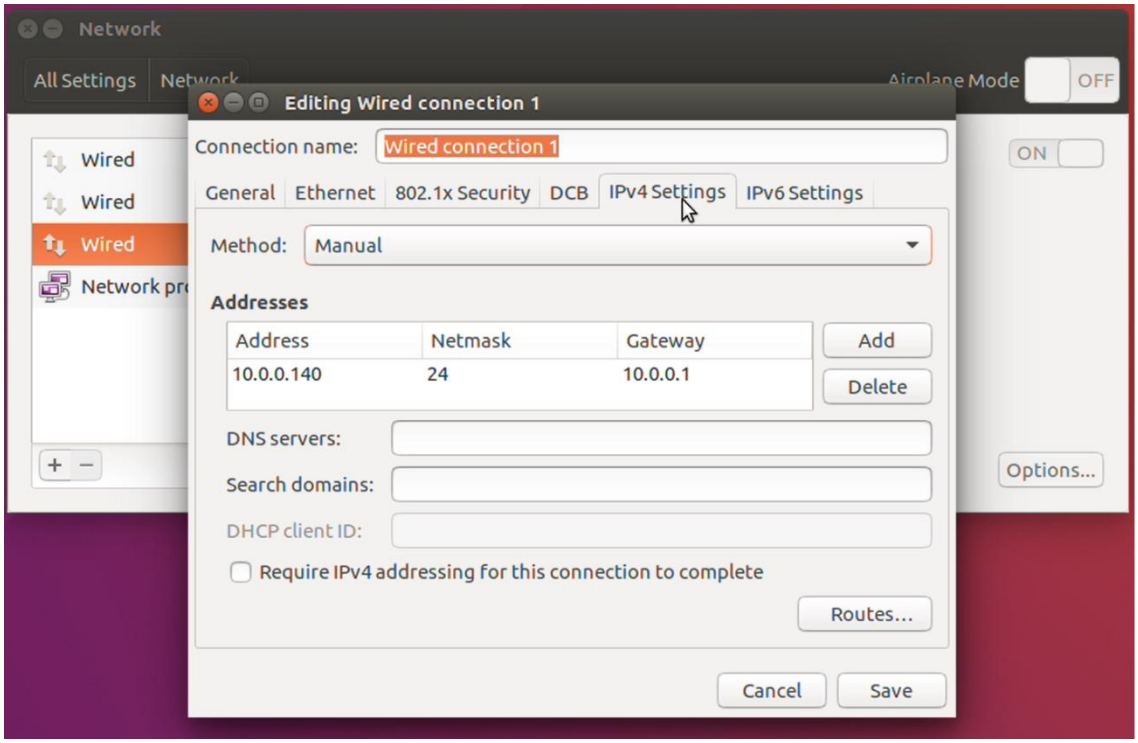



2-2. Select **Network**. Double-click to open the settings.

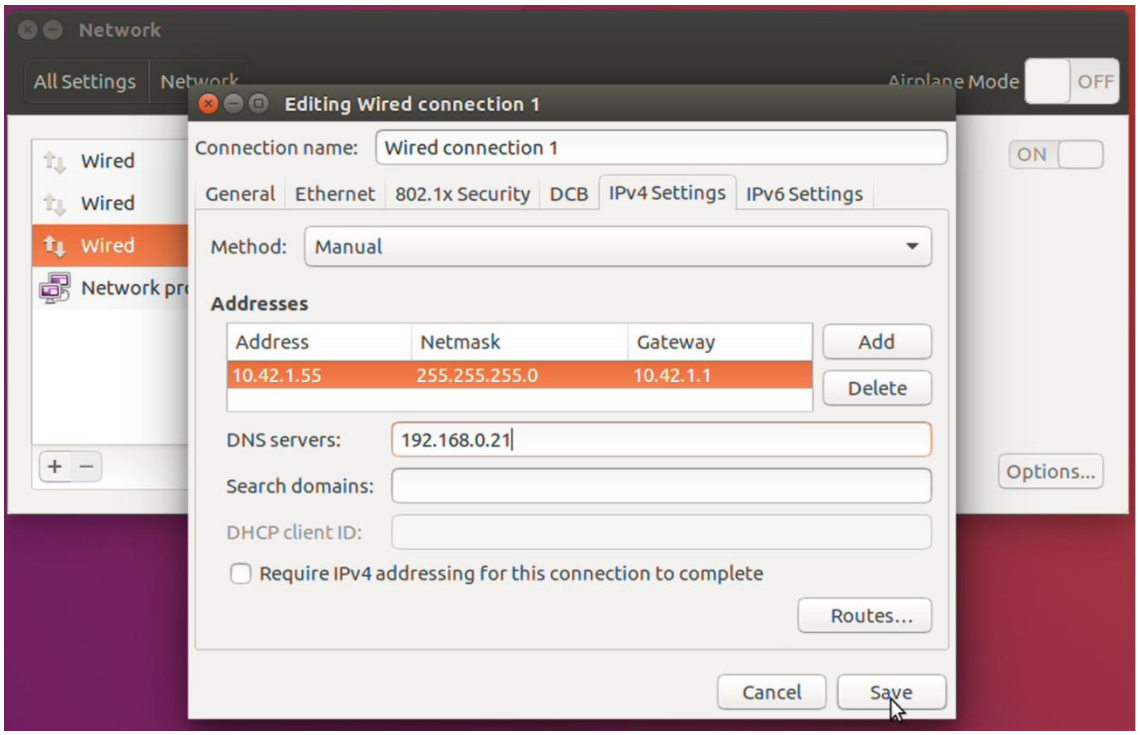


2-3. Select the appropriate wired connection. Click on **Options**.

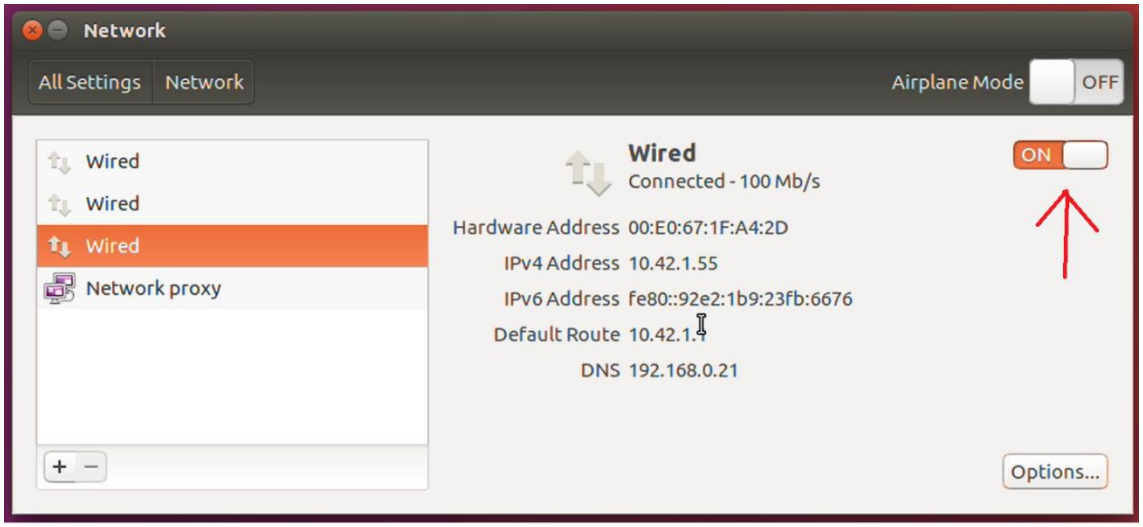

2-4. Click the **IPv4 Settings** tab.



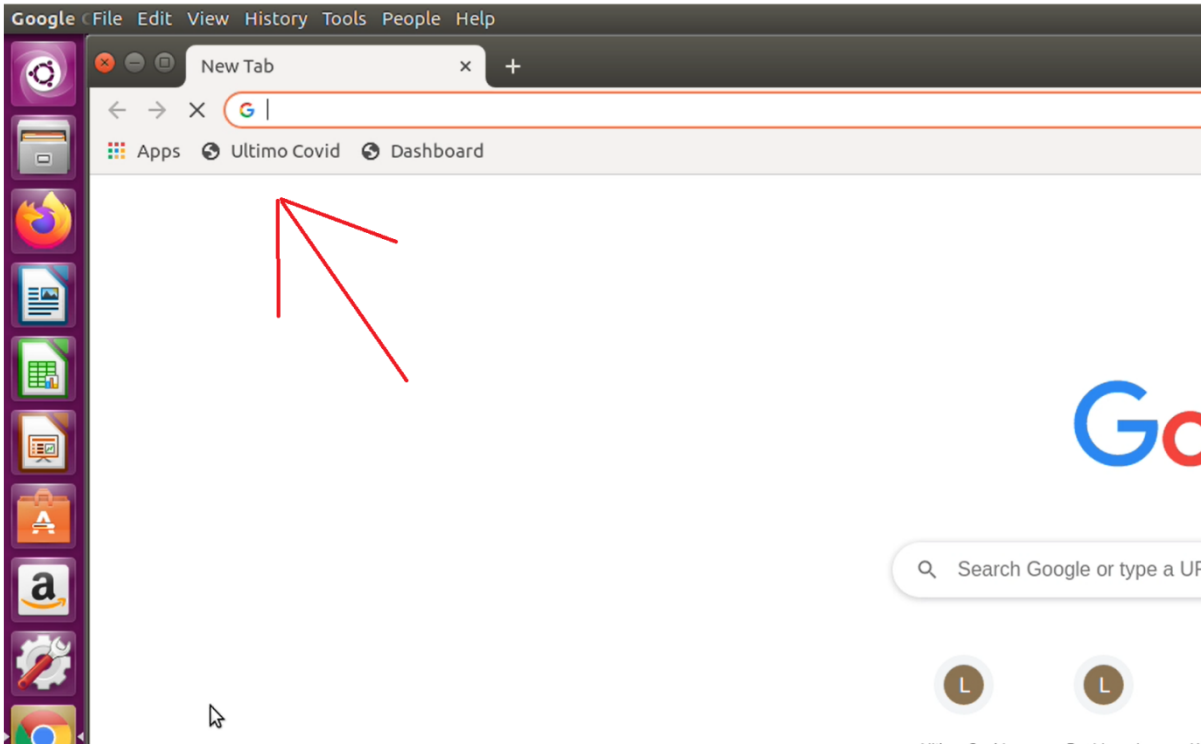
2-5. Enter the IPv4 address, Network mask, Gateway, and DNS server addresses. When done, click Save.



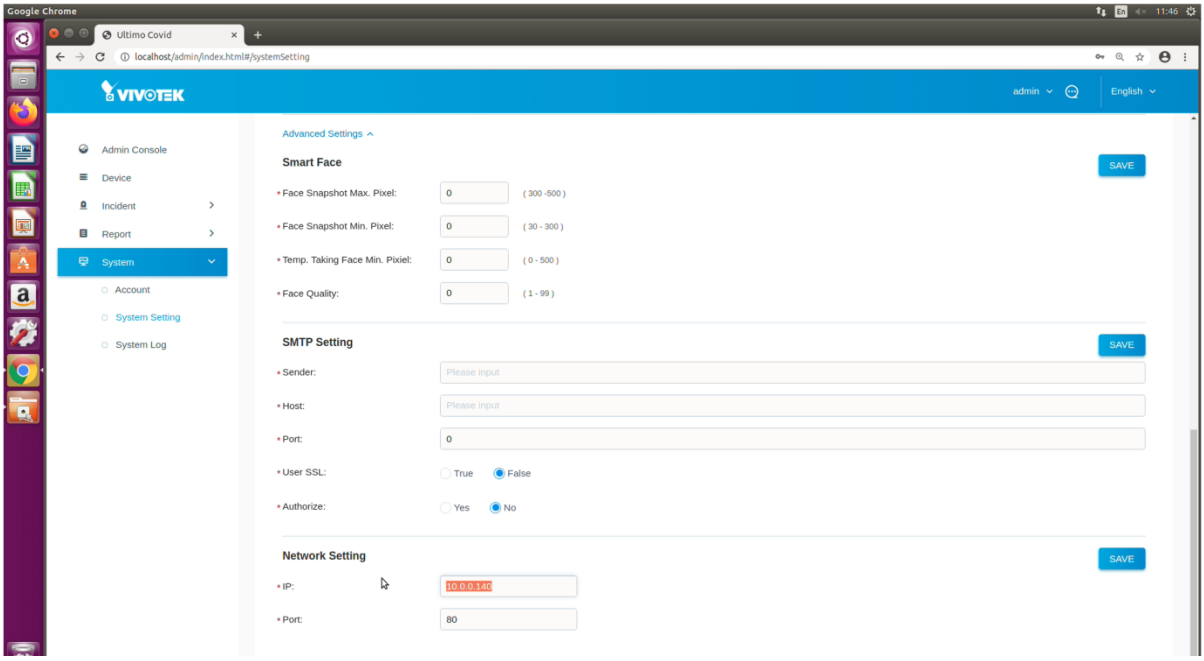

2-6. When done, turn OFF, and then turn ON the wired connection.



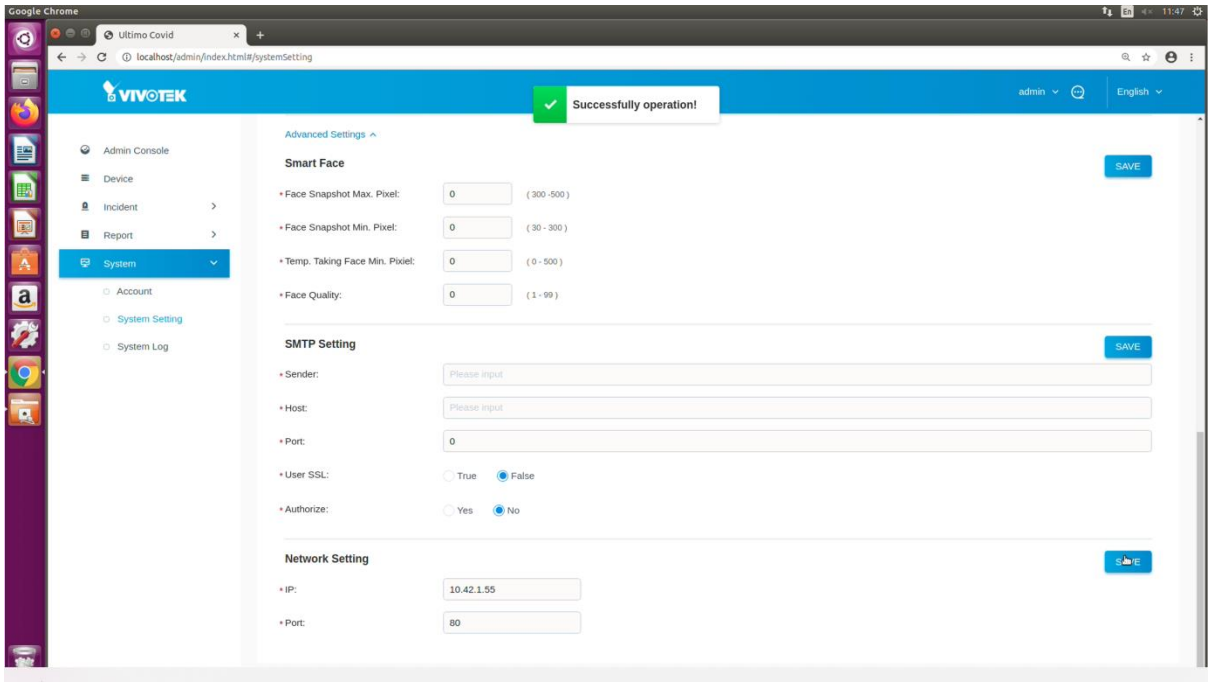
2-7. Open your Chrome browser, and then click on the **Ultimo Covid** shortcut.




2-8. Go to **System** → **System Settings**. Scroll down to find the Network Setting.

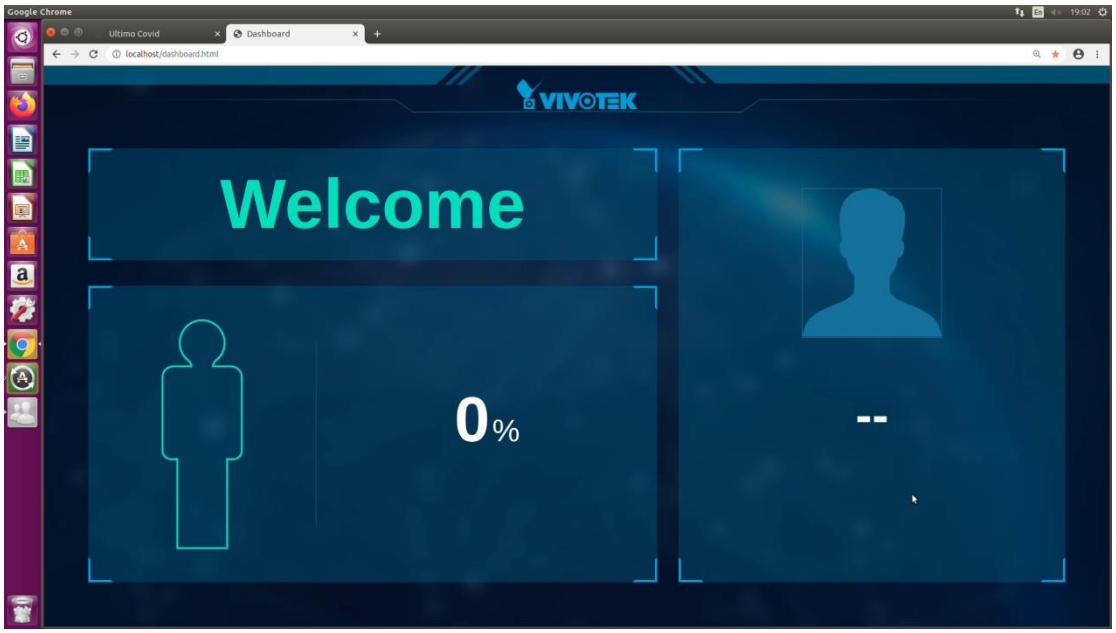


2-9. Enter the IPv4 address you had just configured. Click **Save** to preserve the settings.

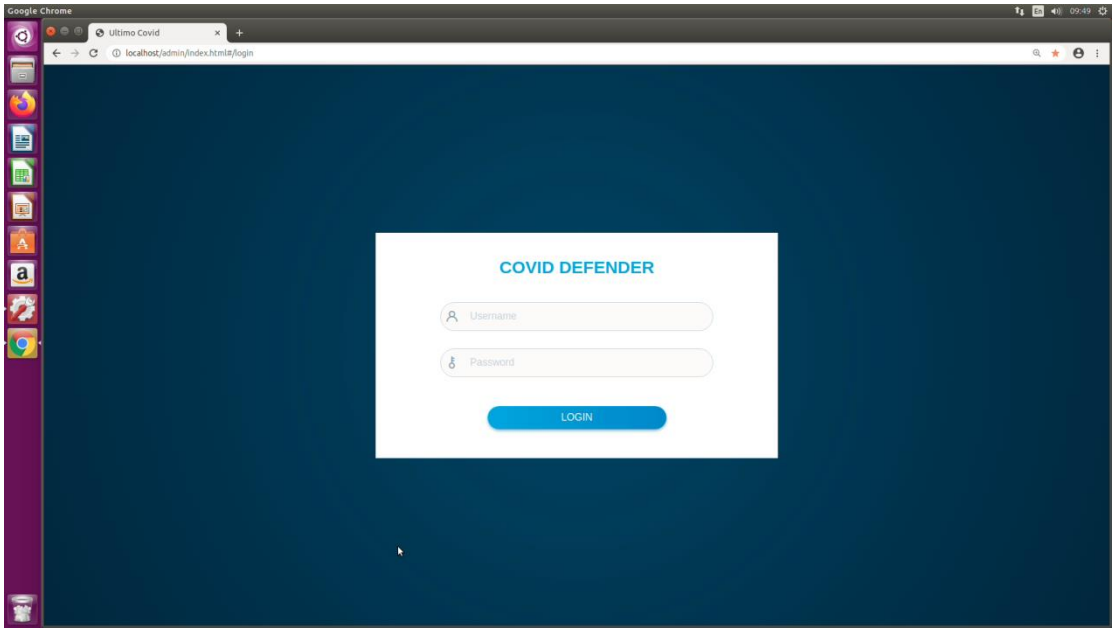


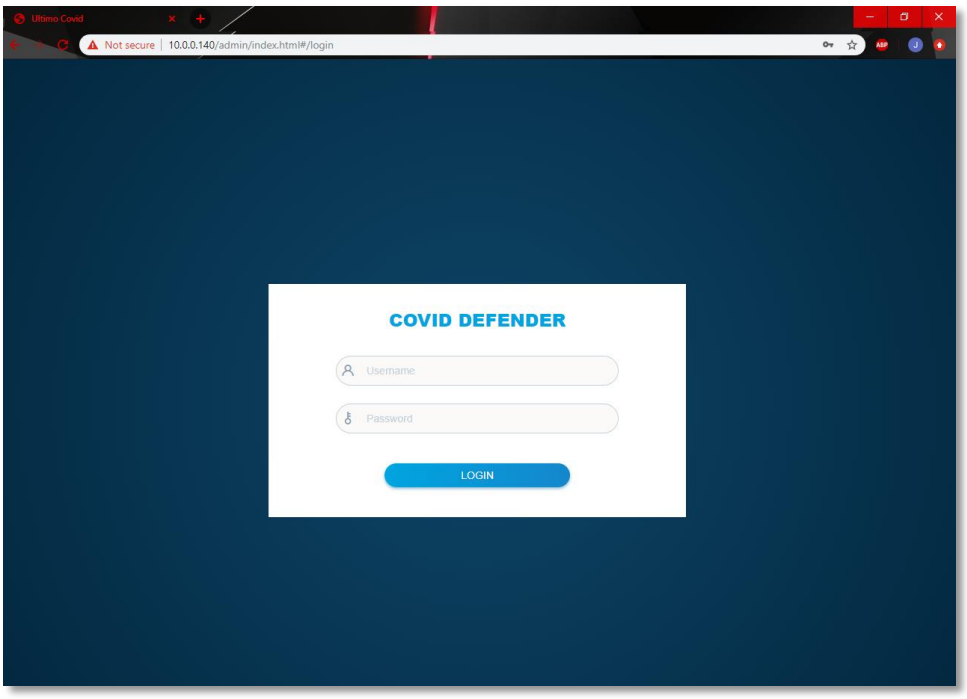
3. Open the Chrome browser embedded in the IPC. There are two embedded hot links on the top of the browser: **Ultimo Covid** and **Dashboard**.


Opening the Dashboard does not require a password.

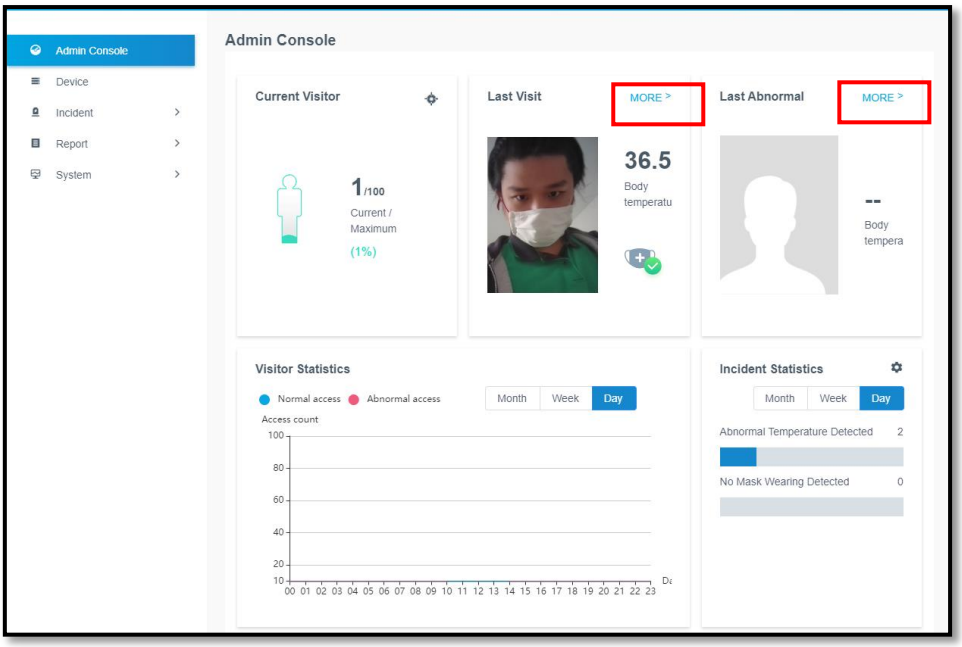



The default user name and password for access to the Ultimo Covid interface are admin/admin.

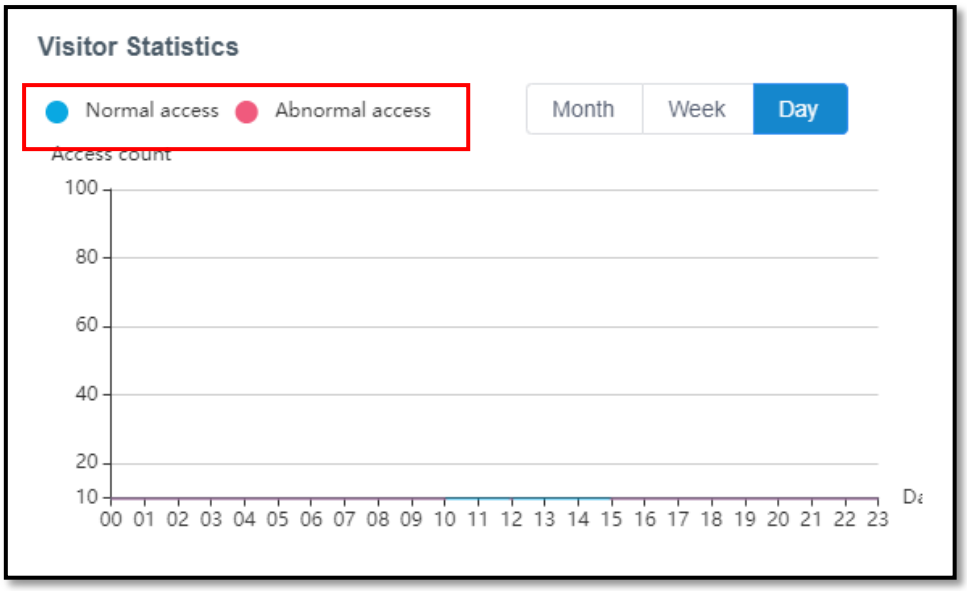


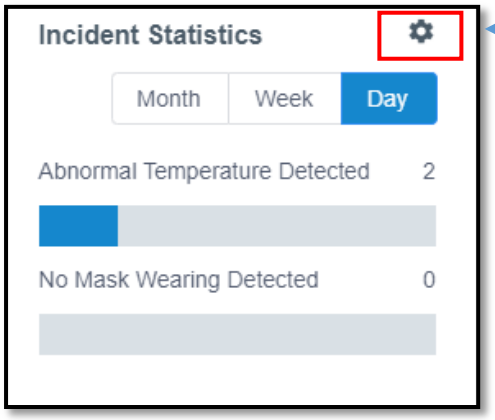

Once the access to COVID defender URL is made, the login page prompts. The default username/password for COVID defender will be **admin/admin.**




After login, it redirects to the Admin Console page. The current visitor indicates the current visitor/maximum numbers of visitors. Last Visit indicates the information for the last visitor (who passed both mask detection and body temperature). The Last Abnormal indicates the person who failed to comply (failed mask detection or body temperature check). By clicking more will redirect to the report page for more access information.

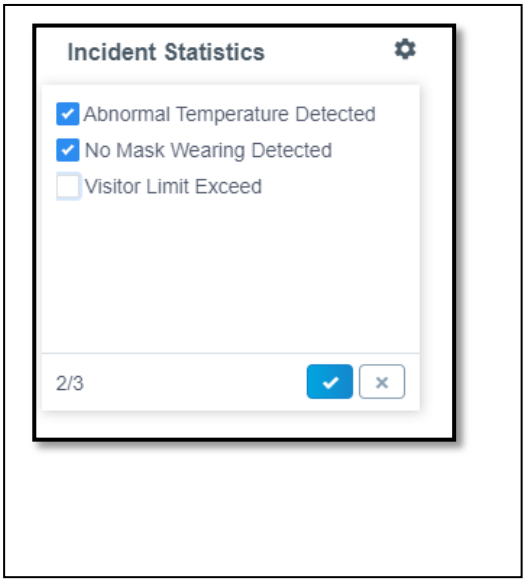



Visitor statistics shows access count and a chart for normal accesses and abnormal accesses. Blue represents normal access and red represents abnormal access. The chart can be arranged in order by month, week or day.

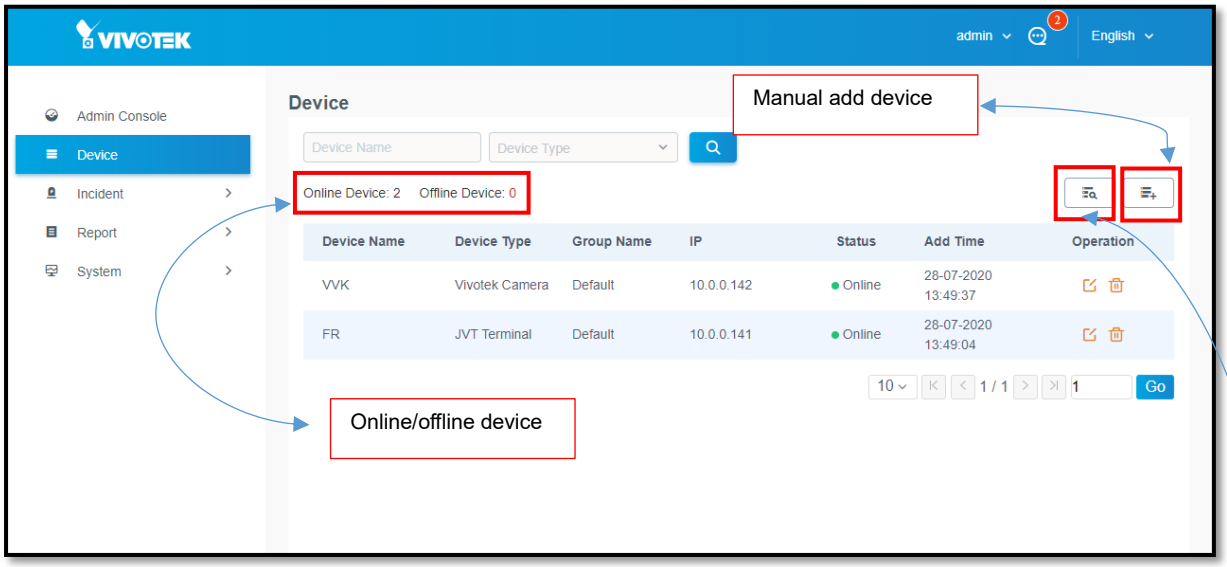



Click gear icon

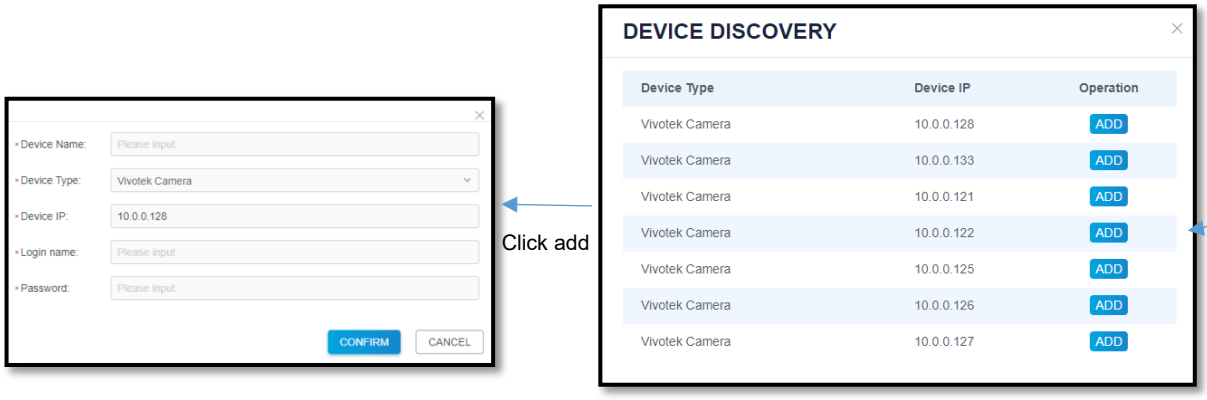
The Incident statistics shows how many times incidents have been triggered. It can be re-ordered by month, week or day. By clicking the Gear icon, you can select which incident to indicate.



## 4. Device



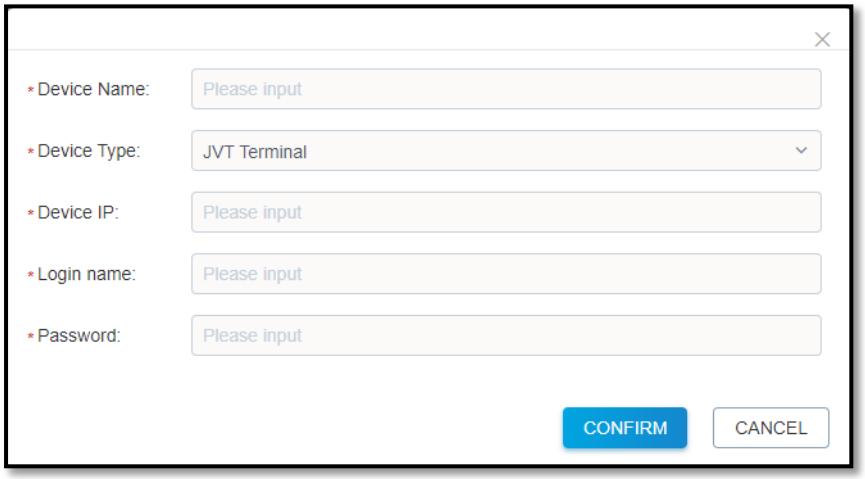

The Device page manages the devices that are connected to the AB-101. We can see device name, device type, group name, IP Address, status, add time. Other than that you can perform operation like edit and delete. You can use the device name and device type to search for the device. Besides, we can tell the device online/offline status at a glance by looking at the online/offline device.




Clicking device discovery allows us to search the devices (VIVOTEK Camera or JVT Terminal) under same range. After click add, we can see the device type and device IP are filled in, at the moment we still need to finish the remaining input box to complete the add device process.

- The precondition is: you must configure the network settings under System Setting before a device can be added to the configuration.

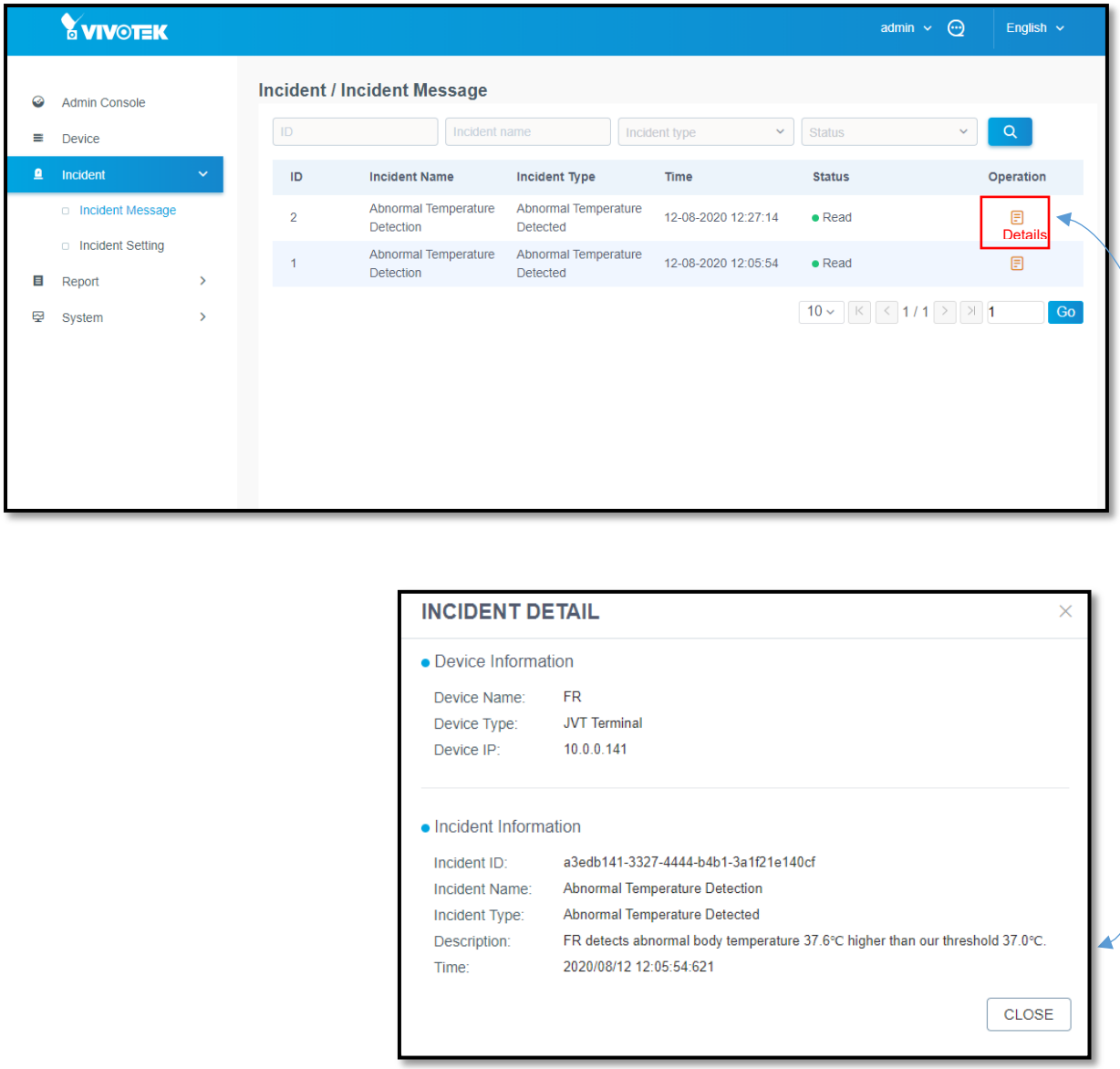
By clicking manual add device you can add device manually. Device type must tally with the actual device (We can select only JVT Terminal or VIVOTEK Camera). Fill in all necessary information in order to add device.



## 5. Incident

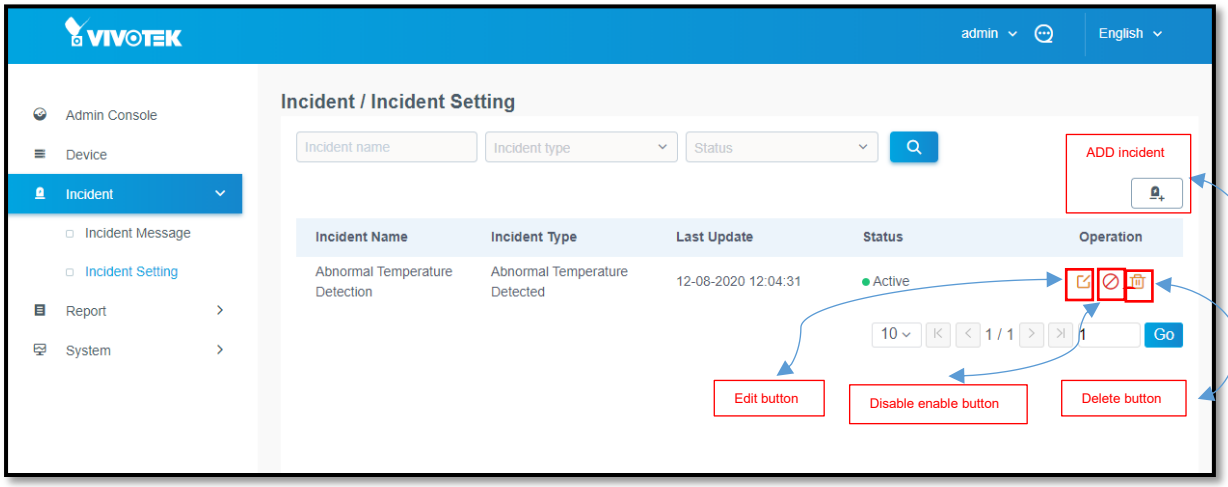
### 5.1 Incident Message

This page shows the incident messages of the system. The Administrator configured with message reception in all incidents can receive messages triggered by this incident. We can search the incident message based on ID, Incident name, Incident type and status.

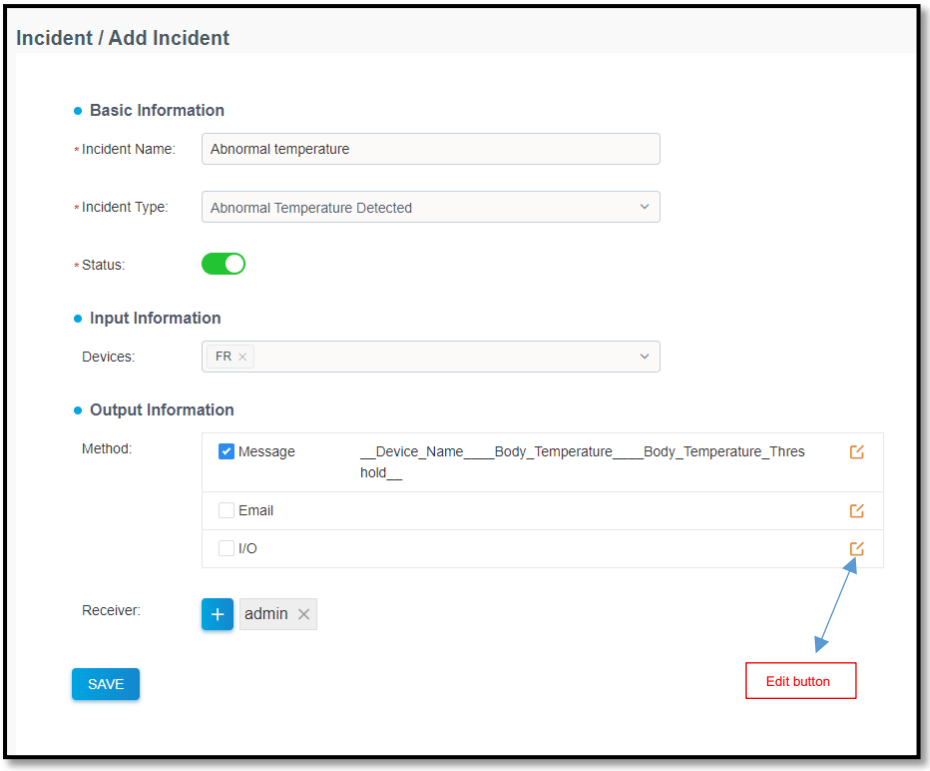



By clicking details button, you can see more information.

## 5.2 Incident setting



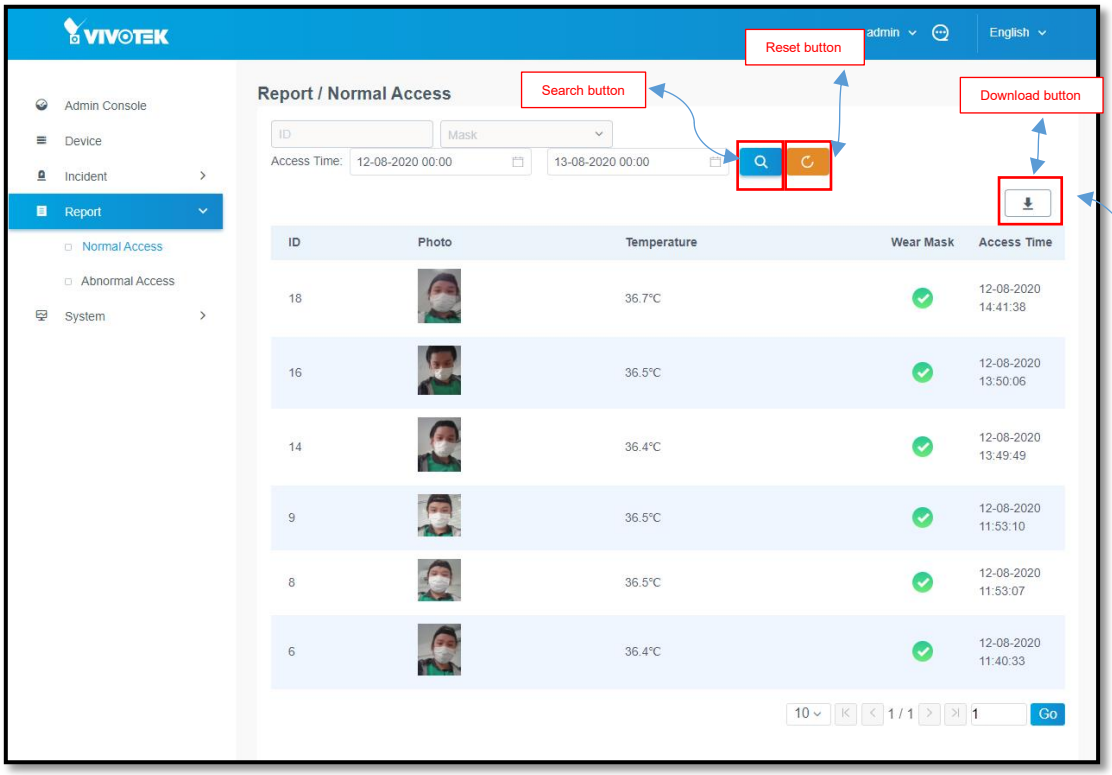

The Incident setting page shows a list of all system incidents added by the administrator. Administrators can add new incidents, edit incidents, or delete incidents, etc.




Below are the steps to add an incident:

1) Enter the incident name.
2) Select incident type.
3) Make sure status is on (green represents on, grey represents off).
4) Input information, under the dropdown list, select the corresponding device.
5) Output information, select the output method of incident triggered, Email, SMS, Message. By clicking edit button to insert template/ add on information.
6) Select the receiver to receive the message.

## 5.3 Normal access



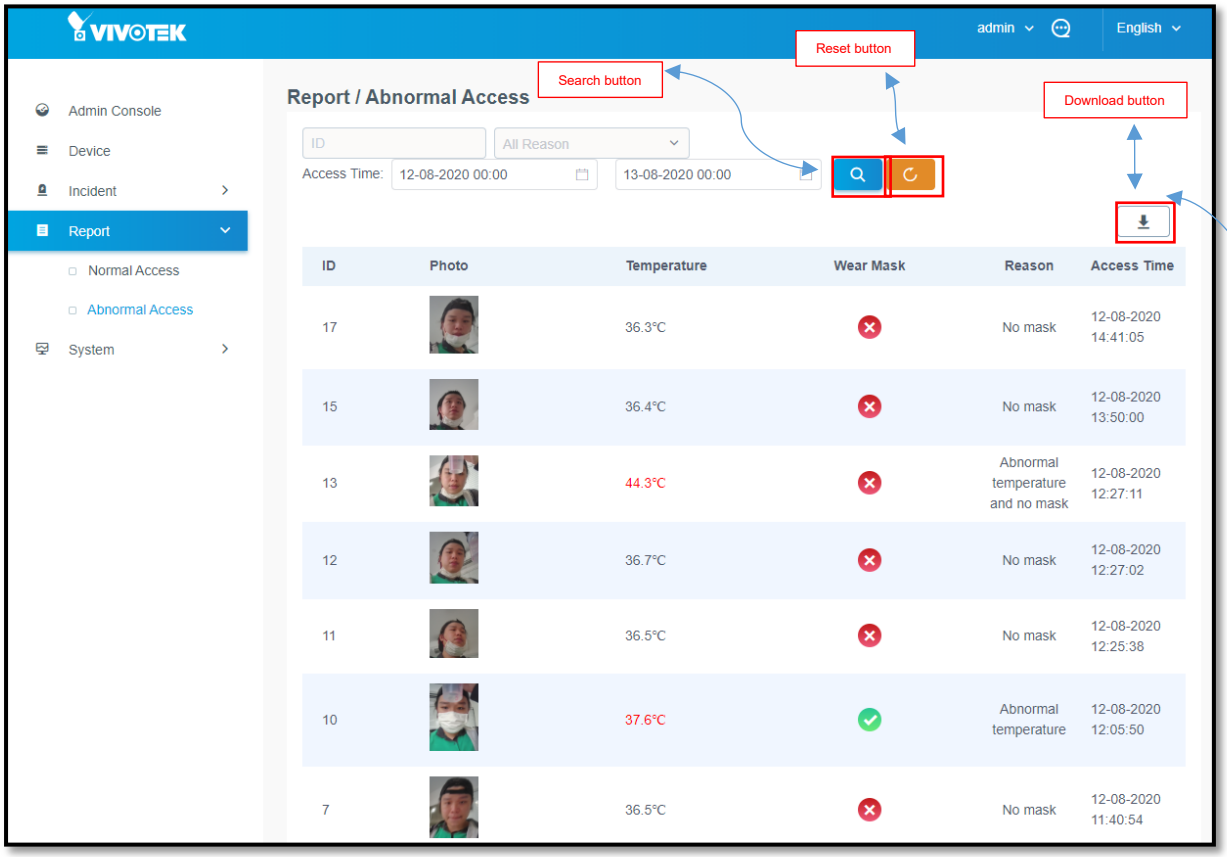

Report – The Normal access page shows normal access records (who passed both mask detection and body temperature).

By entering ID and select mask (Wear mask/ Not detected) can filter and display relevant records only.
Administrators can select the access time in the drop down list to shorten the searching time. System will filter and display relevant records only.

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | ID | Photo | Temperat | Wear Mas | Access Time | |
| 2 | 18 | http://10. | 36.7°C | Yes | 2020/08/12 14:41:38 | |
| 3 | 16 | http://10. | 36.5°C | Yes | 2020/08/12 13:50:06 | |
| 4 | 14 | http://10. | 36.4°C | Yes | 2020/08/12 13:49:49 | |
| 5 | 9 | http://10. | 36.5°C | Yes | 2020/08/12 11:53:10 | |
| 6 | 8 | http://10. | 36.5°C | Yes | 2020/08/12 11:53:07 | |
| 7 | 6 | http://10. | 36.4°C | Yes | 2020/08/12 11:40:33 | |

The downloaded file will be stored in the excel format.

## 5.4 Abnormal access




Report – Abnormal access page shows the abnormal access records (who failed the mask detection or body temperature or both).

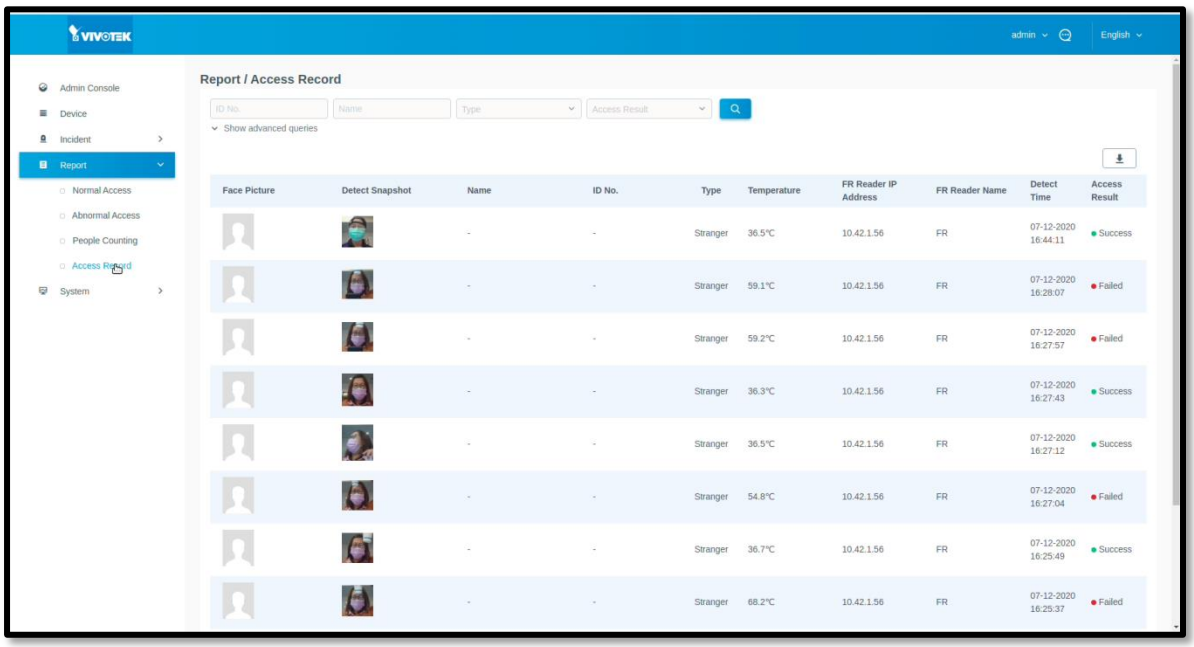
By entering ID and select the reason (No mask/ Abnormal temperature/ Abnormal temperature and no mask) can filter and display relevant records only. Administrator can select the access time in the drop down list to shorten the searching time. System will filter and display the relevant records only.

| ID | Photo | Temperat | Wear Mas | Reason | Access Time |
|---|---|---|---|---|---|
| 17 | http://10. | 36.3°C | No | No mask | 2020/08/12 14:41:05 |
| 15 | http://10. | 36.4°C | No | No mask | 2020/08/12 13:50:00 |
| 13 | http://10. | 44.3°C | No | Abnormal | 2020/08/12 12:27:11 |
| 12 | http://10. | 36.7°C | No | No mask | 2020/08/12 12:27:02 |
| 11 | http://10. | 36.5°C | No | No mask | 2020/08/12 12:25:38 |
| 10 | http://10. | 37.6°C | Yes | Abnormal | 2020/08/12 12:05:50 |
| 7 | http://10. | 36.5°C | No | No mask | 2020/08/12 11:40:54 |

The downloaded file will be stored in the excel format.

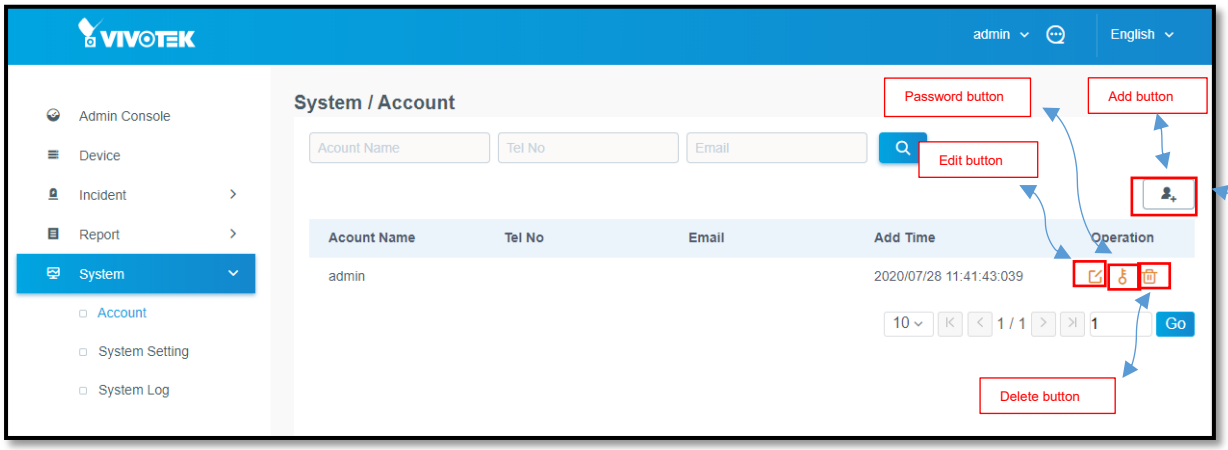
## 5.5 Access Record

The Access record has access to the thermal reader's name list along with a snapshot of the visitor's each appearance. The access report stores and displays the list unless you disable the Storage records option.

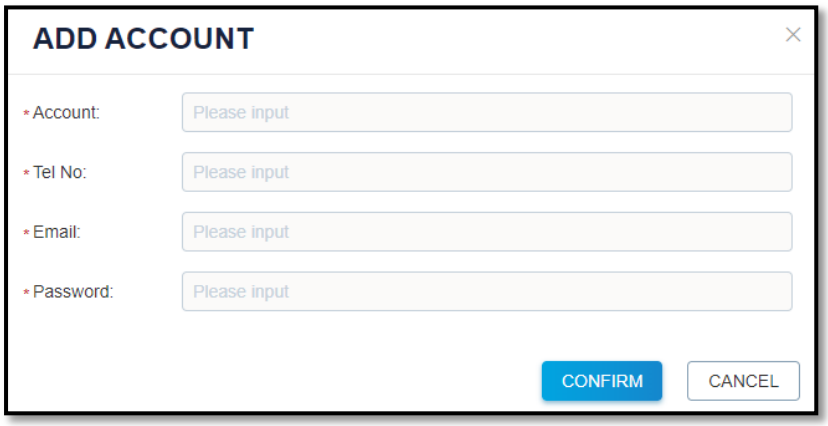


# 6. System

## 6.1 Account

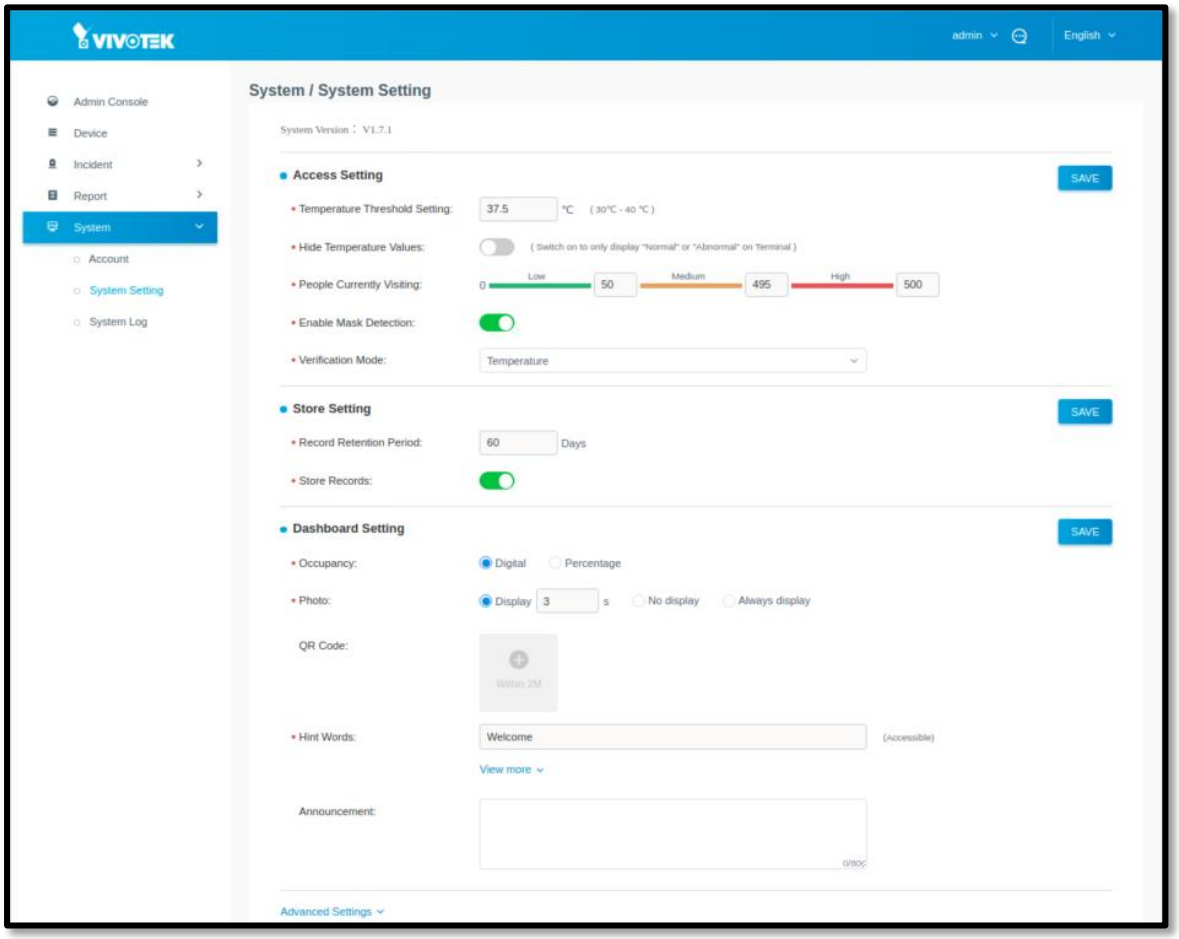



System – The Account page shows the existing accounts in the system. By entering Account name, Tel No, and email to filter and display the relevant records only. Administrators can add new account, edit account information, change password, and delete an account.

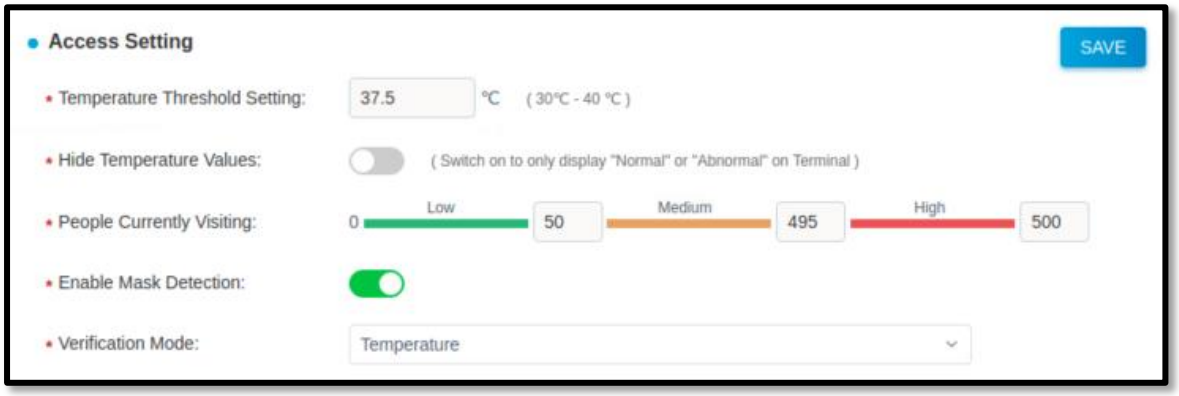



The Administrator needs to enter all of the input boxes in order to create an account. The Tel No must be digit, and the email must follow email format. After you inserted all necessary information, click CONFIRM.

## 6.2 System Setting

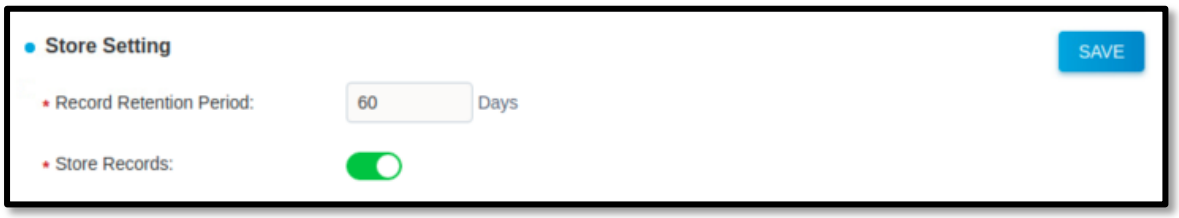



The System setting page allows administrators to manage different type of settings like Access Setting, Dashboard setting, Privacy protection setting, Service setting and Network Setting.



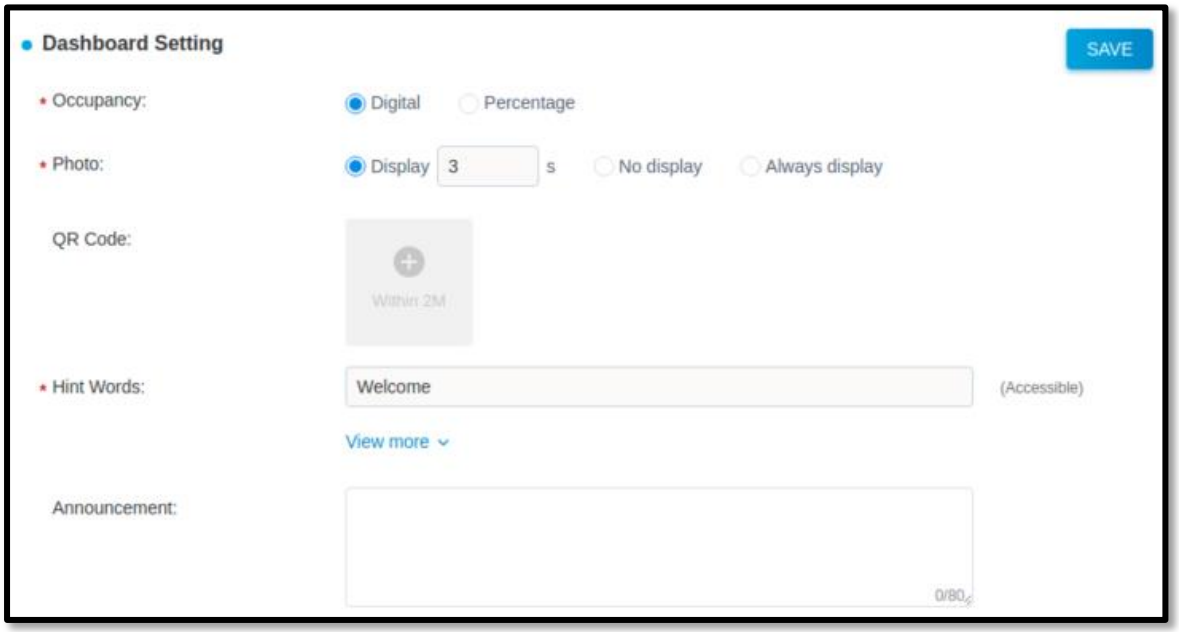

- Temperature threshold setting:
  We can configure the threshold for body temperature (30℃ - 40 ℃). Visitor's body temperature that is higher than the value will be considered an abnormal access.
- Hide Temperature Values:
  Enable it will hide the temperature values. On the terminal, only the normal or abnormal status will display.

- People currently visiting:
  Administrator can define the visitor number, low, medium and high. The farthest right is the maximum number of people allowed to visit, once reached, the system will stop to capture faces and body temperatures.
- Enable Mask Detection:
  To enable the detection of person is wearing mask or not.
- Verification Mode:
  Temperature: Check by temperature threshold
  Temperature + Face: Check by temperature threshold and verify with this person identity.



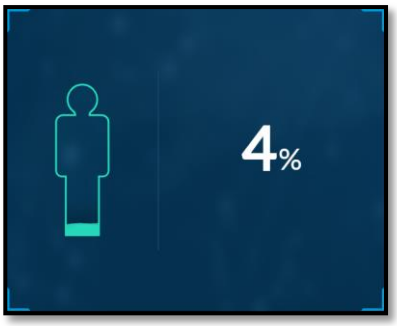

Store setting can configure how many days of data in IPC.

- Record retention period: To delete record data after X days.
- Store snapshot photos: Enable to store snapshot photos.



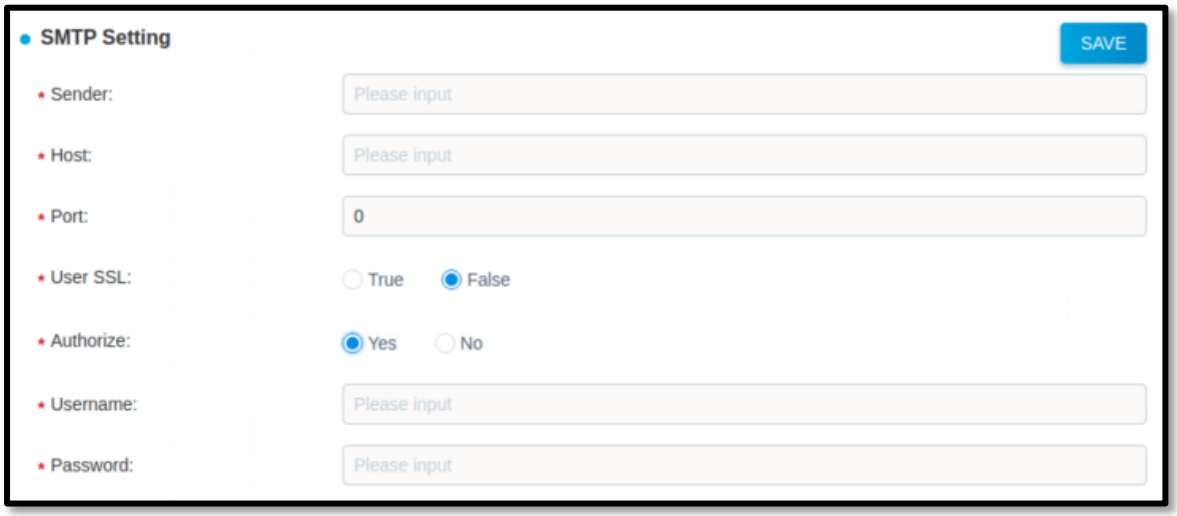

- Occupancy: Change the dashboard setting to digital or percentage.


vs.



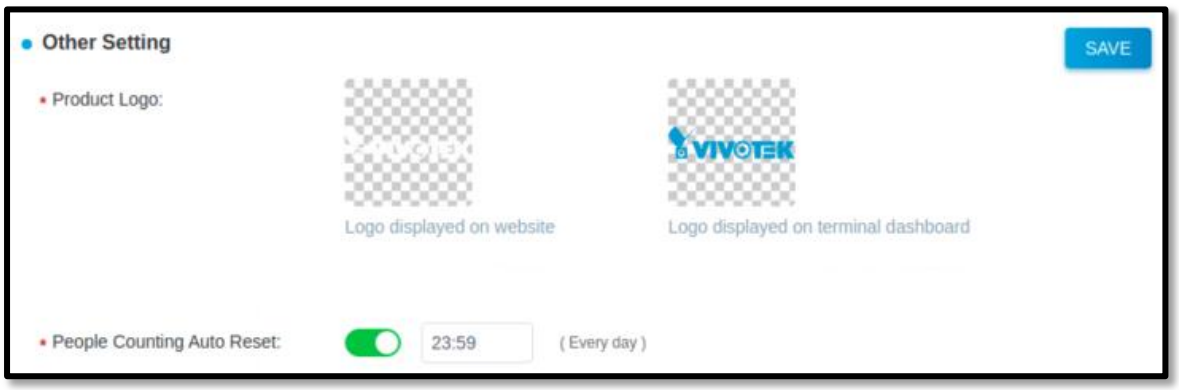

The sample screens for the digital and percentage dashboard are shown above.

- Photo: Display mode settings on dashboard.
- Hint Words: Allow user to enter the words displayed on dashboard.
  For example: Welcome

- Sender: Sender name
- Host: SMTP host (Mail server)
- Port: SMTP port.
- User SSL: Enable or disable Secure Sockets Layer for email.
- Authorize: Select yes if your email service requires service credentials.
  Select no if using mail service that does not require user name/password.
- Username: Sender email address.
- Password: Sender email password.

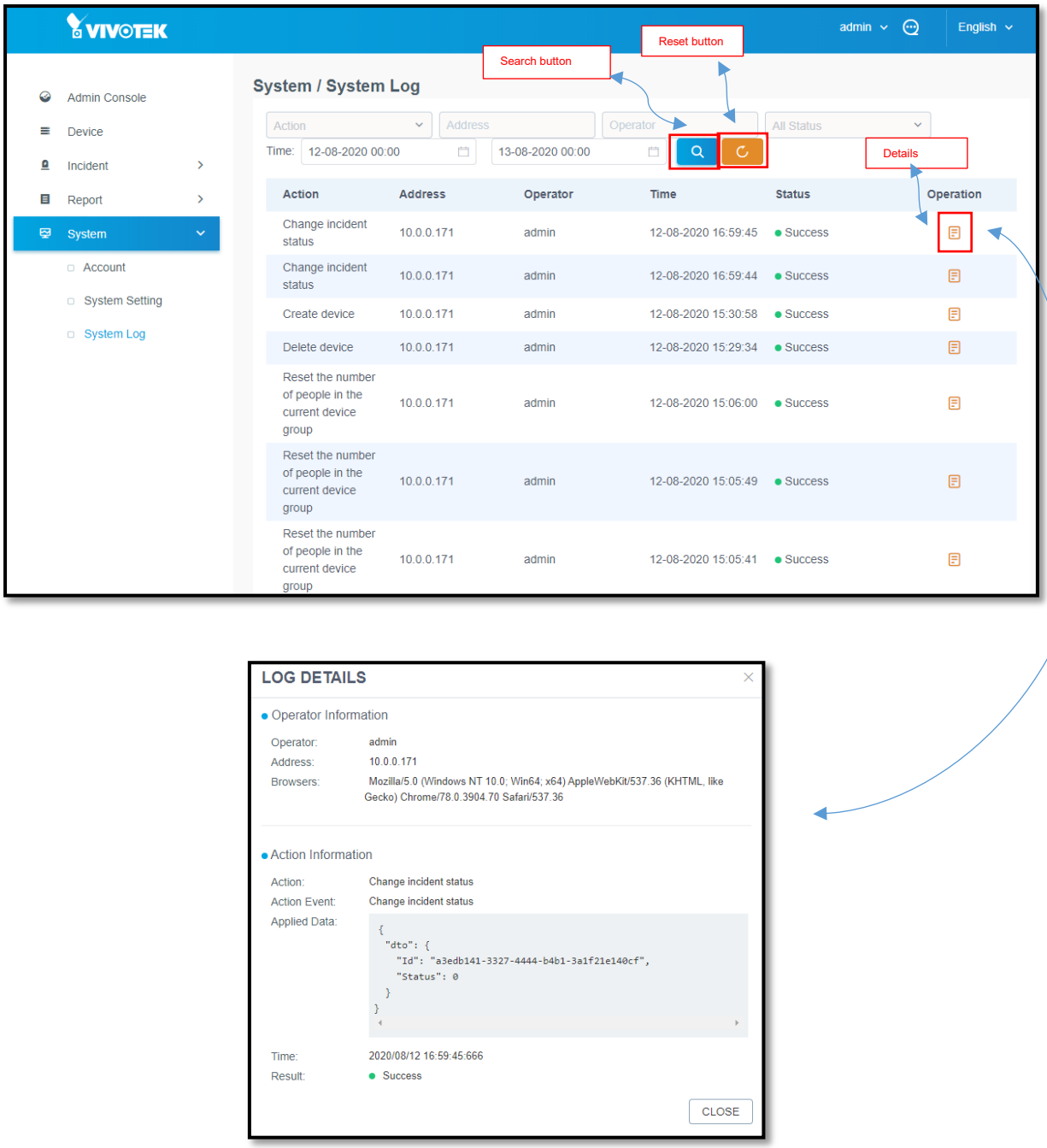

Devices (JVT terminals and VIVOTEK cameras) under this range will be found when using the device discovery function.




- Product Logo: select the picture displayed on website/dashboard.
- People Counting Auto Reset: Enable to choose the timing for people counting data reset for each day.

## 6.3 System Log

This page displays a record of all of the system logs in the system. By entering Action name, IP address, Operator and status, you can filter and display relevant records only. Administrators can select the access time in the drop down list to shorten the searching time. System will filter and display relevant records only.



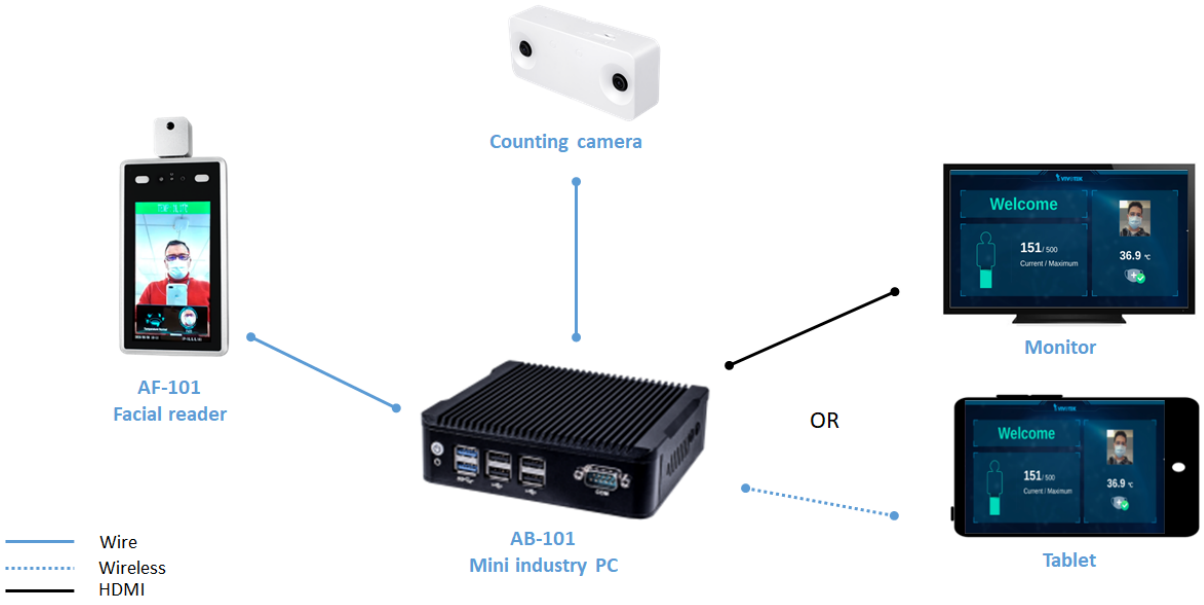




Click on the details button to reveal more information.

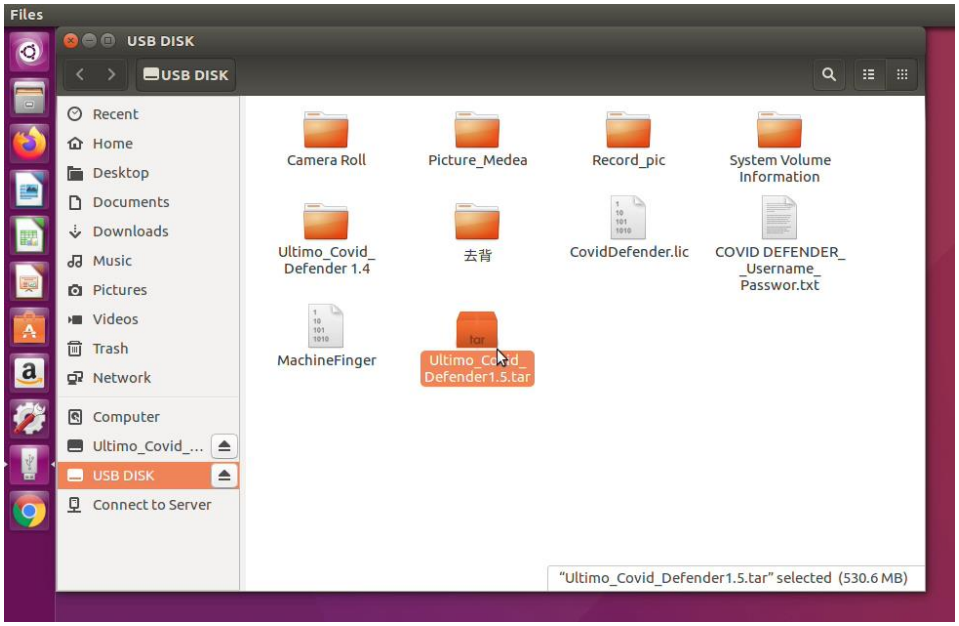
## Appendix

The architecture of **Edge Computing COVID-19 Defender**:

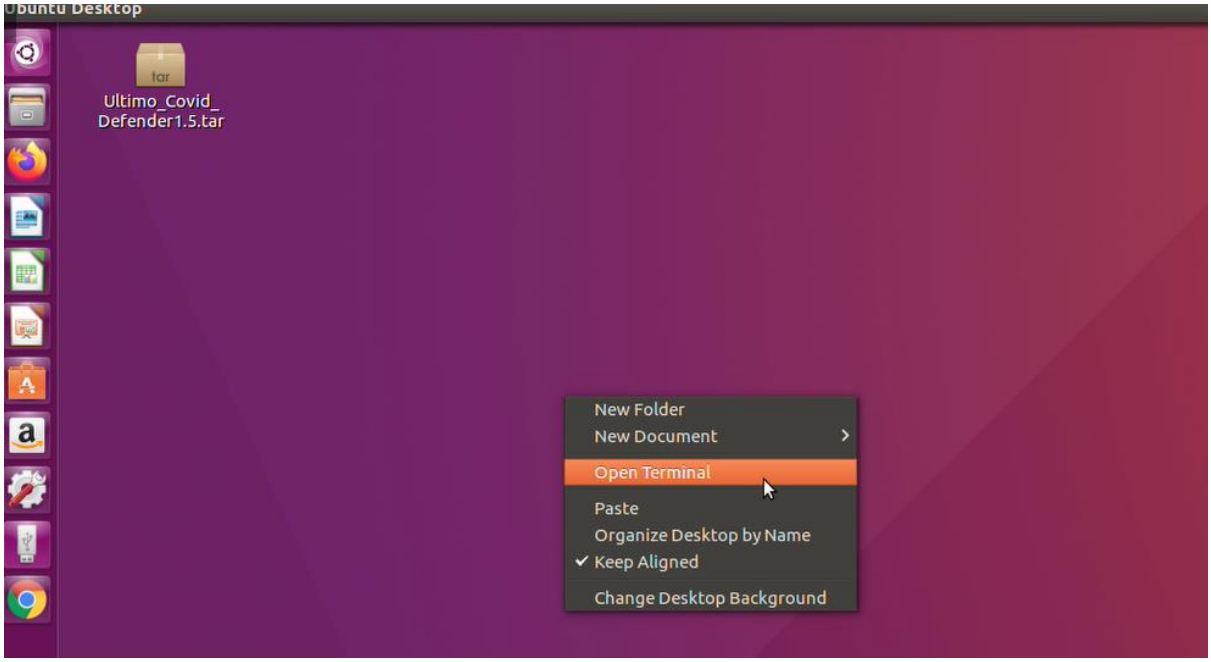



## A-1. Upgrade procedure of AB-101

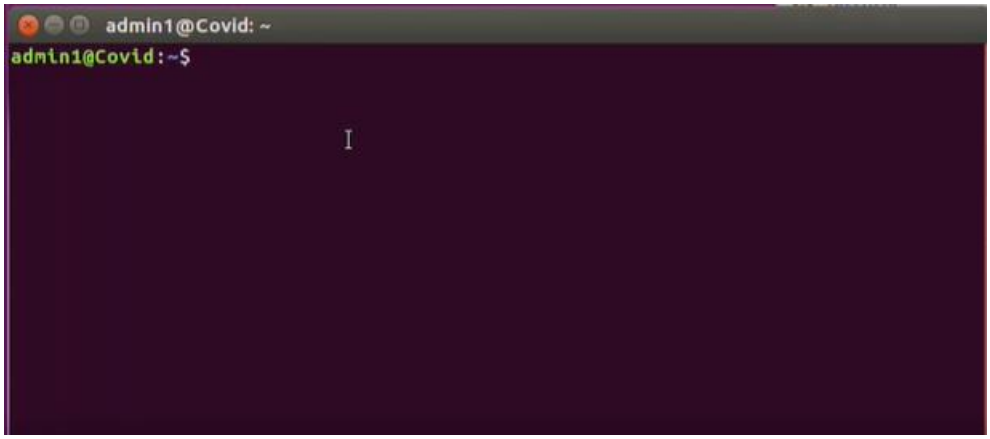
1. Download firmware “Ultimo_Covid_Defender.tar” and copy to Desktop.




2. Right click on desktop and choose “Open Terminal”.




Open Terminal:

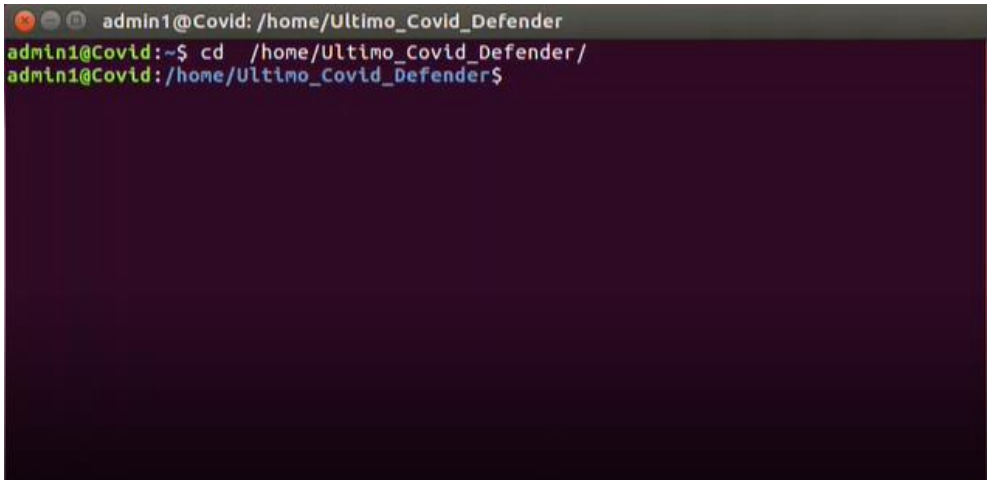



3. Stop Ultimo Covid Defender:

Use below command to stop Ultimo Covid Defender program.

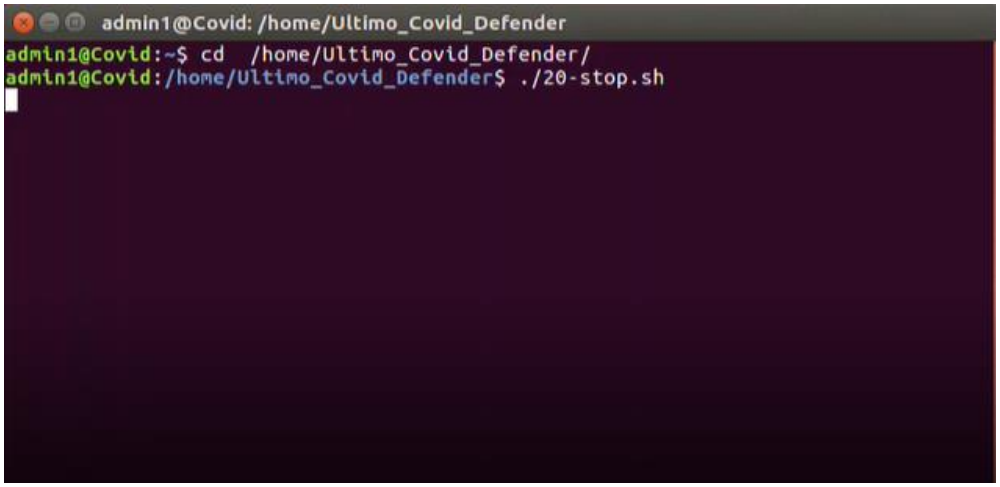
Select Ultimo Covid Defender program first.

*cd /home/Ultimo_Covid_Defender/*




Then stop Ultimo Covid Defender program

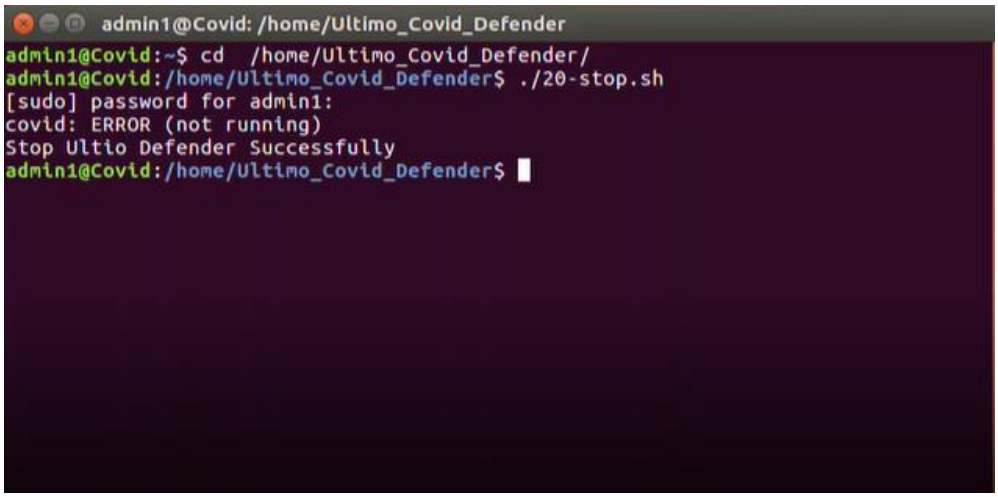
*./20-stop.sh*




[Sudo] password for admin1: *Admin123.*

*Please enter "." at the end of password*

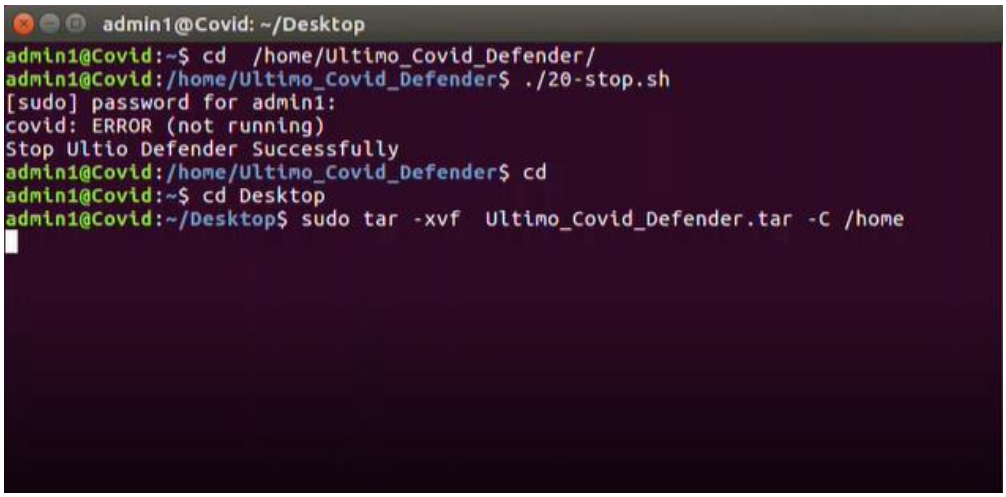
Confirm "Stop Ultio Defender Successfully" showed up.




4. Unzip firmware package for upgrading:

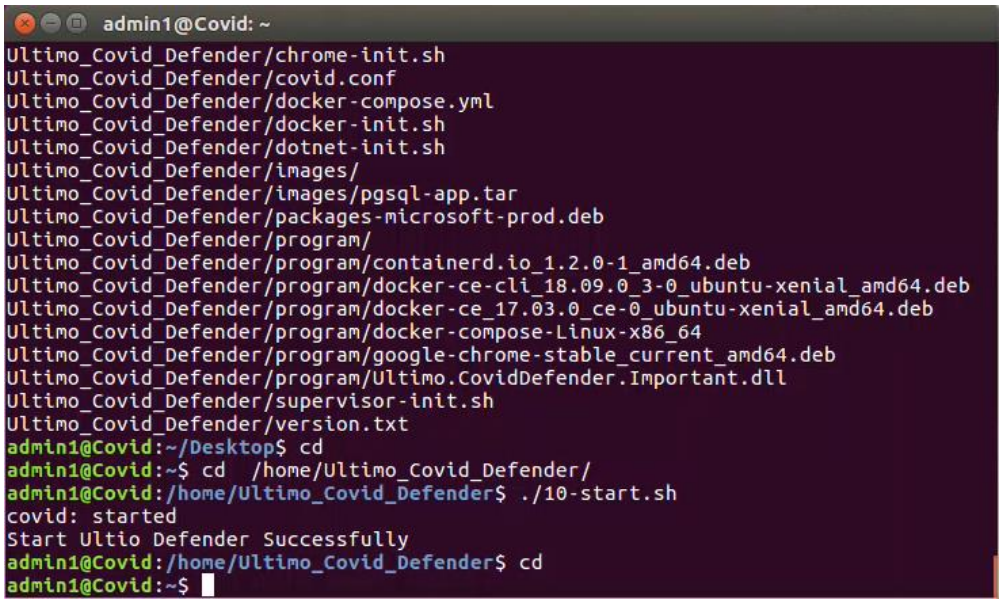
Go back to desktop path

*cd*
*cd Decktop*
*sudo tar –xvf Ultimo_Covid_Defender.tar –C /home*




5. Start Ultimo Covid defender:

*cd*
*cd /home/Ultimo_Covid_Defender/*
*./10-start.sh*

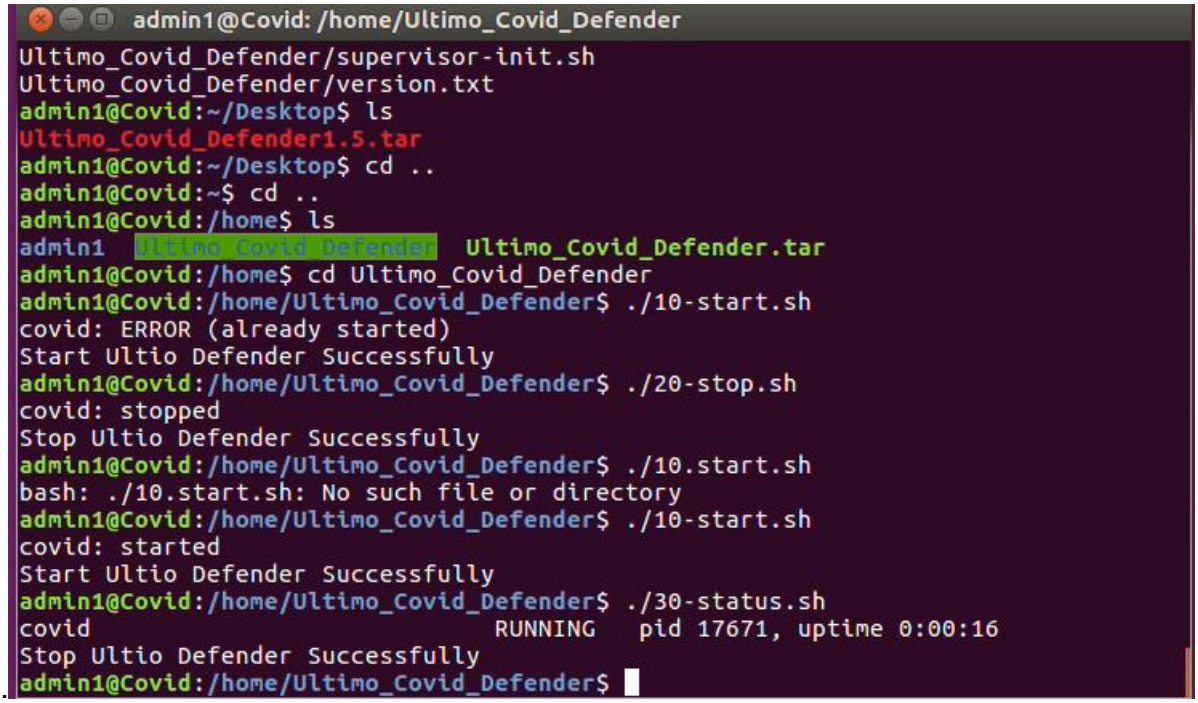



Confirm “Start Ultio Defender Successfully” showed up.

6. You can also use below command to check Covid Defender program status:

*./30-status.sh*

Check if program is “RUNNING” or not.




## A-2. Upgrade procedure of AF-101

Please contact technical support for AF-101 firmware upgrade.