

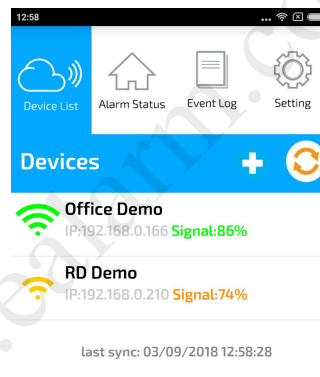
## SCloud App Update Change log(Android Version)

Release: v1.2.7

Google Play Store: <https://play.google.com/store/apps/details?id=com.SCloud>



- Added WiFi signal strength indicator (WiFi module - WiFi Router):
  - The WiFi signal strength will be shown **when the user's app are in the same network with the WiFi Module.**(User's handphone must connect to the same WiFi router with the WiFi module)
  - It takes about 15 seconds for the apps to detect the WiFi module. Once the WiFi module was detected,the WiFi signal strength will be displayed in the device list.



WiFi Signal Strength	Signal Quality	Remarks
76%-100%	Good	Excellent WiFi signal strength.
41%~75%	Medium	Acceptable WiFi signal strength
1%-40%	Poor	The WiFi module has the limited connectivity. Highly recommended to change the installation location of the WiFi module.

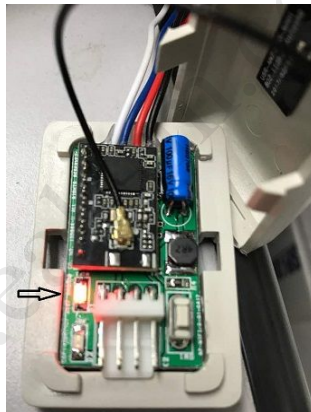
## What can block a WiFi signal?

Everything blocks Wi-Fi signals a little. **Wood**, **plaster**, **cinder blocks**, and **glass** don't interfere much, but **metal wall**, **brick wall**, **stone**, and **water**(aquarium tank) can be more problematic. The shorter the distance between WiFi module and WiFi router, the better the quality of the WiFi signal strength.

Please **do not** put the WiFi module inside the **metal box**.

## Why would the device show “Offline” after the pairing?

- Please check the WiFi LED on the WiFi Module, if the red color LED still **ON** after the pairing, it means that the WiFi module failed to connect to the WiFi router. In this case:
  - Please check again the WiFi password.
  - Pair again the WiFi module without removing device from the user account.
  - Change the installation location of the WiFi module based on the WiFi signal strength. ( During the selection of WiFi SSID)



- In some cases, the WiFi module failed to connect to the WiFi router is due to the incorrect security mode. Please ensure that the WiFi router is working under WPA/WPA2 or WPA/WPA2 Mixed mode and AES as encryption standard instead of old WPE technology in the WiFi router setting.

Wireless Network: <input type="button" value="Enabled"/> <input type="button" value="Disabled"/>	
Network Name (SSID): <input type="text" value="HOME-D12F"/>	
Mode: 802.11 b/g/n	
Security Mode: WPA2-PSK (AES)	
Channel Selection: WPA2-PSK (AES)	
Channel: WPA2-PSK (AES)	
Network Password: WPA2-PSK (AES)	
Show Network Password: <input checked="" type="checkbox"/>	

## WiFi Router

The SCloud WiFi module only supports 2.4GHz WiFi frequency band. It would enable DHCP mode by default, connect to the internet through the WiFi router and share the internet bandwidth with other devices in the router's Network.

Some useful information will be discussed here to help the SCloud user/installer to build a reliable, stable, and secure security system using the SCloud WiFi module.

Every brand of WiFi router has its own limitation, for example:

- Limited number of connected devices/clients
- Limited network bandwidth support
- Outdated WiFi router's firmware
- Misconfigured security rules

## QoS Priority Rules List

Since the internet bandwidth is shared among the devices in the router's network, when the connected device number exceeds the limits of the WiFi router, or someone is watching online movie/video/playing or online games that consume majority of internet bandwidth, some devices in the same router network may not be able to connect to the internet.

In this case, setting up the QoS (Quality of Service) rules in the router may help the SCloud WiFi module to report the security event without bandwidth sharing issues:

The screenshot shows the 'Applications & Gaming' section of a router's web interface. The 'QoS (Quality of Service)' tab is selected. The 'Internet Access Priority' is set to 'Enabled'. Below this, there is a table of priority rules. A red arrow points to the 'High' priority rule for 'USR-C215'.

Priority	Name	Information	Remove	Edit
Medium		MAC	Remove	Edit
High	USR-C215	MAC	Remove	Edit

## Firewall's Rules

There are some brands of WiFi router come with default firewall rules to block unauthorized inbound/outbound data. In this case:

1. Please add a rule/whitelist in the router's firewall to allow outbound data of the SCloud WiFi module:
  - Source Mac Address : **WiFi module's Mac Address**
  - Source Port : **5000**
  - Destination Domain : **app.ssmarttech.com**
  - Destination Port : **5000**
  - Protocol : **TCP**

the specified duration, clients in the white List and other network clients will not be able to access the Internet or any Internet service.

**NOTE :** If you set the subnet for the White List, IP addresses outside the subnet will not be able to access the Internet or any Internet service.

**Network Services Filter**

Enable Network Services Filter ☒ Yes ☐ No

Filter table type **white List**

Well-Known Applications **User Defined**

Date to Enable LAN to WAN Filter ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri

Time of Day to Enable LAN to WAN Filter 00 : 00 - 23 : 59

Date to Enable LAN to WAN Filter ☒ Sat ☒ Sun

Time of Day to Enable LAN to WAN Filter 00 : 00 - 23 : 59

Filtered ICMP packet types

**Network Services Filter Table (Max Limit : 32)**

Mac Address	Port Range	Destination Domain	Port Range	Protocol	Add / Delete
	5000		5000	TCP	+
No data in table.					

**Apply**

[Help & Support](#) [Manual](#) | [Utility](#) [FAQ](#)