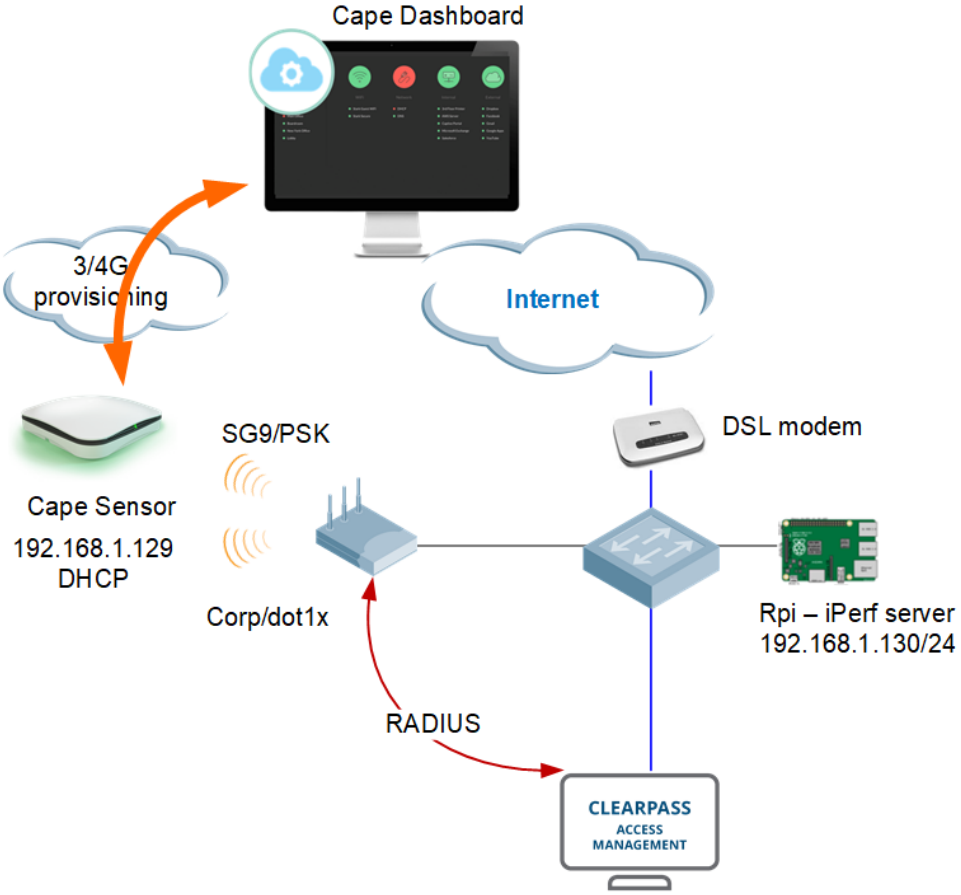
1 Table of Contents

Table of Contents

2 Introduction

The main objection of this document is to be able to understand the Service Assurance Sensor capabilities and to be able to effectively demonstrate them in a Proof of Concept (PoC).

Service Assurance Sensors provides the visibility of network based services by simulating real-world user and client experiences. It continuously tests network and connectivity performance in high-value locations like office spaces, auditoriums, high density areas and remote offices.



Here is our lab setup, which is pretty straight forward, I have included Rpi as an iPerf server but you can run it on any device that support iPerf application.

2.1 Things you need

- Aruba Service Assurance Sensor
- Optional iPerf sever
- Aruba Instant APs to provide WiFi for Cape tests
- Optional ClearPass for dot1x authentication

Also note that all the Service Assurance documentation is available online from here.

https://cape.readthedocs.io/en/latest/

3 Service Assurance Sensor Initial Setup

Service Assurance Sensor (Cape Sensor) is a very simple device and the main aim here is to simulate a client device to be able to automatically test a number of workflow and then time stamp it so that we can see the trend or an issue.

The Sensor runs a simple zero config process, it

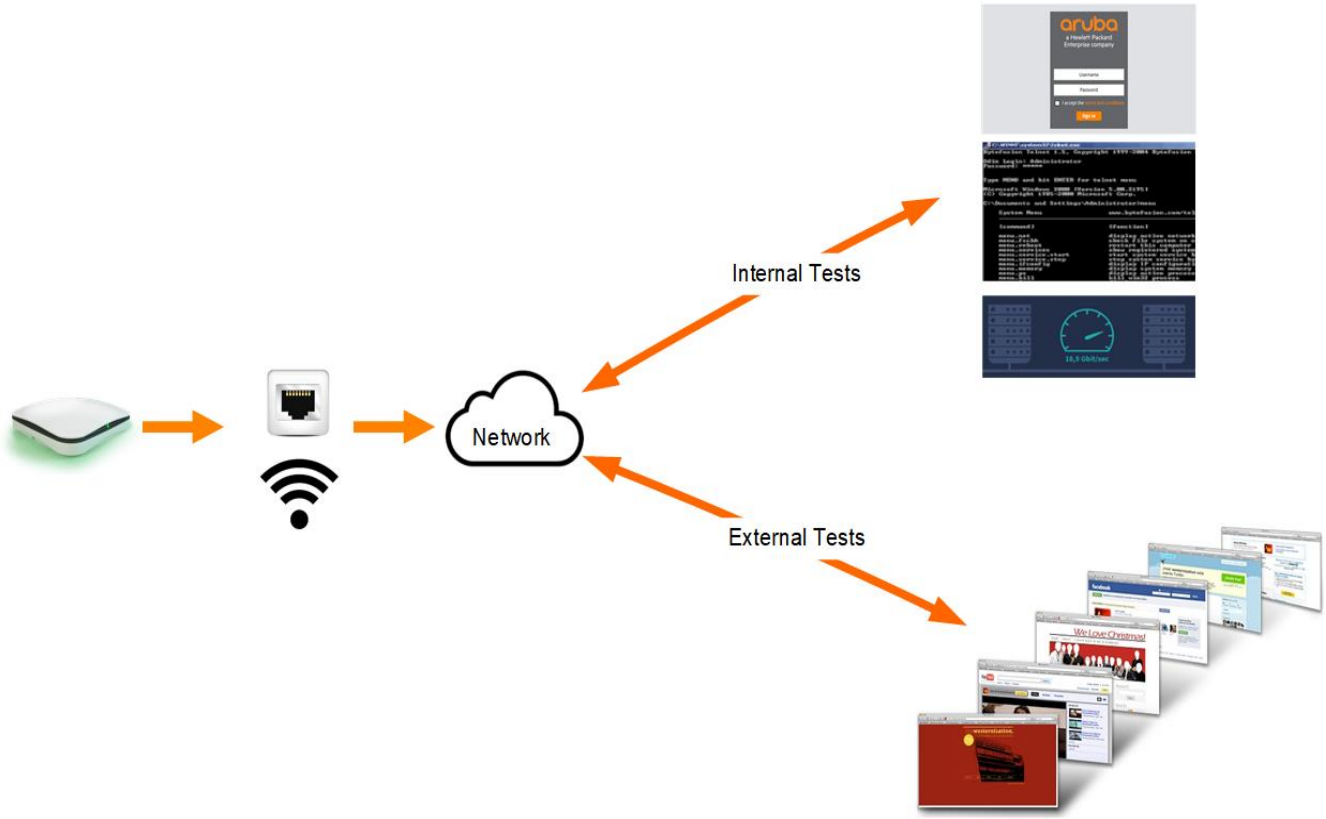
- Has 1x GigE PoE interface
- Supports 802.11n WiFi on supports both 2.4 and 5GHz (the newer models will support 11ac)
- Has a cellular connection to get its initial config from the Service Assurance cloud.
- Has a Chrome browser that can be used for various tests
- Power adapter to power up the unit.

3.1 How it works

You basically power it up either with PoE or power adapter, it will then either use wired connection if present or cellular to contact Service Assurance Cloud to register and then download its configuration, networks it needs to connect to for various test that it need to perform. The sensor has an ID that is used for its registration. Besides powering up the unit, there is nothing else to be done for this sensor to be operational.

It is important to note that in the countries that the sensor is not certified for it will not be able to connect via cellular, in those cases then you need to ensure wired connection to internet for it to be able to reach Service Assurance cloud.

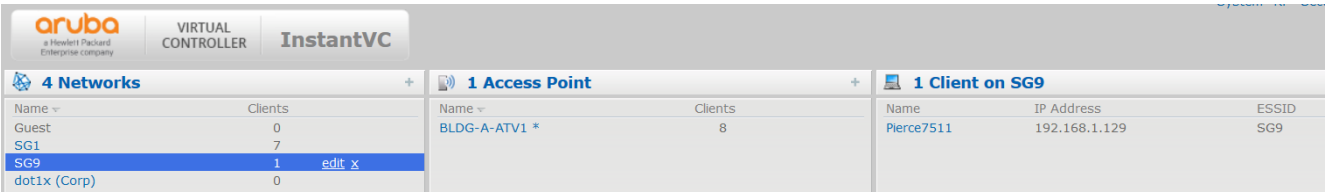
The sensor runs the tests that it needs to perform 24x7 continuously, some tests can be scheduled as well.



The sensor then runs the end to end tests. It can check connectivity to an SSID, association time, time it takes for DHCP, DNS and Authentication. Then it can go on to test Captive portal and other gateways and finally can check for web pages loads, throughput, etc. and reports all these to Service Assurance dashboard.

3.2 Aruba Instant Configuration

Here we are using instant AP to configure two WLANs, one is SG9 which is PSK based and the other is Corp which is dot1x based authentication.



3.3 Service Assurance Sensor Setup

Once you have received your sensor, you need to power it on and go through the 2-minute setup process to configure SSID's and testing profiles. Beforehand you need to send the Sensor ID and its MAC address to the Service Assurance team so they can add it to your Service Assurance dashboard and also provide you with your login credentials.

Now you can either power up the sensor with power adapter that cones with the sensor or using PoE. Note that sensors have a 3G/4G cellular connections and if that is certified in your country you can make use of it so that the sensor can register with the Service Assurance dashboard, otherwise you can power it up and connect it to Ethernet LAN and as long as it has access to the Internet it can contact and register with the Service Assurance dashboard.

Once you have powered up your sensor note the status LEDs. The Service Assurance Sensor has only one visible LED and its status is as indicated below.

- **Purple:** Powered on
- **Blue:** Booting
- **White flashing:** Software starting
- **White:** Software started
- **Green flashing:** Waiting for configuration
- **Green:** Testing your network
- **Yellow:** Power outage
- **Orange:** No connectivity
- **Red:** Sensor issues

The URL for your Service Assurance dashboard is https://dashboard.capenetworks.com/ and based on your credentials you should see your sensors.

4 Proof of Concept Setup

Before starting a PoC, most likely you need to figure out how many sensors do you need. Generally you need to have one sensor in every area where you have a group of users/devices or areas with Wi-Fi performance issues. For the wired testing with multiple access and aggregation switches, perhaps you want to place one sensor per access switch.

4.1 Whitelisting of URLs

Here is the list of URLs that sensors need to communicate with.

- The primary URL for all sensor configuration/test

  https://device-gateway.capenetworks.io

- For sensors to upload results, and to download OTA (over the air) firmware updates, tools, and patches:

  https://cape-device-binaries.s3.amazonaws.com

  https://cape-build-artefacts.s3.amazonaws.com

  https://cape-storage-service.s3.amazonaws.com

- For testing external connectivity

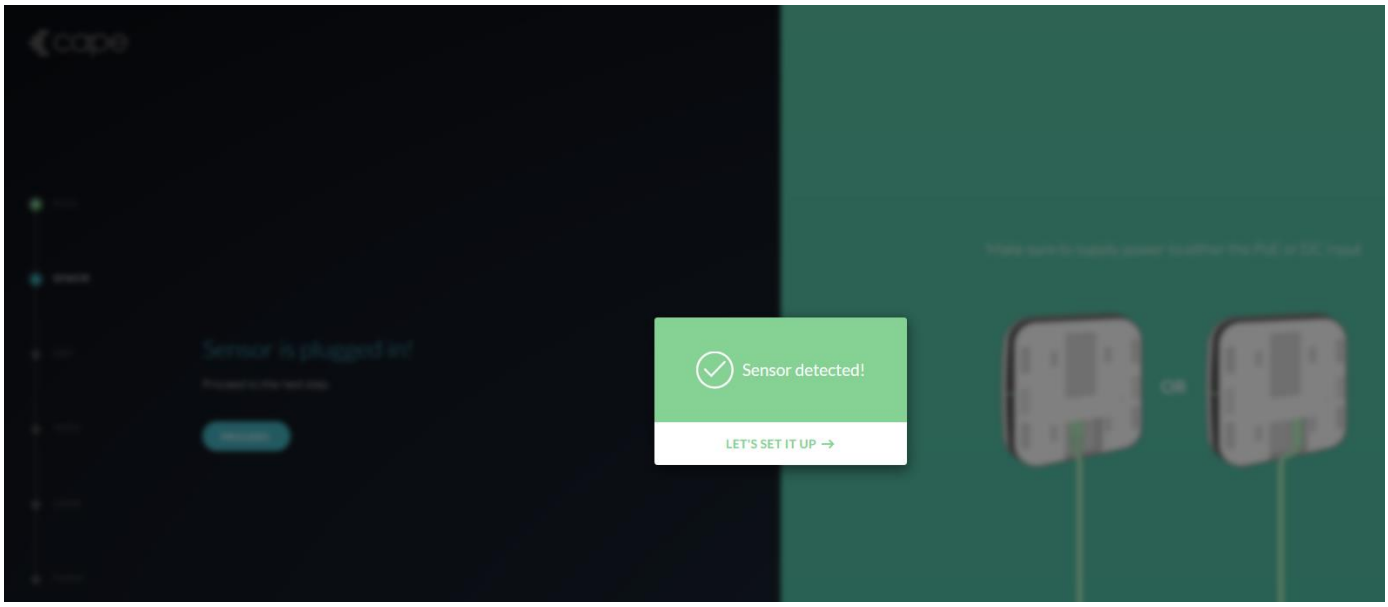
  http://cdn.capenetworks.io/auth

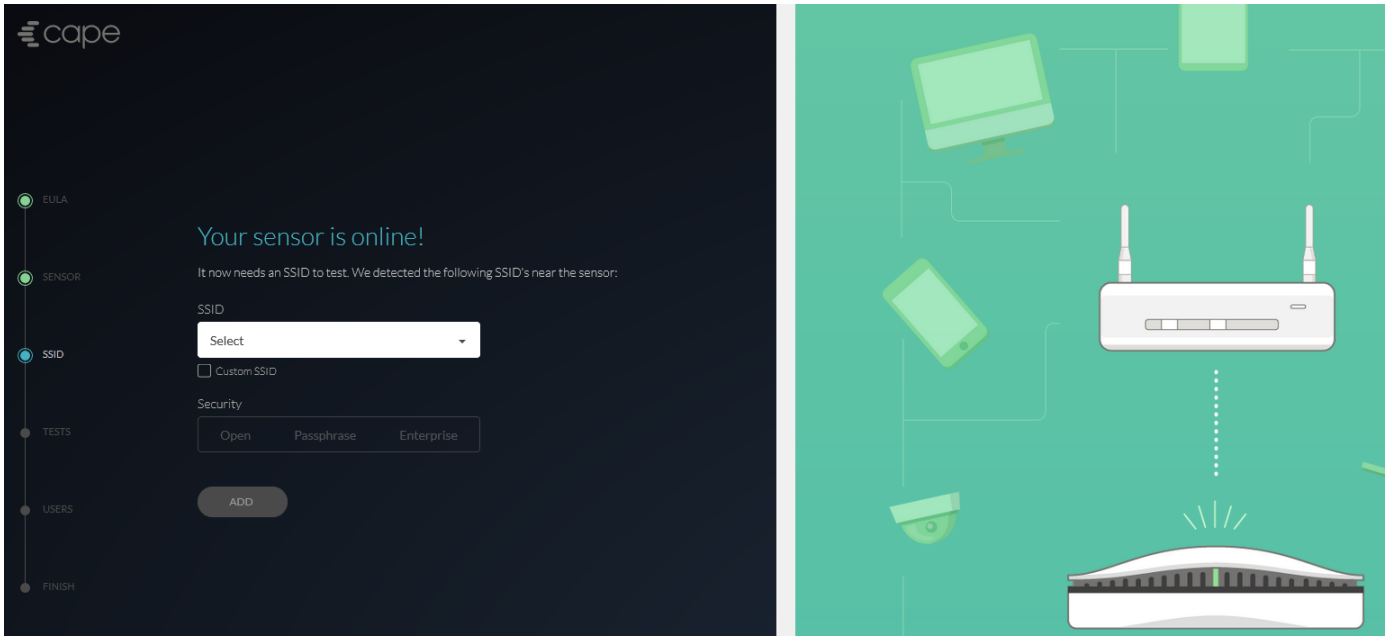
  http://35.241.22.134/auth.html

  http://captive.apple.com/hotspot-detect.html

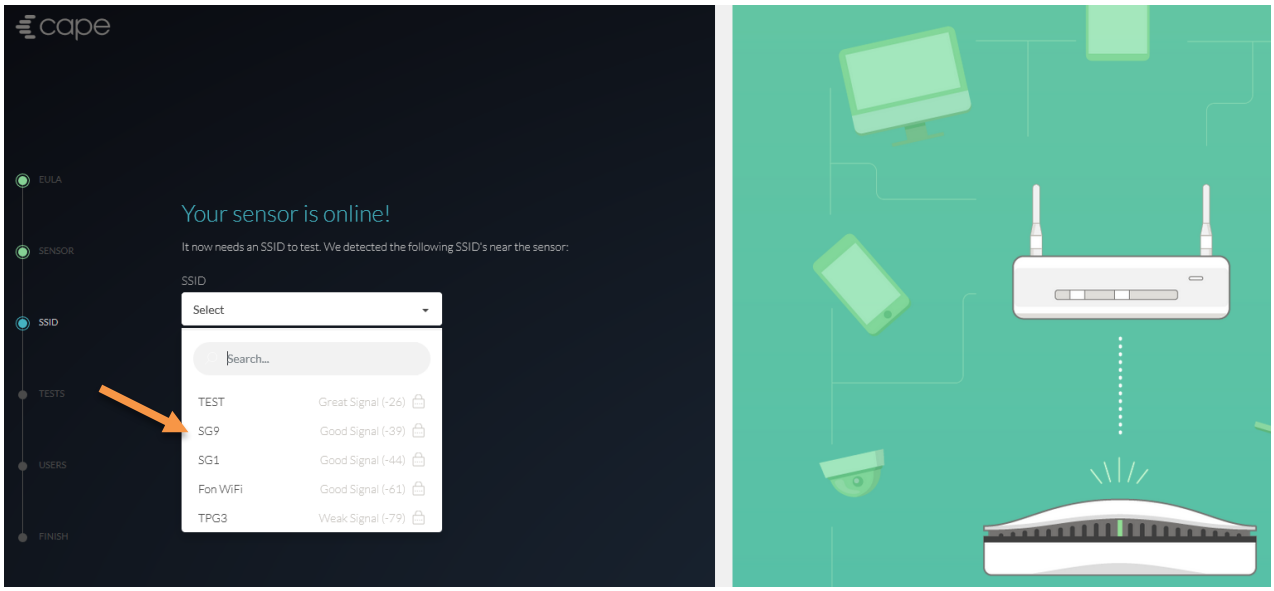
4.2 Initial Setup

Once the Service Assurance team has added you to the Service Assurance dashboard, you can login and then go through the initial setup as you can see from the following screenshots.

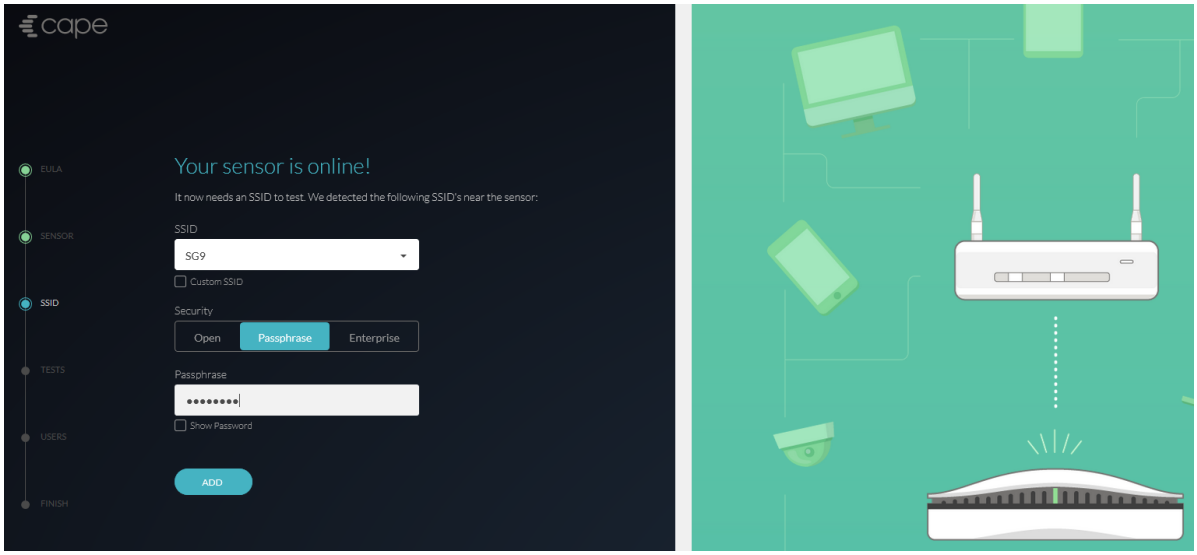




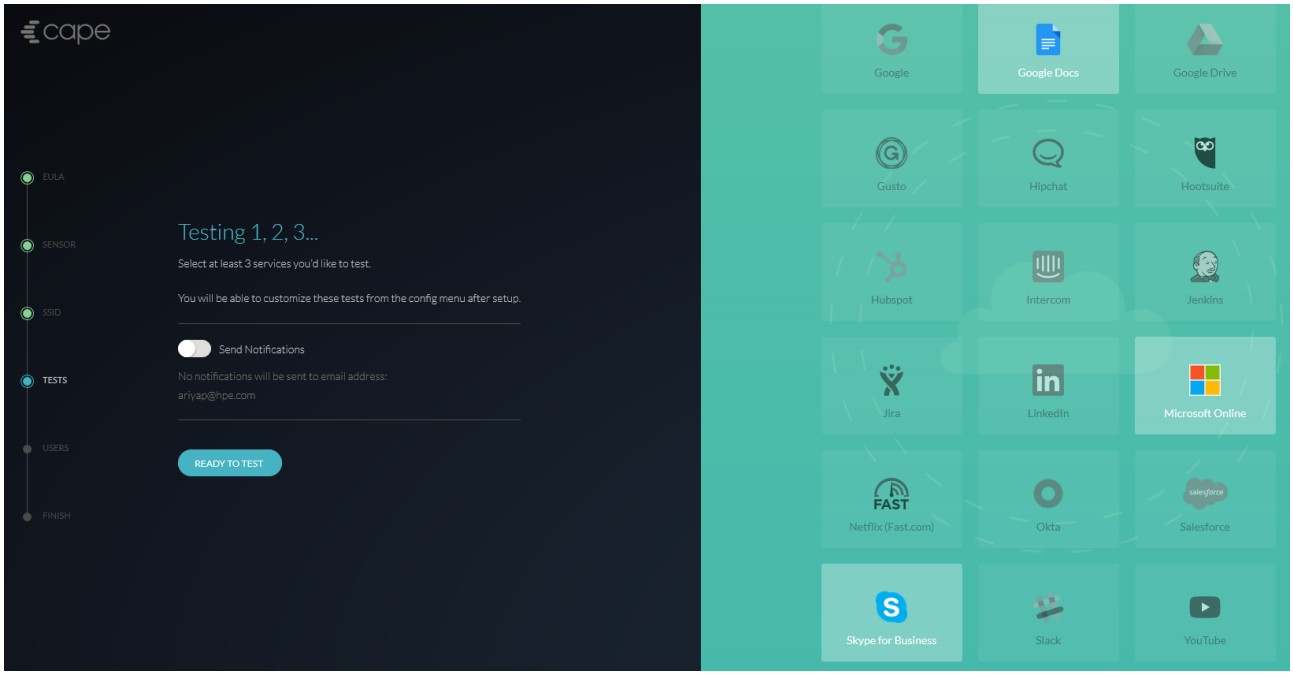
You should note that once the Service Assurance Sensor is powered up it will detect the SSIDs that are broadcasting around it. Here as you can see it has picked about a few SSID and you can choose to select one of them or if you want choose the custom setting. In our case we'll choose SG9 that have been configured on the Aruba Instant AP.



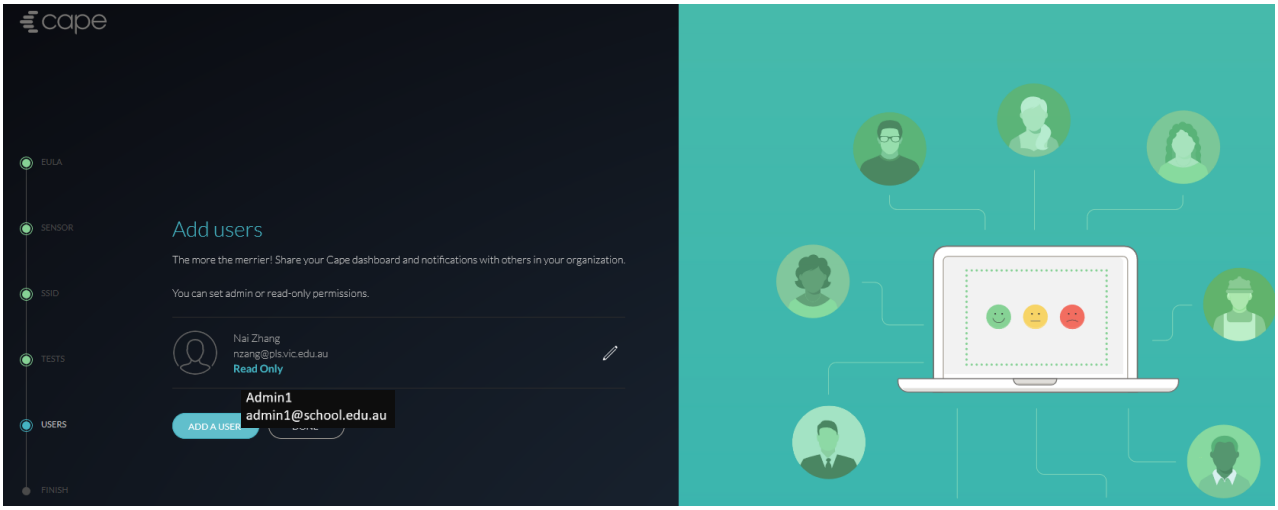
Here we select SG9 that is PSK based WLAN.

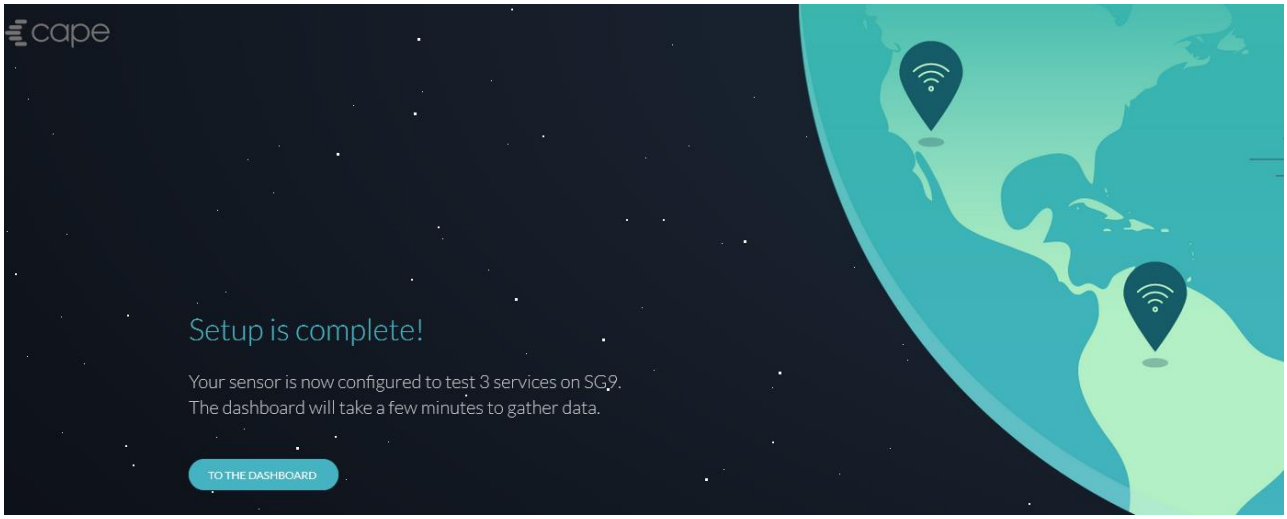


And finally select at least 3x tests for the sensor to run. Later we can change all these test as well.



You can also add a number of other users to be able to view the dashboard.

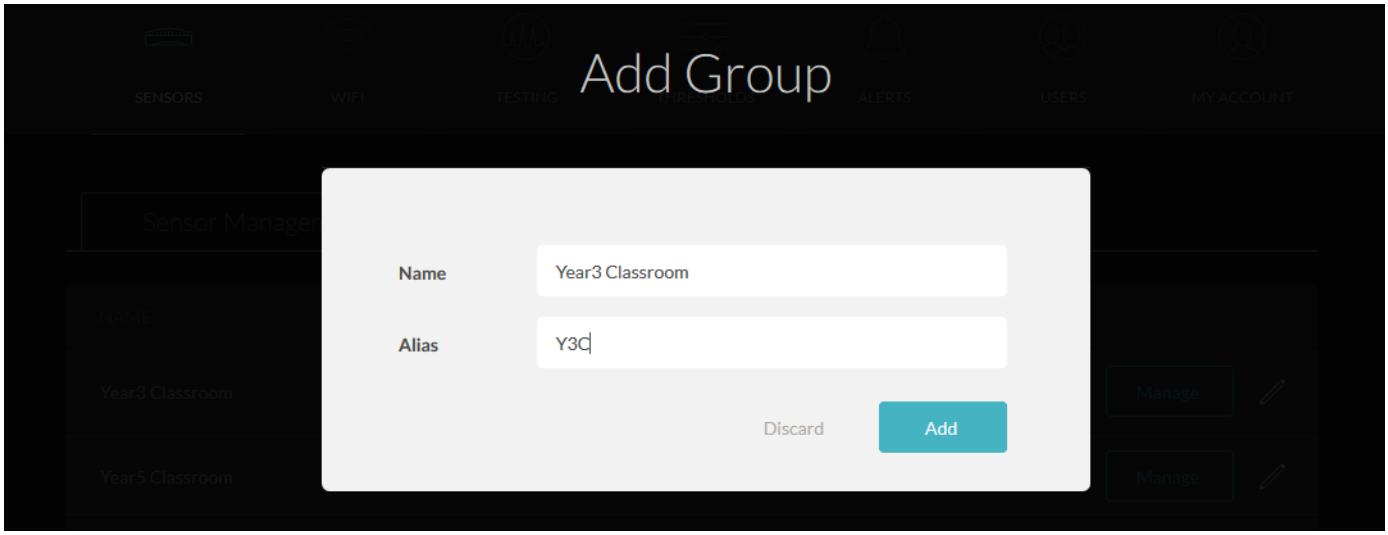




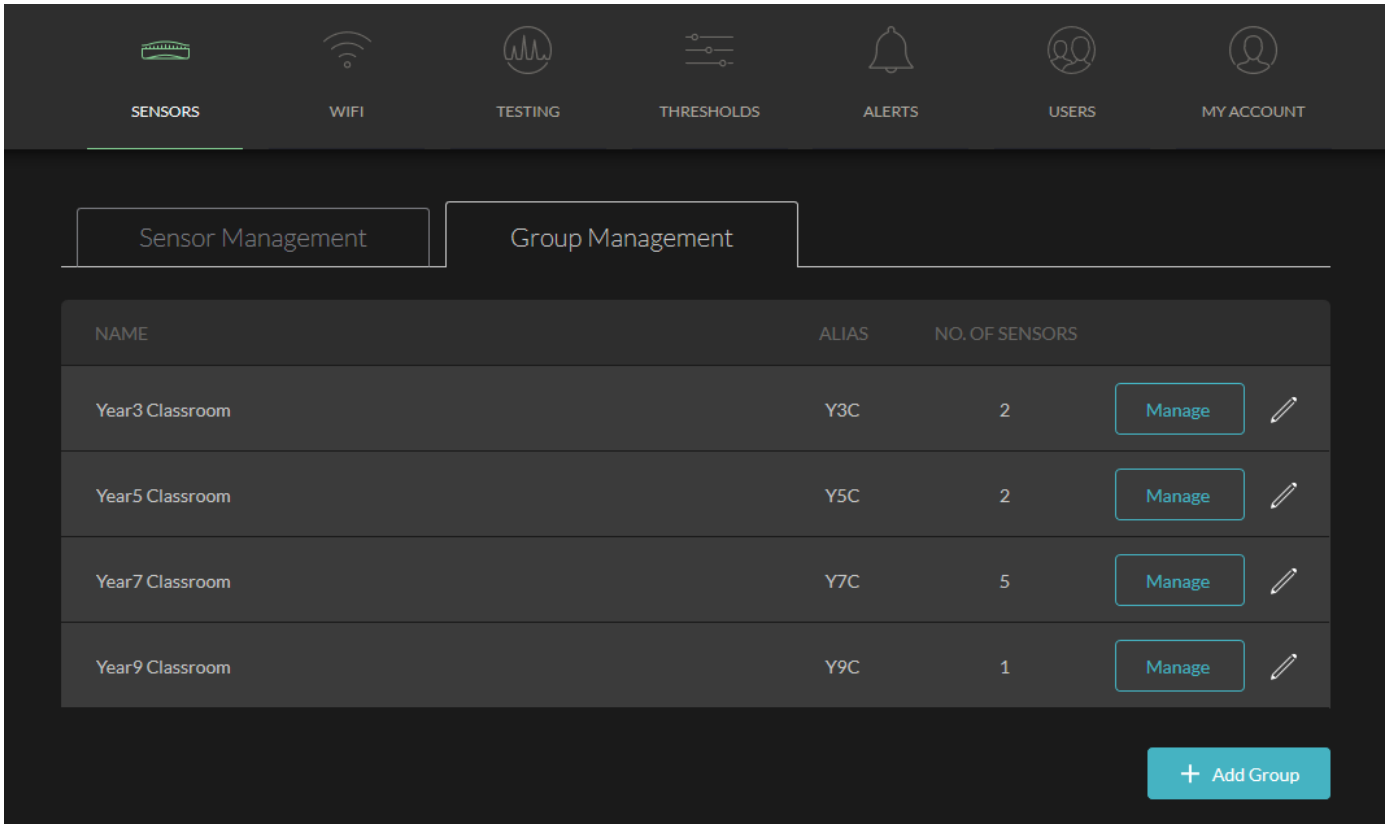
4.3 Group Management

In most of the PoCs you might want to have a number of sensors in a specific area to run specific tests. For this we have to configure different groups.

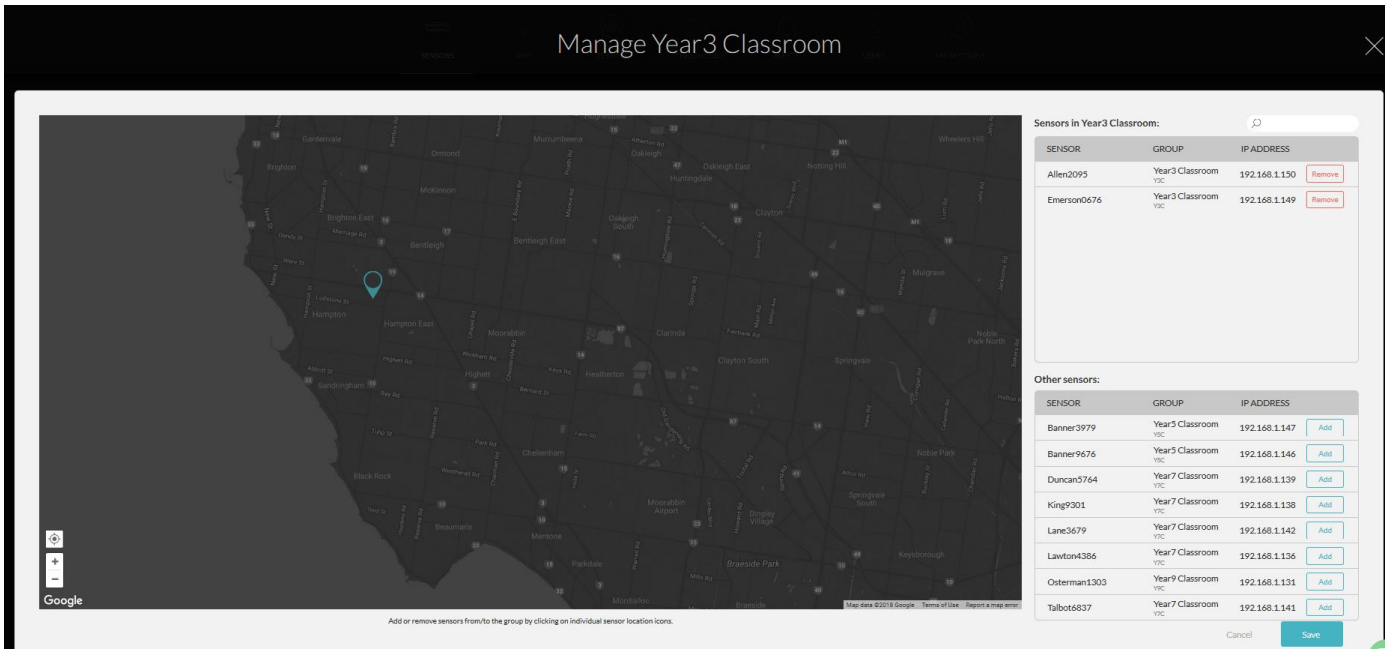
Here we are creating a group called Year 3 Classroom group.



And here are the other groups that I created.



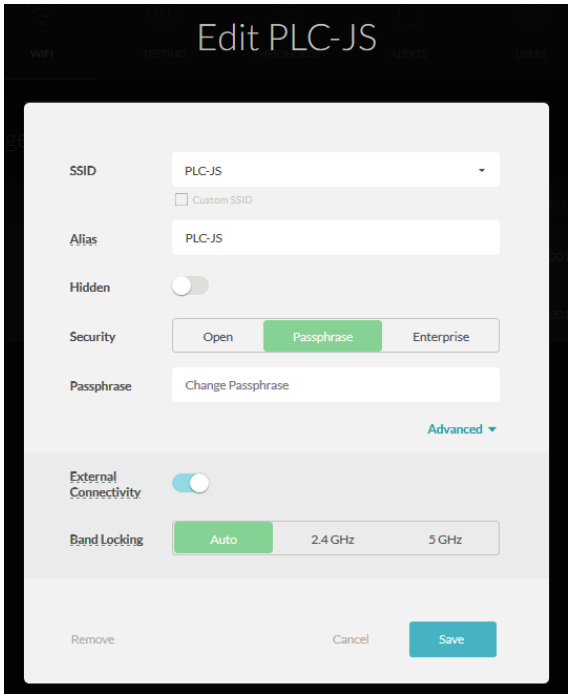
Then you need to click on the "Manage" button to add a specific sensors to each group. This is how you can run specific WLANs, test for each group.

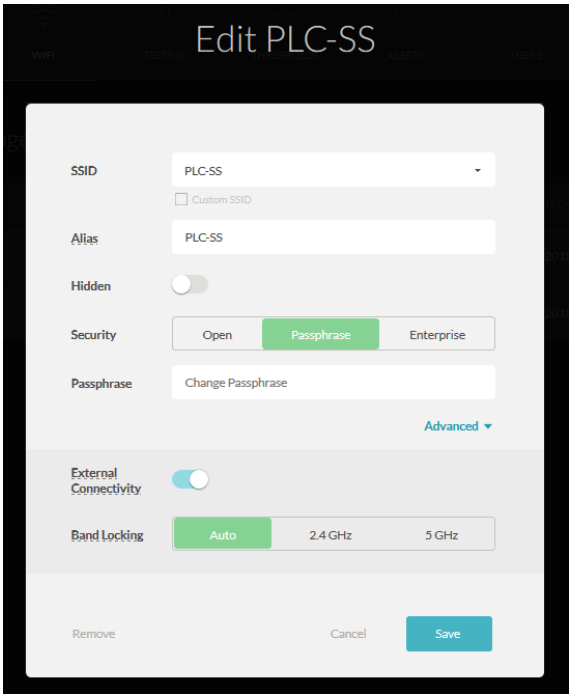


4.4 Wireless PSK Configuration

In most of the PoCs you'll have PSK and Dot1x wireless networks that you want to test.

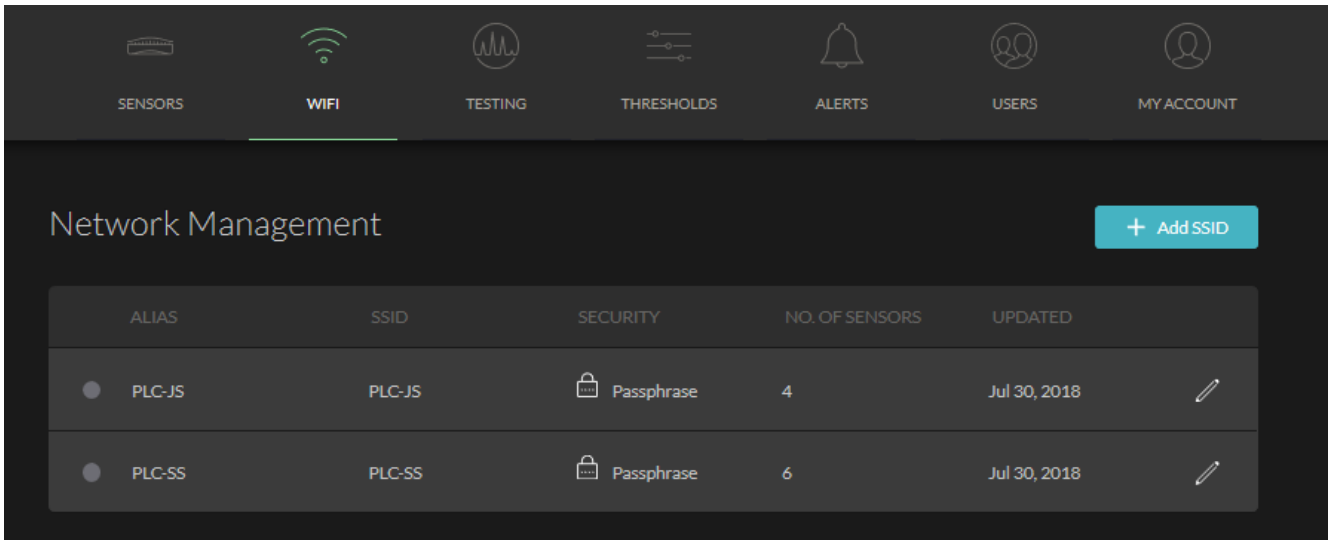
Here we are showing that you can configure two PSK based SSIDs (PLC-JS and PLC-SS) and then used each of them for a specific set of sensors based on the sensor group management. In this example each of these SSIDs are being broadcasted in part of the campus and hence why we need to assign a set of sensors to test a specific SSID.





Once you have added the SSIDs, then you can assign which WLANs needs to be test for each of the sensors.

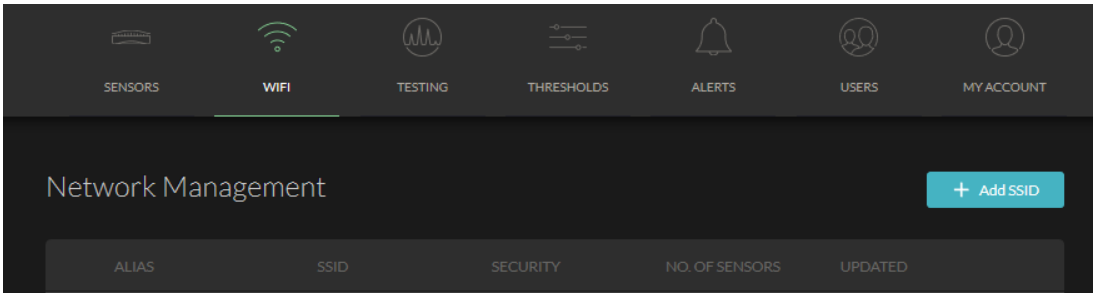
Note that currently the max 3 SSIDs can be tested by any sensor.



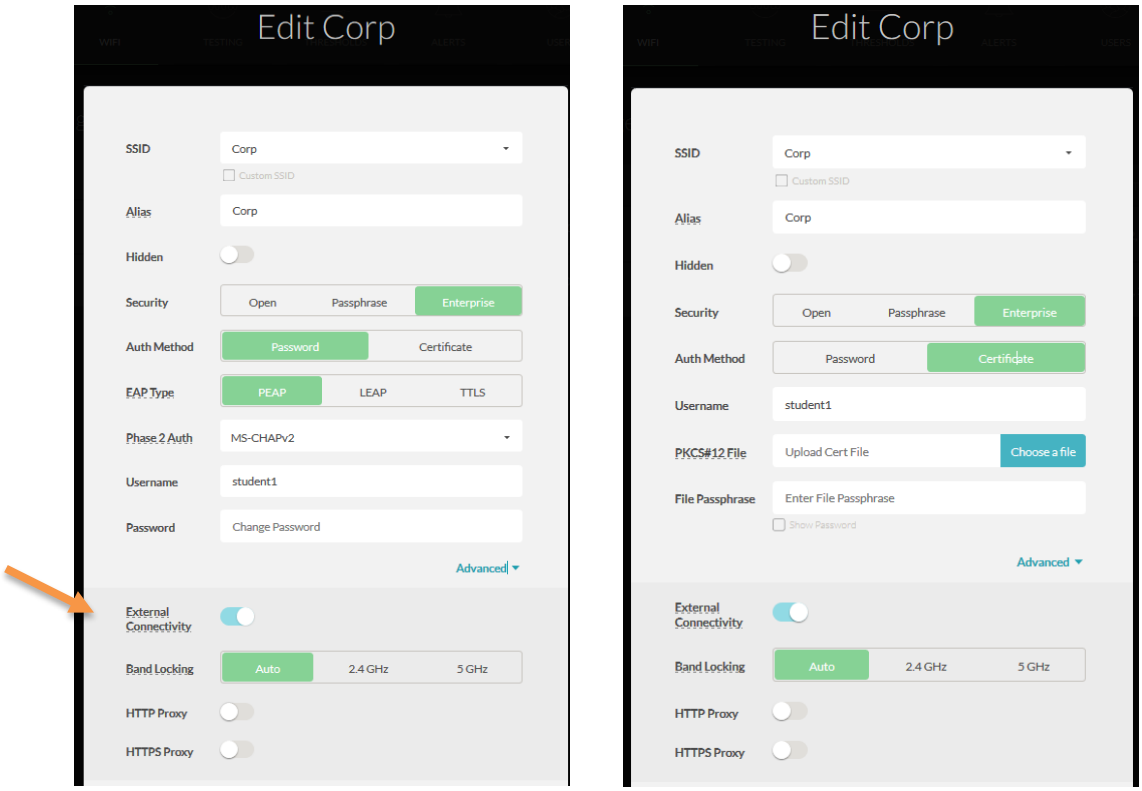
The sensor will disassociate from one SSID, associate to the next SSID and run the full set of tests. More than 3 SSIDs causes the data to become sporadic and there is a long wait period for the sensor to retest that SSID after a full loop.

4.5 Wireless dot1x Configuration

To add a new SSID you go to the setting and then WiFi as shown below.



Here we are showing dot1x SSID Corp and will also configure a test user as it will be using EAP-PEAP as authentication. As you can see the sensors support EAP-TLS as well.



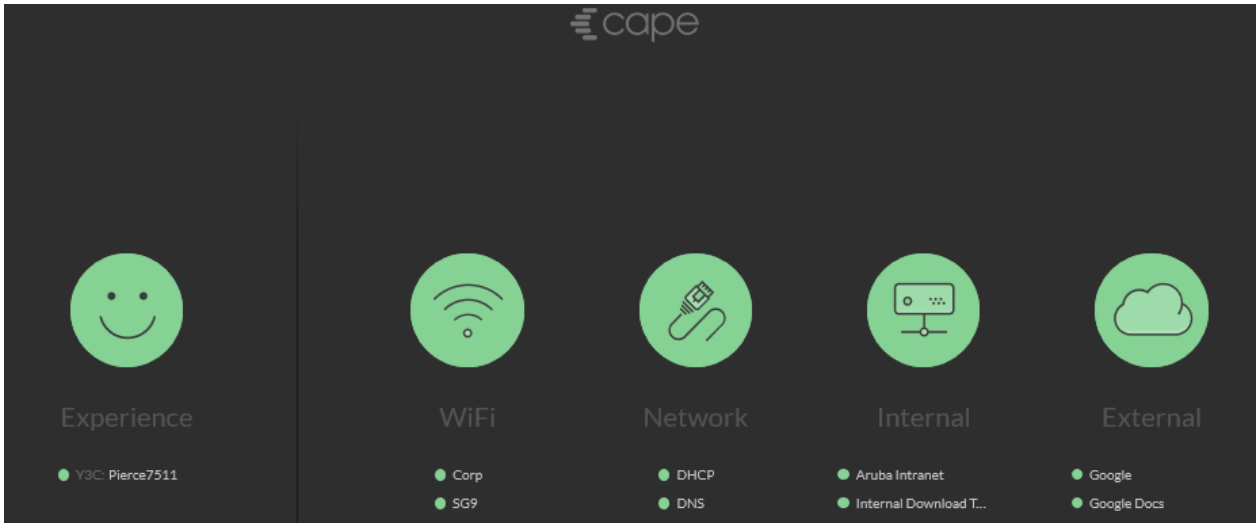
You can also lock a WiFi test to a particular band as shown above. This means that sensors will only connect to the SSID and test it on the specified band. An SSID can be locked to 2.4 GHz only, 5 GHz only, or set to “Auto”. In Auto mode, which remains the default setting, the sensor will choose the best band to connect to similar to a regular client.

Also note the External Connectivity Override which can be disabled on any specified SSID (or alias). Toggling this will disable testing, errors, and notifications related to external connectivity. This is helpful for networks where external connectivity to the internet is not supported or no DNS servers are configured. If no external connectivity is available via Wi-Fi or Ethernet, Service Assurance Sensors will upload test results via built-in cellular connectivity.

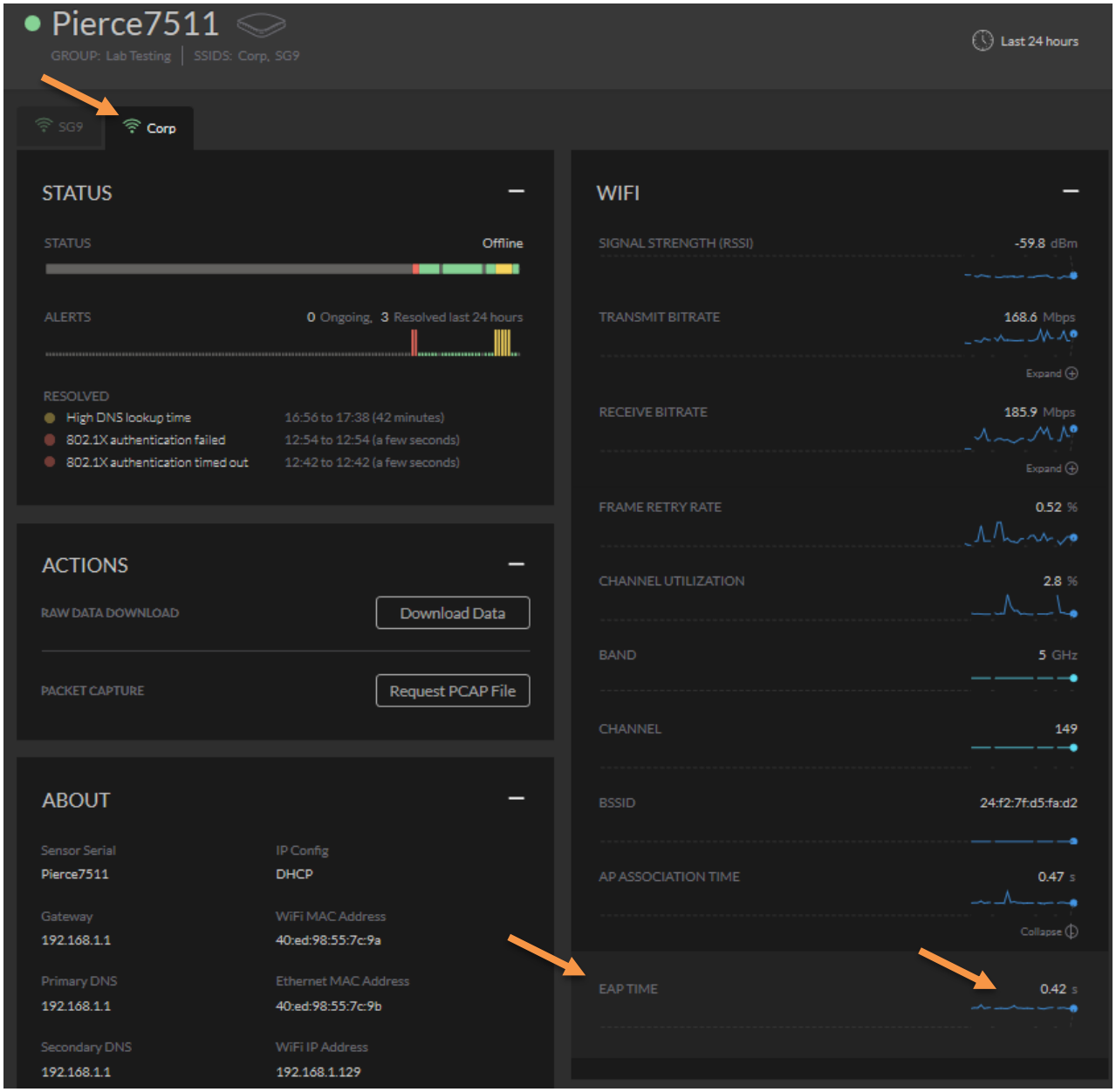
4.6 Client EAP timing Visibility

Service Assurance Sensors can also provide Extensible Authentication Protocol (EAP) timing as a new metric that is tracked historically. Tracking EAP timing can help to identify issues with 802.1X (i.e. RADIUS authentication) performance.

You can see the EAP timing by clicking on your specific sensor under Experience

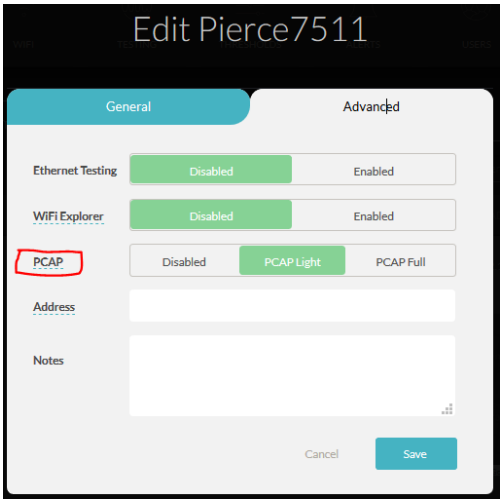


Choosing the dot1x WLAN which is Corp in our case



4.7 Packet Capture

You can also request a packet capture by clicking on the “Request PCAP File”. The dashboard will inform you when the PCAP will be ready so you can download it. By default each sensor is already configured with a real-time rolling pcap buffer. It will capture packets as soon as an issue is detected.



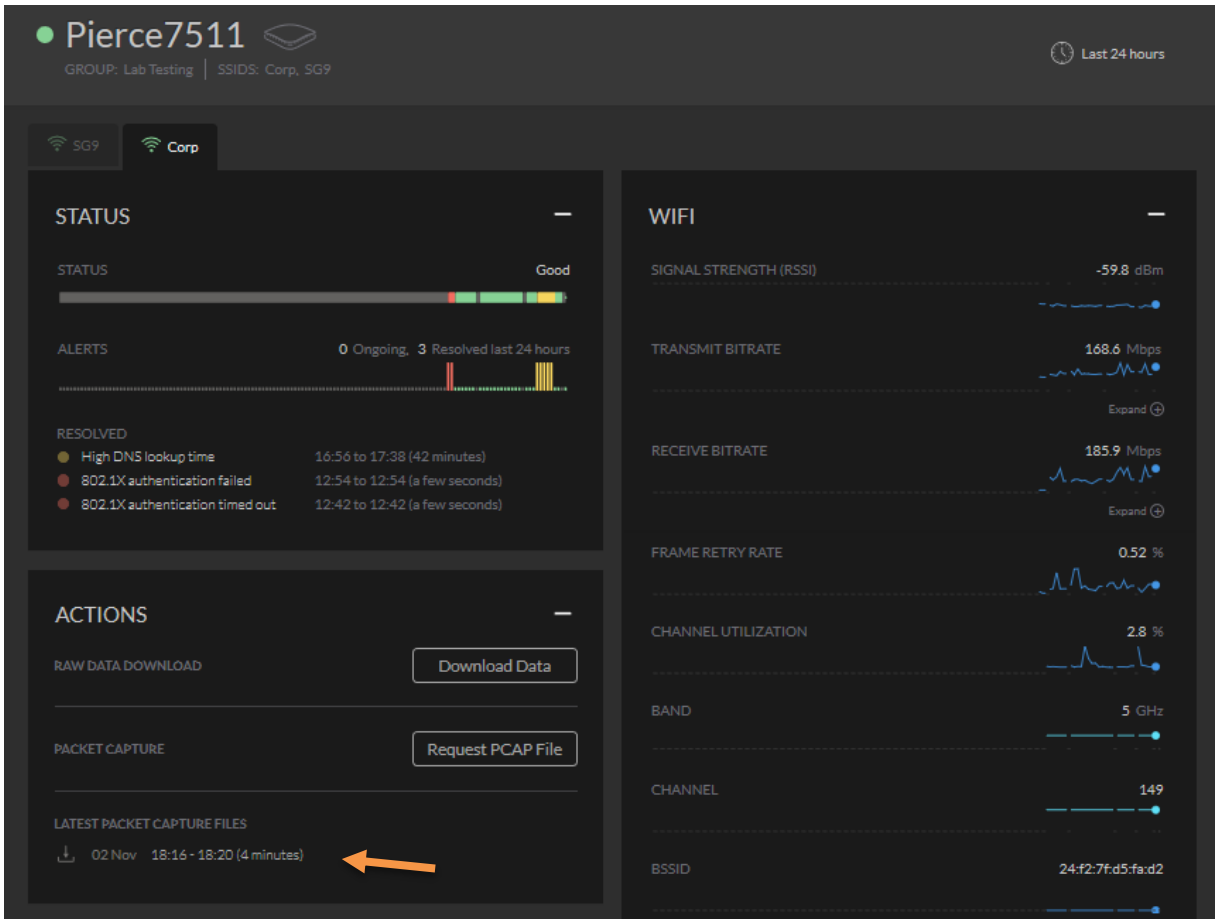
You can configure the pcap setting from by selecting the “Advanced” tab when editing a sensor.

As you can see it has three modes, when you hover your mouse over PCAP, it will give you the definition of the PCAP light and full.

PCAP Light: the sensor will only upload a PCAP file on the first discovery of an issue.

PCAP Full: the sensor will upload a PCAP file on the first discovery and confirmation of an issue.

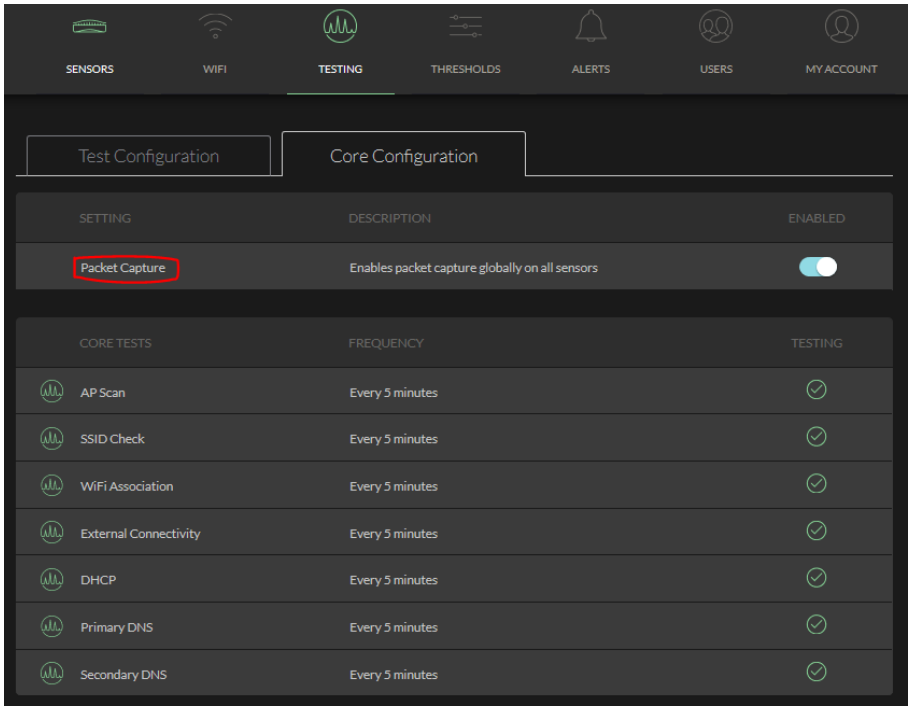
So now going back the previous screenshot you can click on the “Request PCAP” button and view the packet packer file.



Now you can download the pcap which will be in zip format.

Name	Type	Compressed size
Pierce7511-1541142964.pcap	Wireshark capture file	12,116 KB

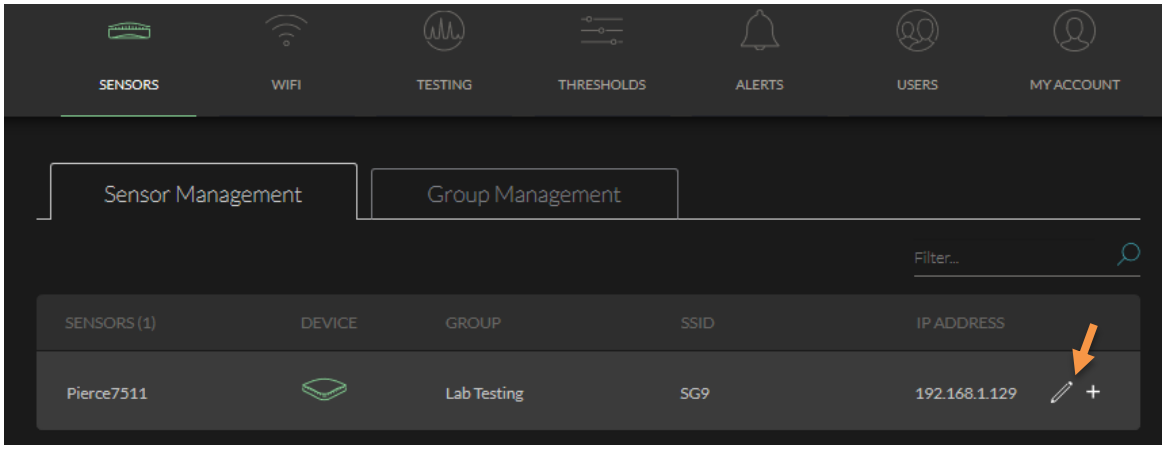
Last thing to note is that you can disable pcap on all the sensors globally and then enable it individually on specific sensors.



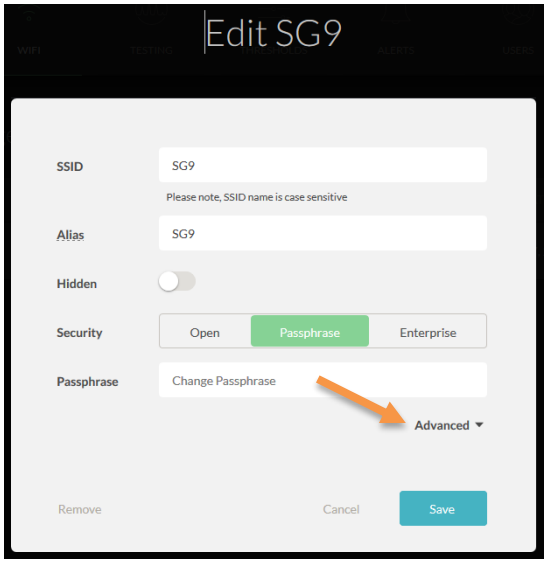
4.8 Network Proxy Configuration

In most of the cases there will be a network proxy in place and you need to configure the sensors to use it. From the dashboard you click on the settings.

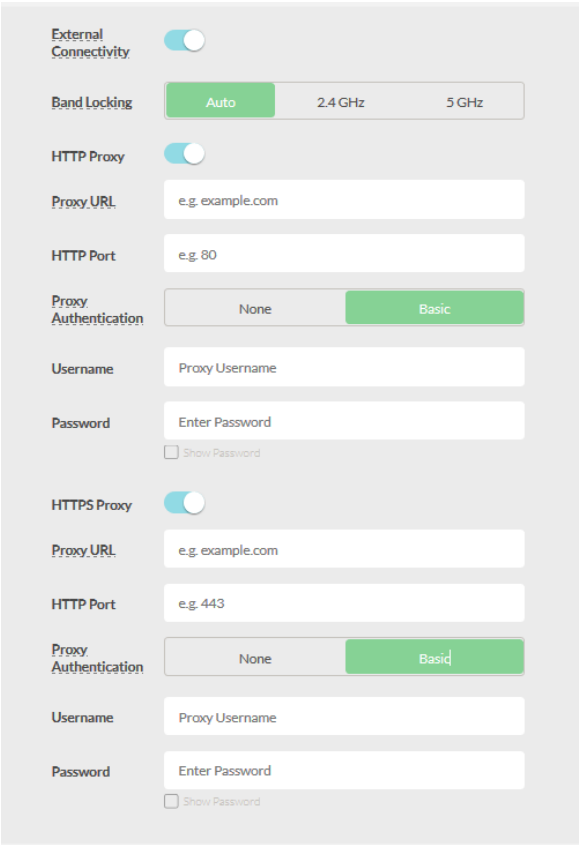
The select the sensor or a group and click on the pencil icon to edit it.



You then click on the “Advanced” button.

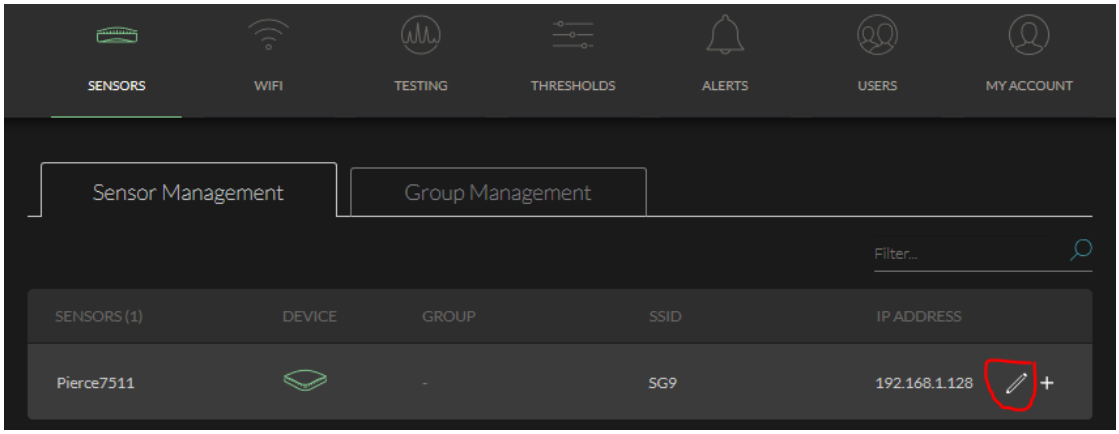


The advance button gives you the options to lock the sensor to a particular WiFi band and to allow proxy access.

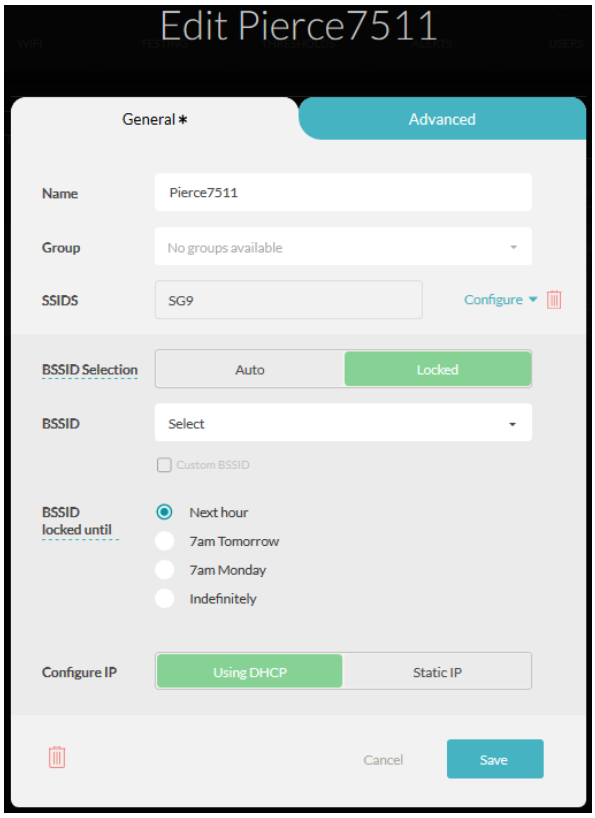


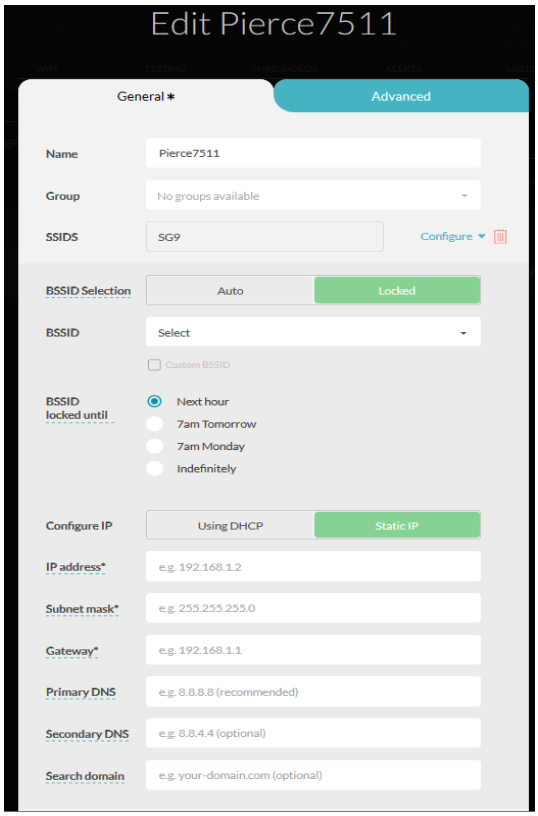
4.9 BSSID Locking and Static IP address

Service Assurance Sensors by default, test the client experience with the BSSID selection criteria based on RSSI, throughput, and probability the connection is stable. However, at times you will want to see what other parts of your network are doing, or what the experience is like for clients which might have a different BSSID preference (This is because BSSID selection methods are vendor specific). To do this you can lock the sensor to test only your BSSID of interest, this will ensure that you get the full view of how that radio is functioning on your network.



Click on configure next to the SSID name and then select the BSSID you would like to test from the drop down menu, or type in a BSSID by choosing custom. Do the same for every SSID you would like to enable BSSID locking for.

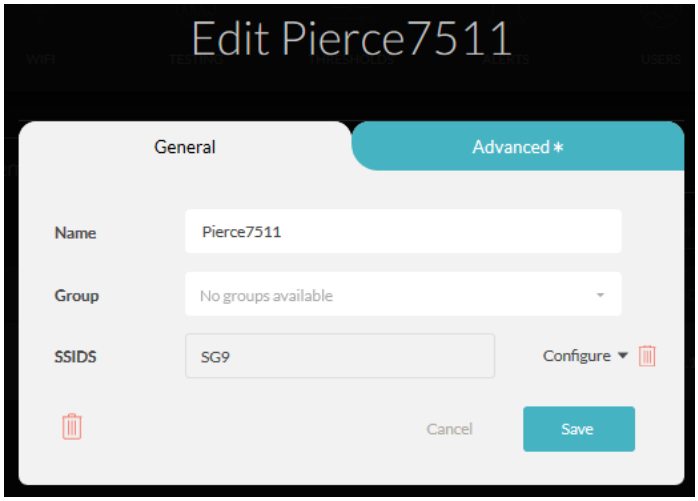




You have the option to enable locking permanently or for a specific period of time

4.10 Ethernet Testing

You can also enable Ethernet testing and generally this is a great way to compare the test results of a wireless test against a wired test. So you select a sensor as before and click on the Advance tab.



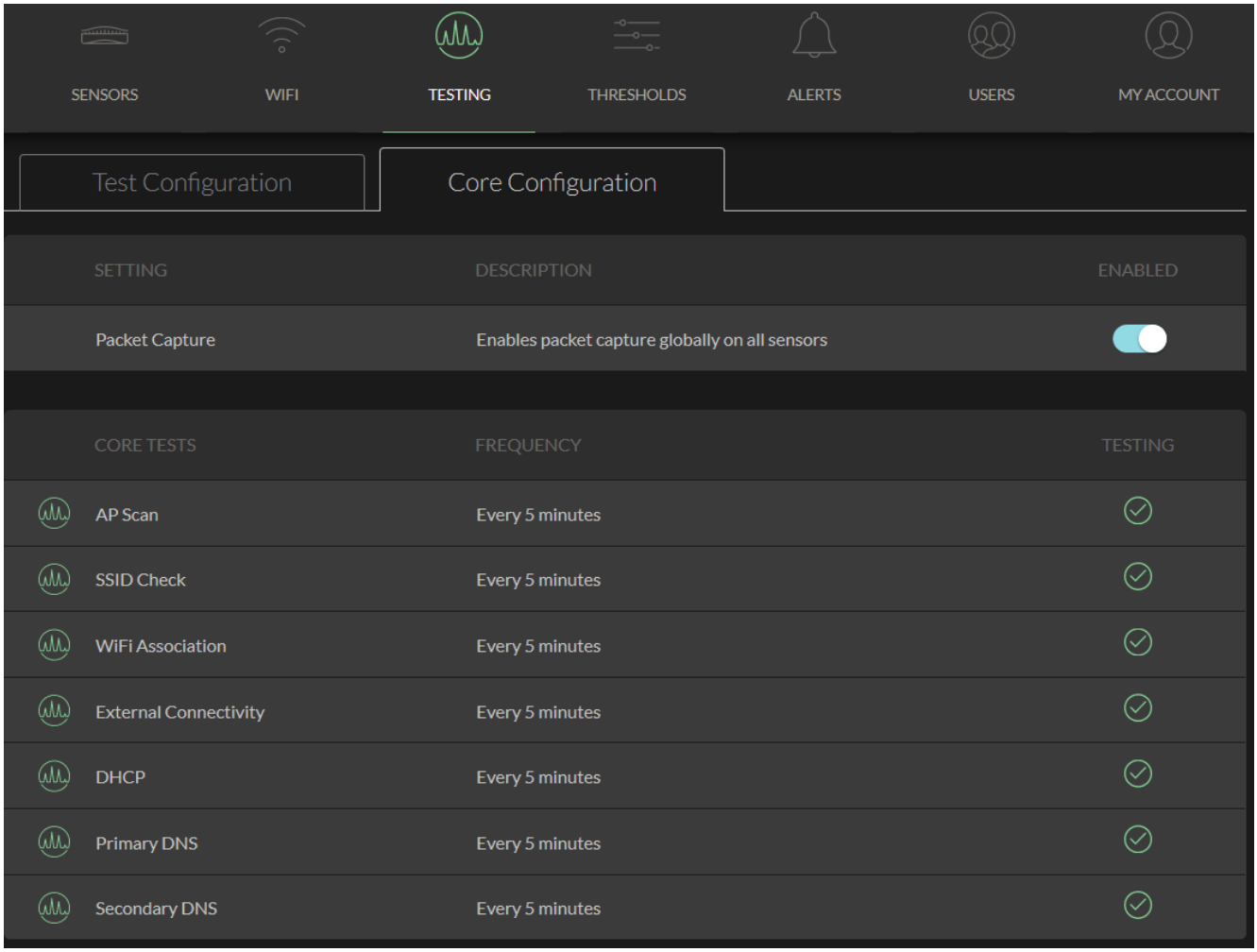
Also note that the sensors support WiFi Explorer. This allows the sensor to be used as WiFi Explorer Pro remote sensor. When this is enabled the sensor will listen on port 26999 for WiFi Explorer pro connections.

WiFi Explorer is uses Mac's built-in Wi-Fi adapter to scan, monitor and troubleshoot wireless networks.

Additional viewing options in WiFi Explorer Pro let you organize scan results by SSID, access point or access point radio to better visualize multiple networks per access point.

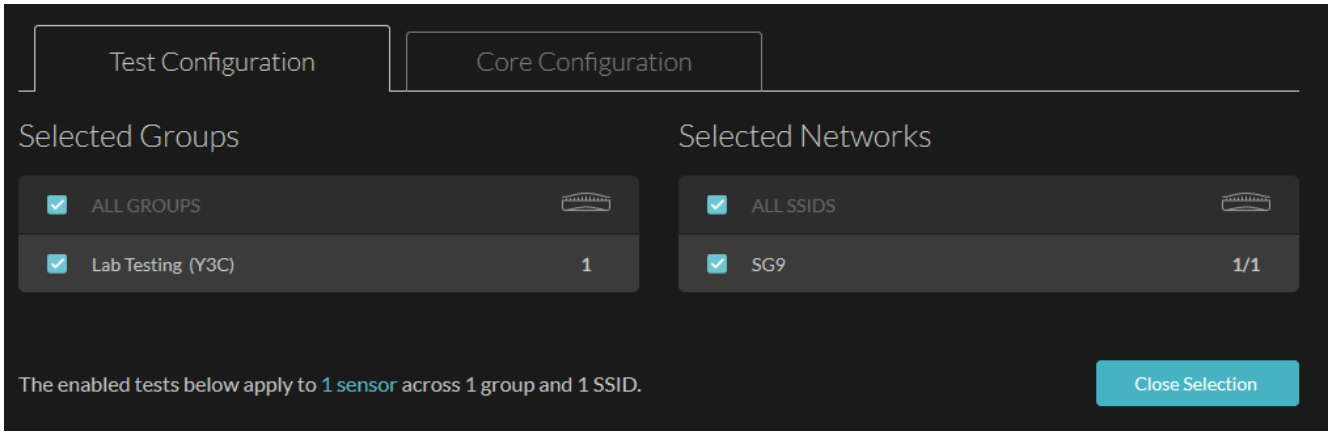
5 Sensor Tests

Here we'll discuss a number of tests that sensors can run. There are two broad categories of tests as shown below. The Core tests are enabled by default.



You don't need to do anything on the core test except if you want to disable packet capture.

Now for the main test configuration you can select the groups and the WLANs for each test as shown below.

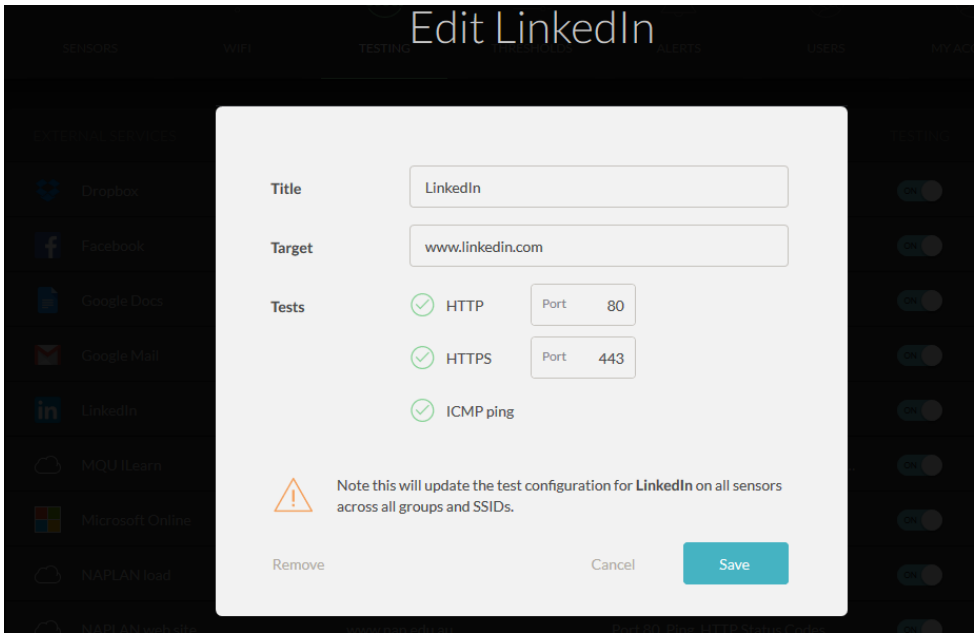


Once you have selected the groups and networks then you can turn on each of the predefined tests.

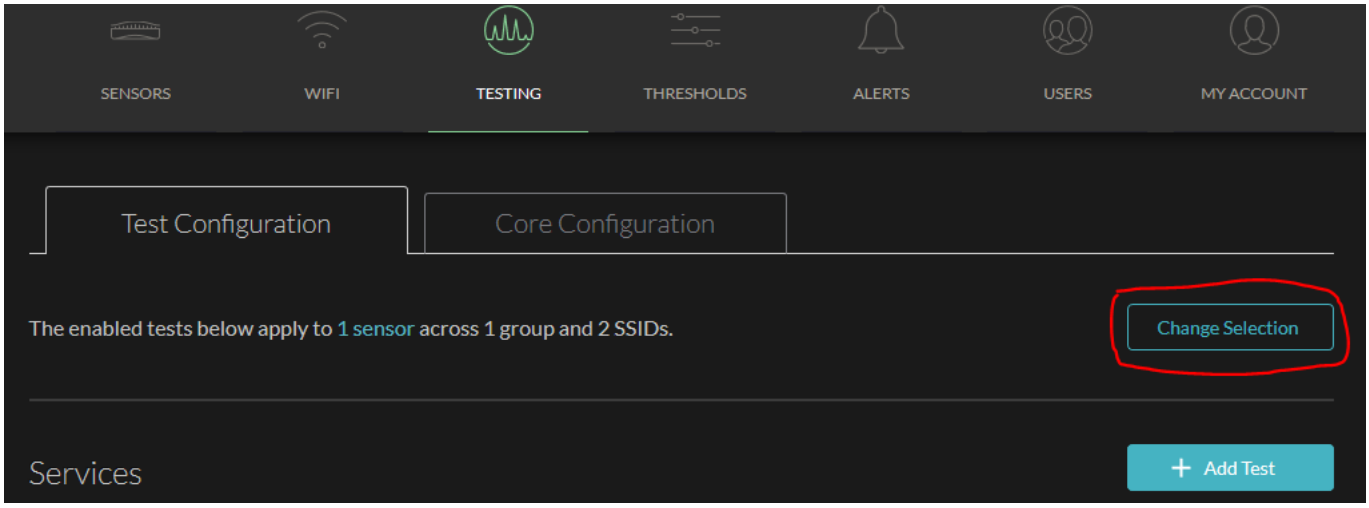
Here is a sample of the tests. Notice that there are internal and external tests. The internal tests are the web based application on the customer's network while External tests are Internet based.

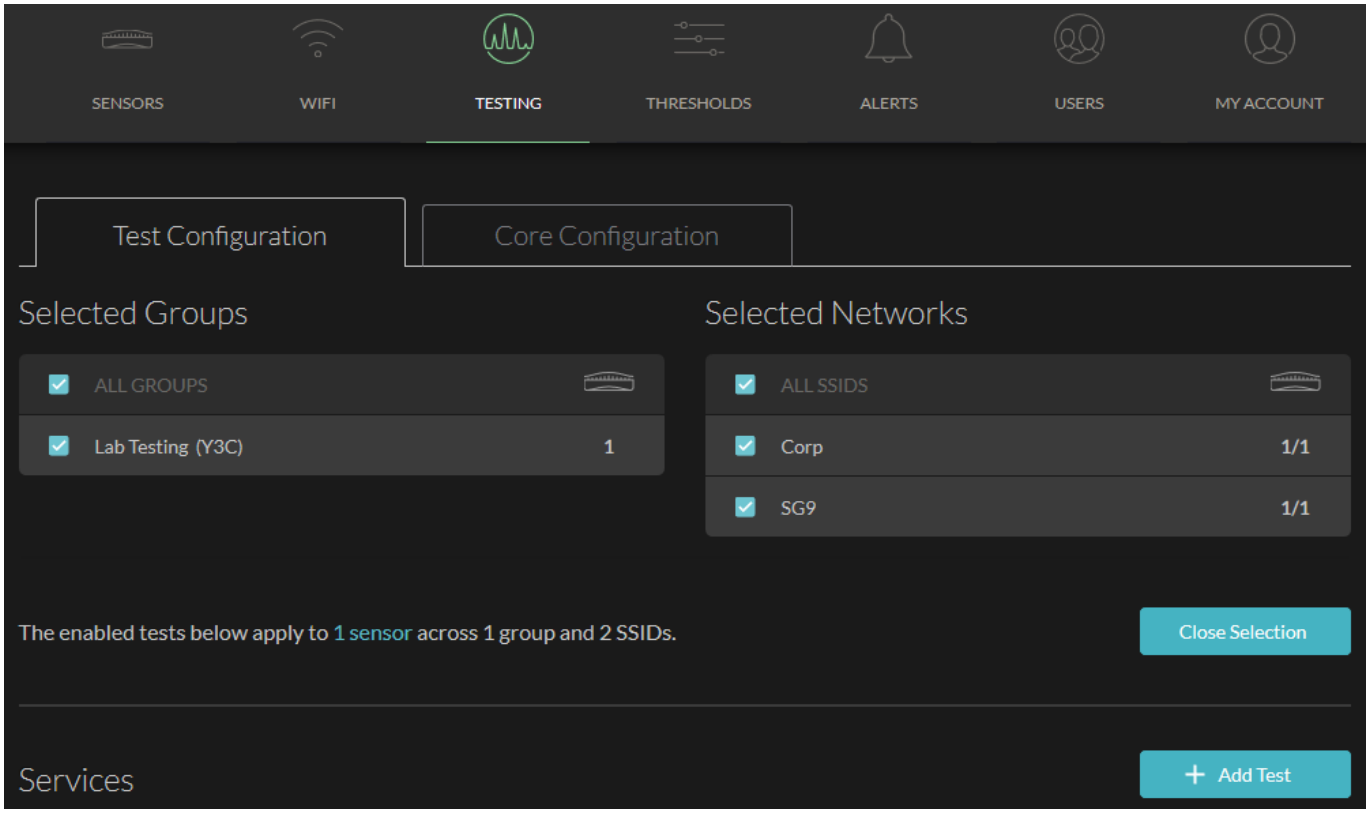
EXTERNAL SERVICES	TARGET	TESTS	TESTING
Dropbox	www.dropbox.com	Port 80, Port 443, Ping, Throughput	ON
Facebook	www.facebook.com	Port 80, Port 443, Ping	ON
Google Docs	docs.google.com	Port 80, Port 443, Ping	ON
Google Mail	www.gmail.com	Port 80, Port 443, Ping	ON
LinkedIn	www.linkedin.com	Port 80, Port 443, Ping	ON
Microsoft Online	login.microsoftonline.com	Port 80, Port 443	ON
Netflix (Fast.com)	www.fast.com	Throughput	ON
Salesforce	www.salesforce.com	Port 80, Port 443, Ping	ON
YouTube	www.youtube.com	Port 80, Port 443, Ping, Video Down...	ON

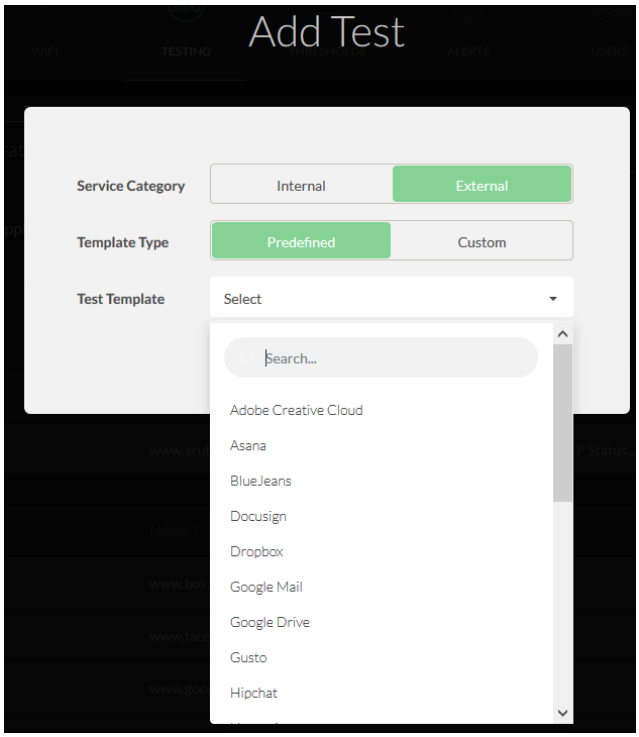
You can edit or disable any of these test, as shown here.



And add other external tests as well. Note that you can select a specific test to run on a specific SSID.



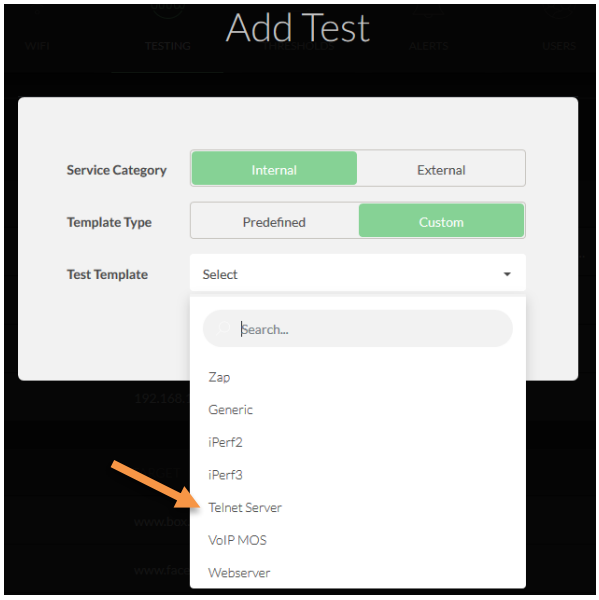


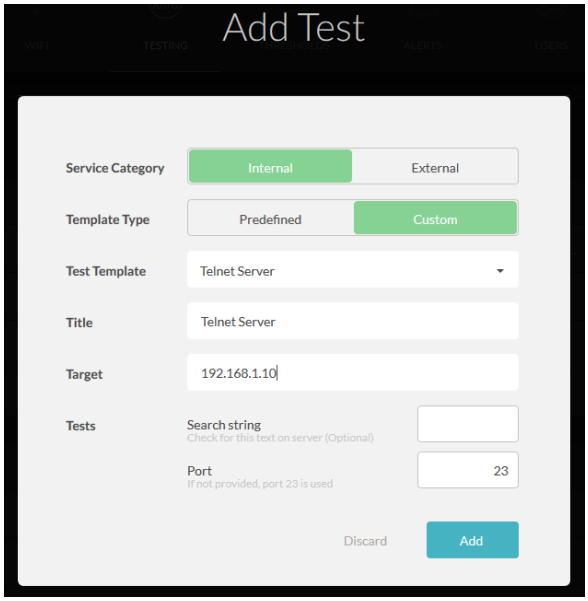


You can also add both custom internal and external tests.

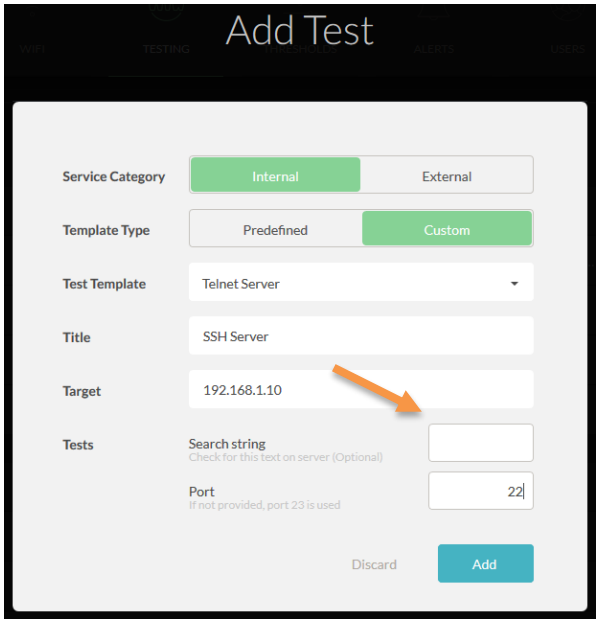
5.1 Internal Custom Tests

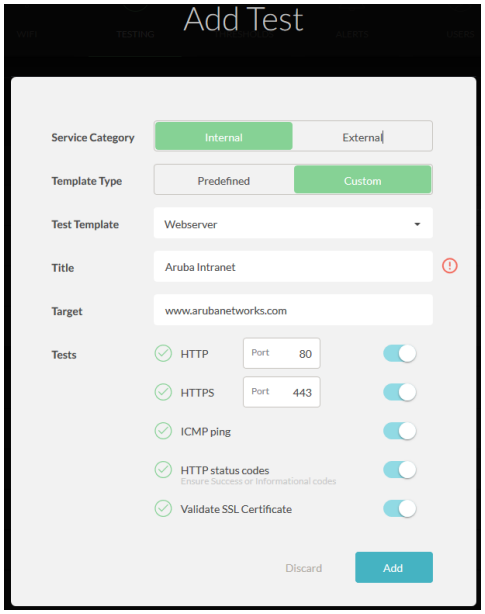
Here we'll add an internal Telnet server, SSH server and a web server. For Telnet test, we'll choose the telnet template. Note that the sensor will not login to the telnet/SSH server rather it will check of the services is available and can respond.

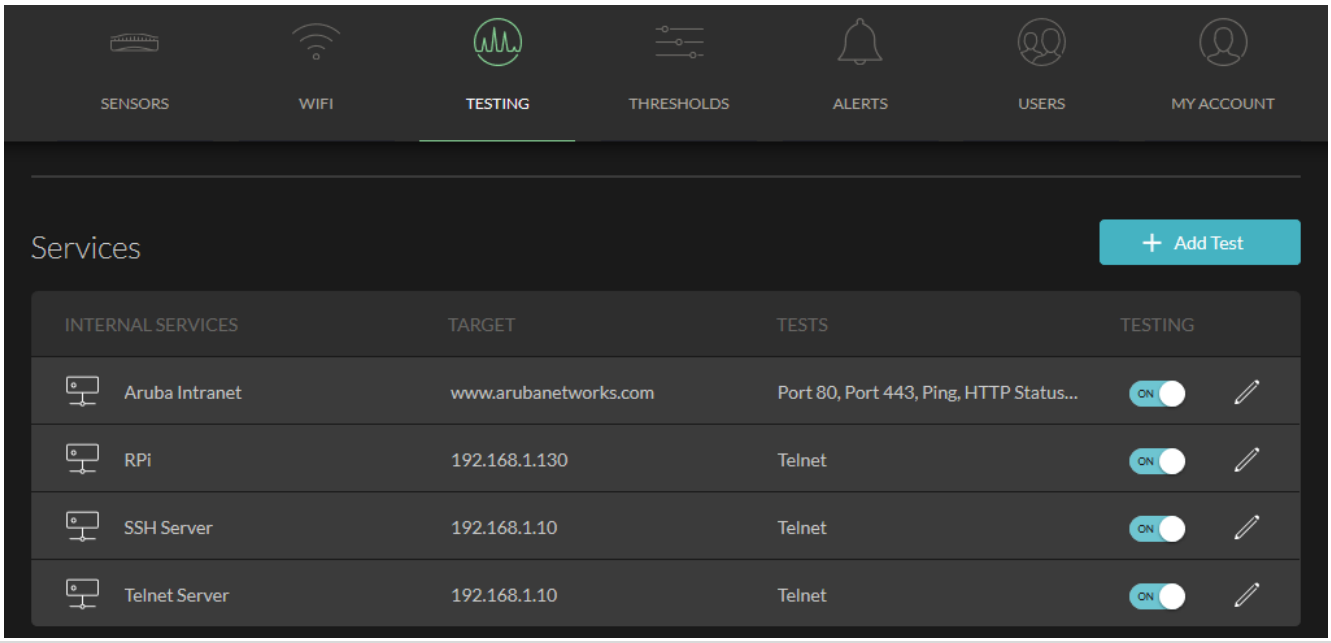




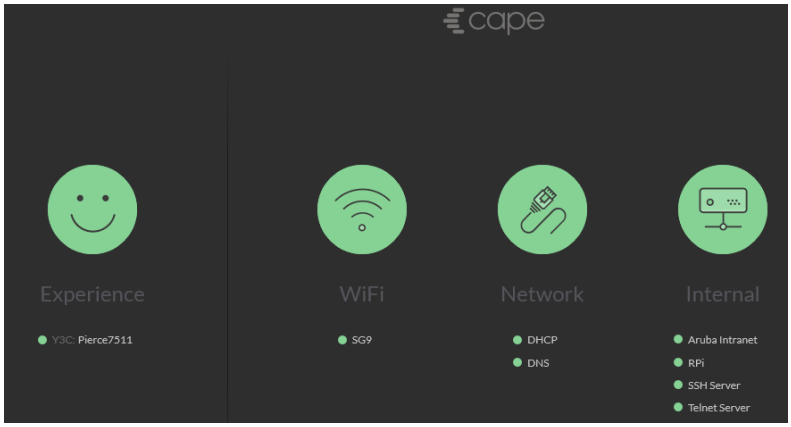
The following are the screen shots of an SSH server and an internal web server.





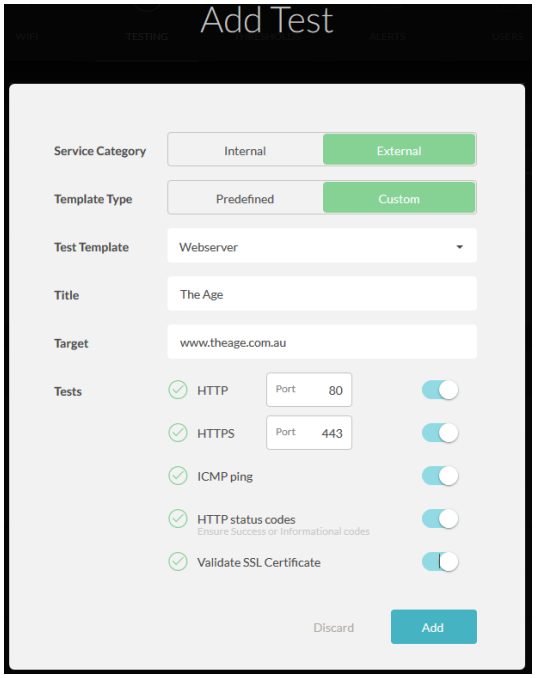


Now you need to wait to see if all new tests will be successful. So once the sensors runs the tests you should get the following results from the dashboard.

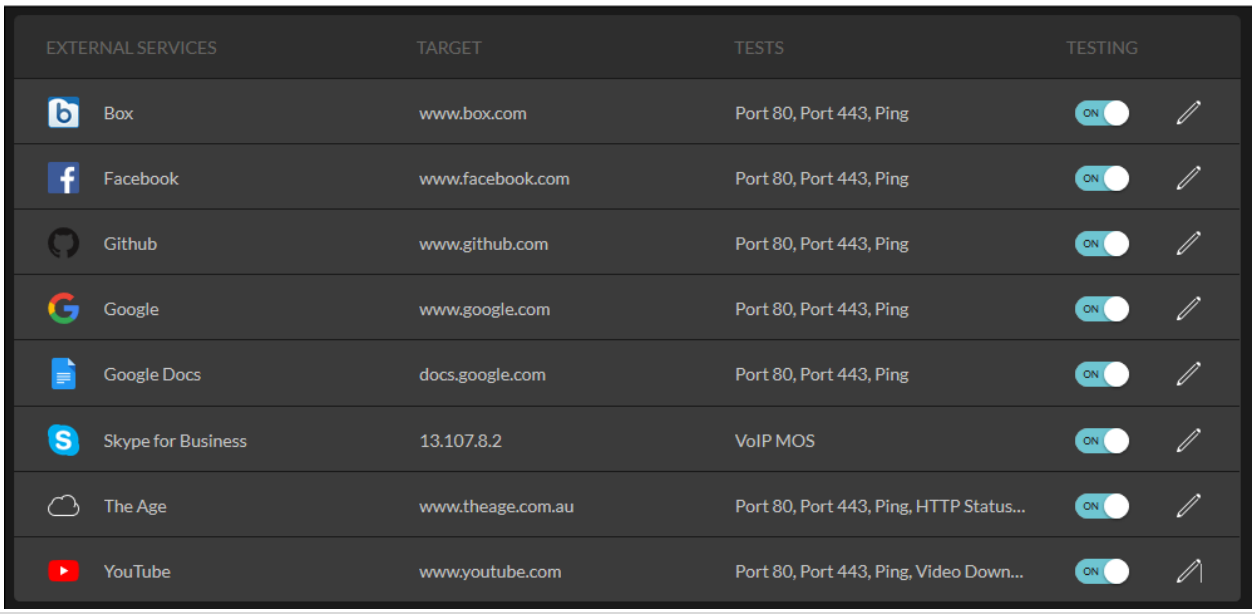


5.2 External Custom Tests

Similarly you can add any external custom test by choosing the relevant templates.



So here are the external tests that we have chosen.



EXTERNAL SERVICES	TARGET	TESTS	TESTING
Box	www.box.com	Port 80, Port 443, Ping	ON
Facebook	www.facebook.com	Port 80, Port 443, Ping	ON
Github	www.github.com	Port 80, Port 443, Ping	ON
Google	www.google.com	Port 80, Port 443, Ping	ON
Google Docs	docs.google.com	Port 80, Port 443, Ping	ON
Skype for Business	13.107.8.2	VoIP MOS	ON
The Age	www.theage.com.au	Port 80, Port 443, Ping, HTTP Status...	ON
YouTube	www.youtube.com	Port 80, Port 443, Ping, Video Down...	ON

Remember only 7-8 of the tests gets displayed on the dashboard at a time. You need to wait for the other tests to cycle through.

5.3 Captive Portal Test Configuration

Captive portal configuration is currently a manual process that is undertaken by Service Assurance engineers.

They generally need to know the following details

- The sensor serial
- SSID
- Any credentials for the portal
- An HTML dump/file of the portal login page(s), i.e. one HTML file per page in the portal journey, saved to disk after page has loaded
- A log of a user authenticating with the portal

You need to contact them support@capenetworks.com

5.4 Internal iPerf Test Configuration

You can use Service Assurance Sensors for load test too. It currently supports bandwidth measurements using iperf3. Here you can read about iperf3 and download your copy. (https://github.com/esnet/iperf)

I have setup an iperf3 on my RPi (192.168.1.130). You can install iperf3 with the following command.

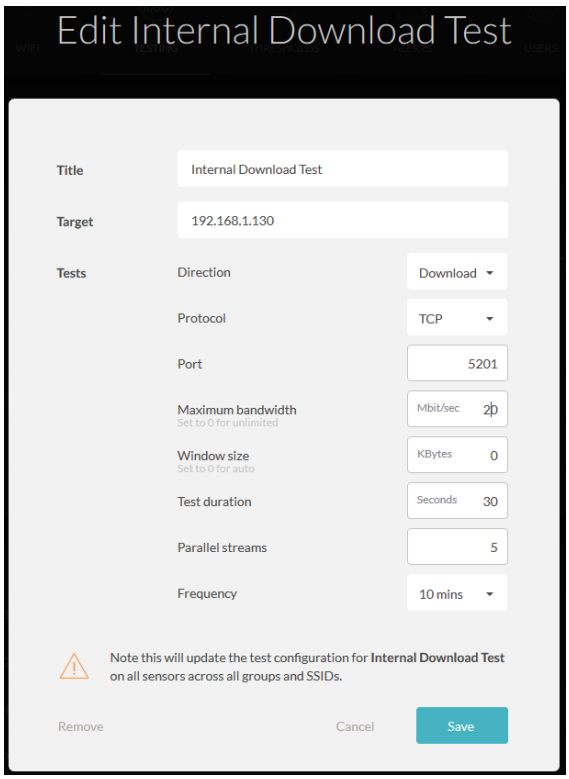
```
pi@raspberrypi:~ $ sudo apt-get install iperf3 -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libiperf0
The following NEW packages will be installed:
  iperf3 libiperf0
0 upgraded, 2 newly installed, 0 to remove and 119 not upgraded.
Need to get 73.0 kB of archives.
After this operation, 183 kB of additional disk space will be used.
Get:1 http://raspbian.melbourneitmirror.net/raspbian stretch/main armhf libiperf0
armhf 3.1.3-1 [54.6 kB]
```

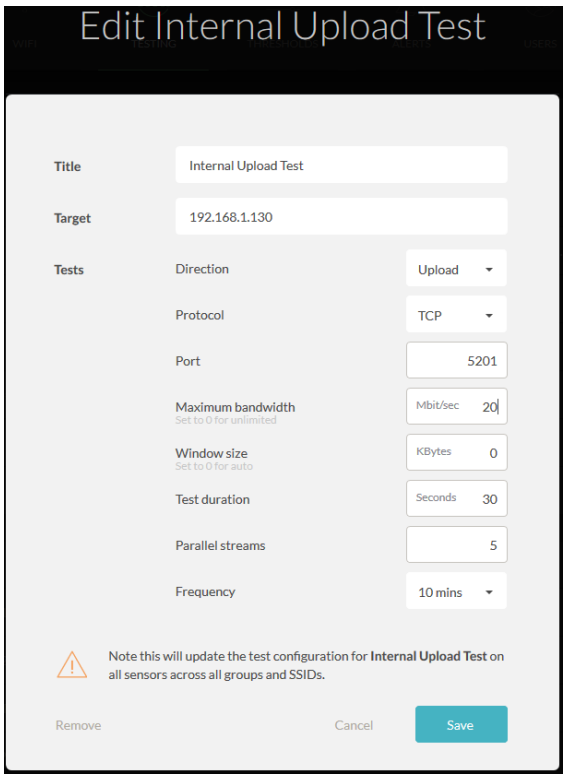
```
Get:2 http://raspbian.melbourneitmirror.net/raspbian stretch/main armhf iperf3 armhf
3.1.3-1 [18.4 kB]
Fetched 73.0 kB in 1s (46.6 kB/s)
Selecting previously unselected package libiperf0:armhf.
(Reading database ... 125298 files and directories currently installed.)
Preparing to unpack .../libiperf0_3.1.3-1_armhf.deb ...
Unpacking libiperf0:armhf (3.1.3-1) ...
Selecting previously unselected package iperf3.
Preparing to unpack .../iperf3_3.1.3-1_armhf.deb ...
Unpacking iperf3 (3.1.3-1) ...
Processing triggers for libc-bin (2.24-11+deb9u1) ...
Setting up libiperf0:armhf (3.1.3-1) ...
Processing triggers for man-db (2.7.6.1-2) ...
Setting up iperf3 (3.1.3-1) ...
Processing triggers for libc-bin (2.24-11+deb9u1) ...
pi@raspberrypi:~ $
```

Now that it is installed and we need to run it.

```
pi@raspberrypi:~ $ /usr/bin/iperf3 -s
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
pi@raspberrypi:~ $
```

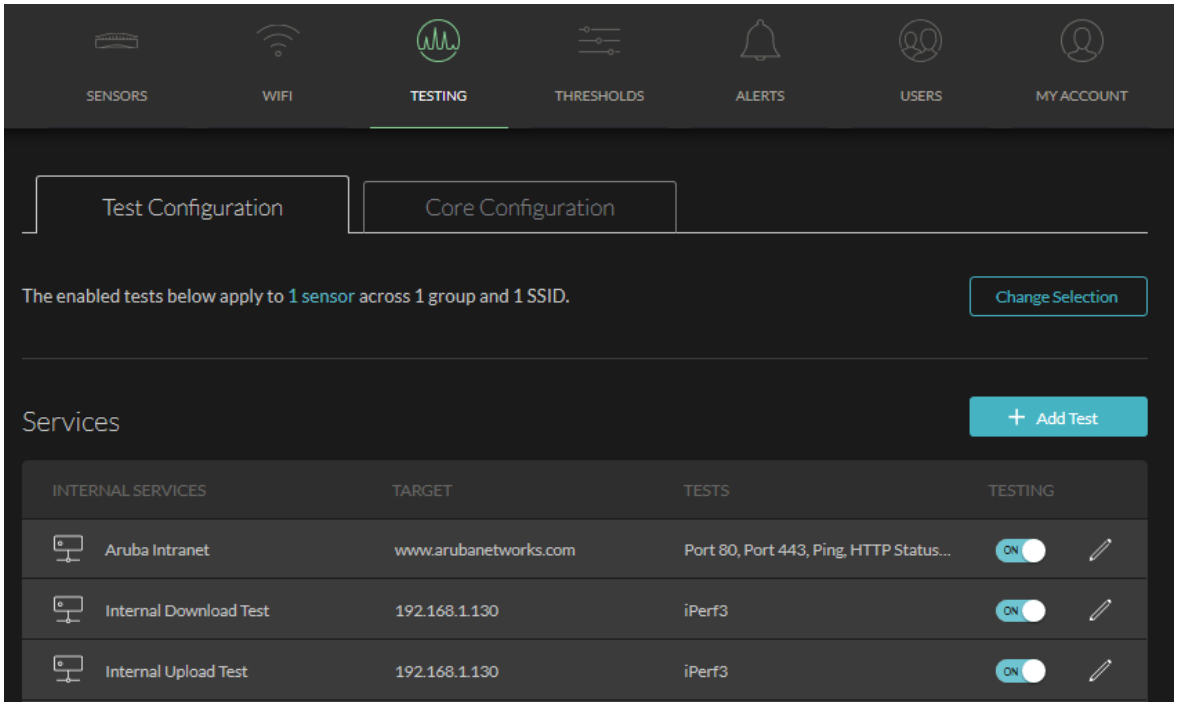
You need to configure an iPerf test from Service Assurance dashboard, make sure it matches the port that the iPerf server is listening on. (5201)



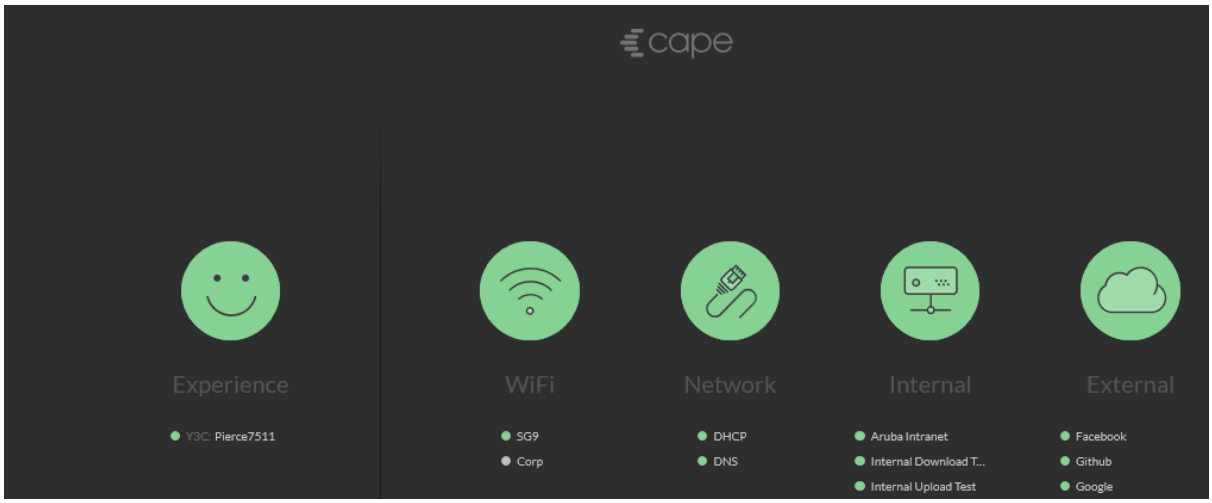


Window size is to set the socket buffer size (for TCP this is the TCP window size)

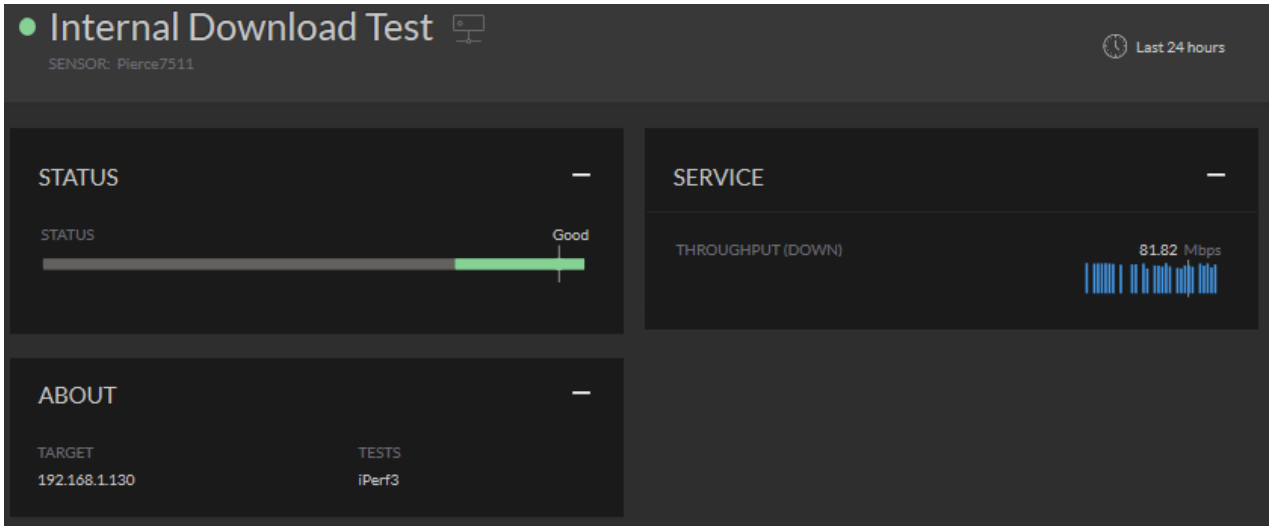
Here are our internal tests that we have configure.

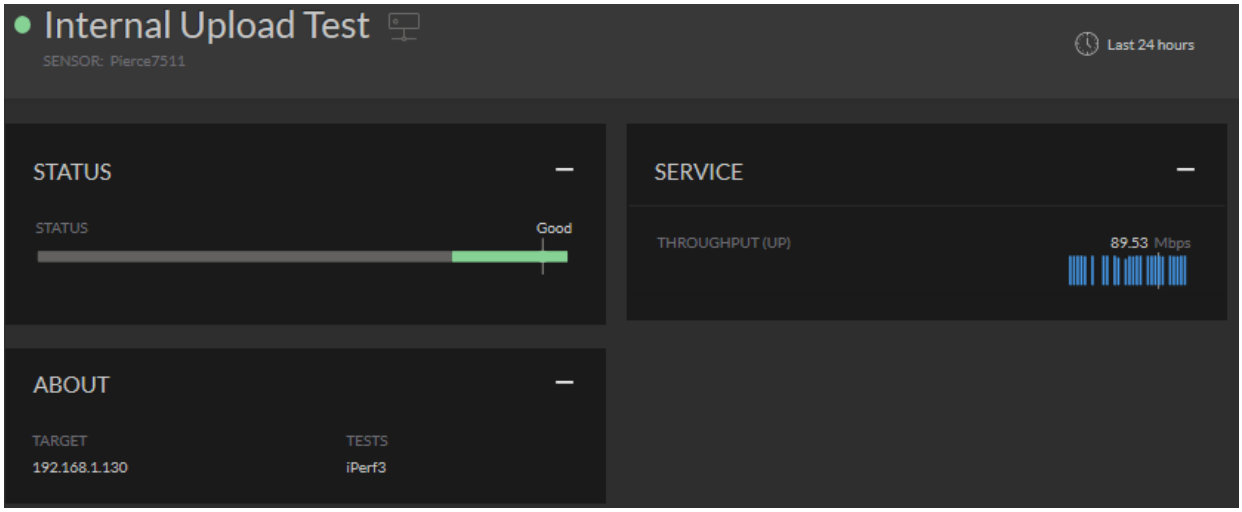


Now we need to wait for the Service Assurance Sensor to run these test.



As you can see above they have run successfully

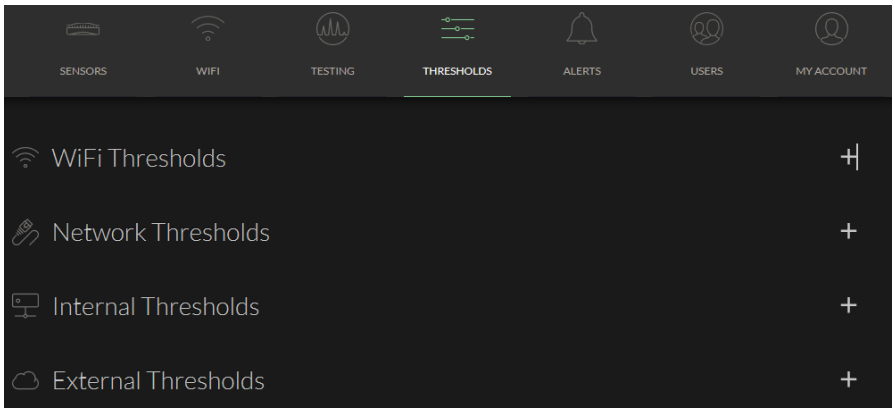




Note that iperf3 is single threaded and as such only allows one client to connect at a time. This means that if you have multiple sensors all testing against the same iperf3 server with high frequency that you may get some incomplete test results.

5.5 Threshold Configuration

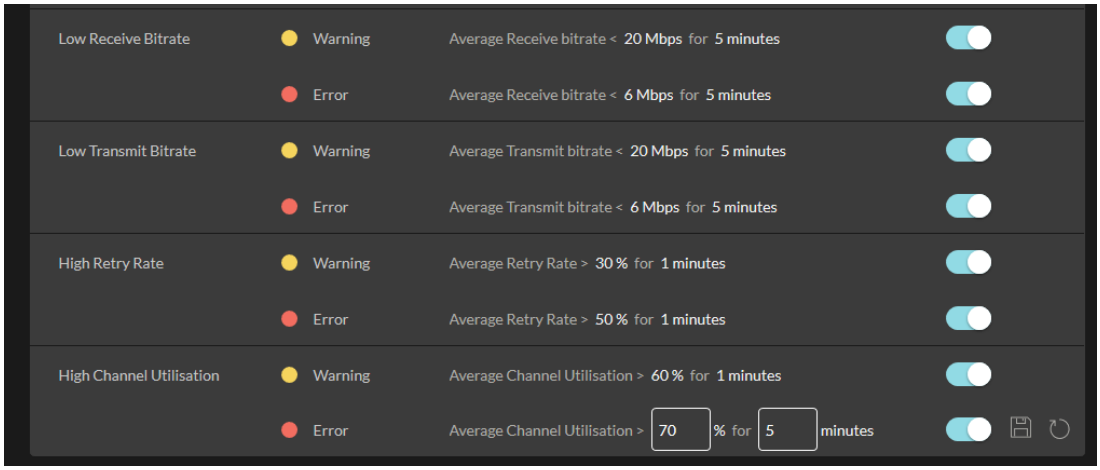
You can set various threshold for the WiFi, Network Internal and external tests as shown below



These threshold dictates if you get a smiley face or not. The WiFi threshold can be set for the following and also note that not all of them are enabled by default.

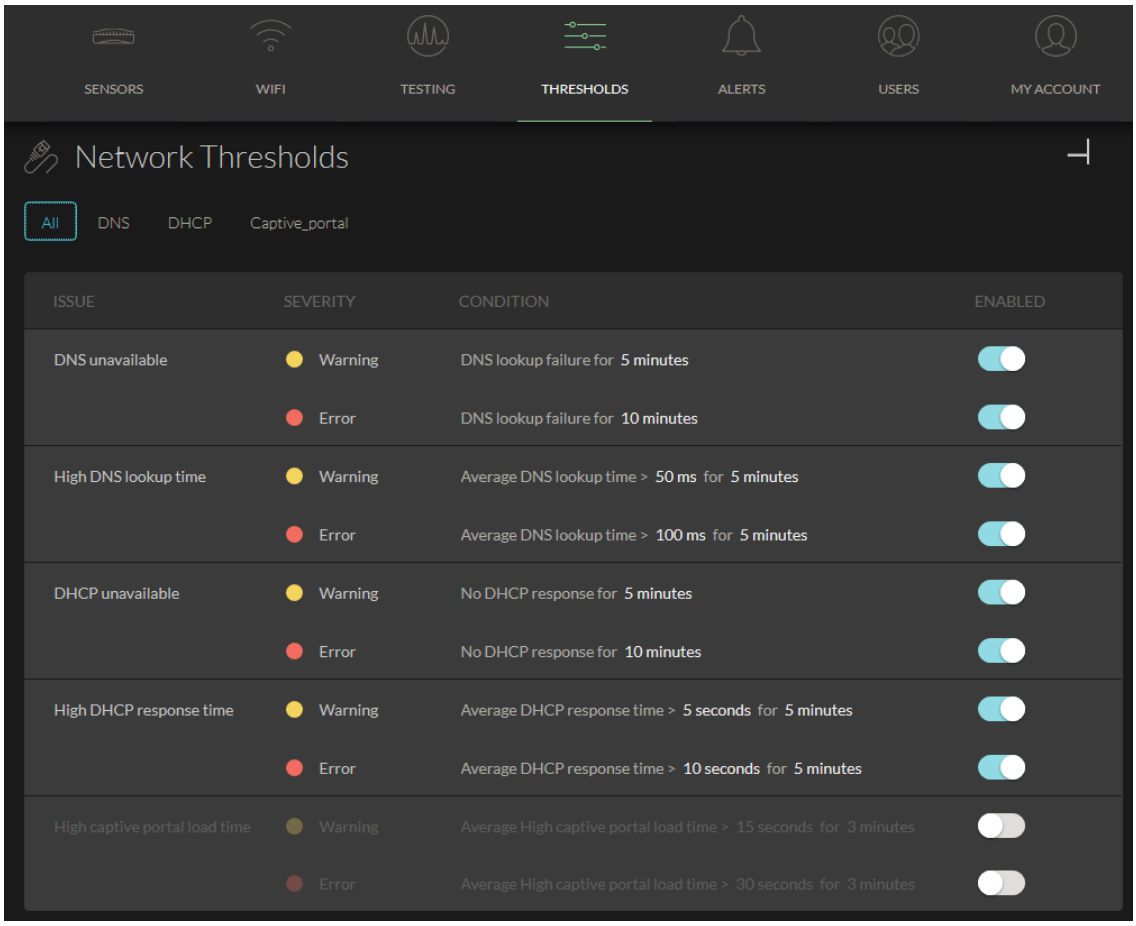
- Availability
- Bitrate
- RSSI
- Retry Rates
- Channel Utilisation

Here is sample threshold for Channel utilisation



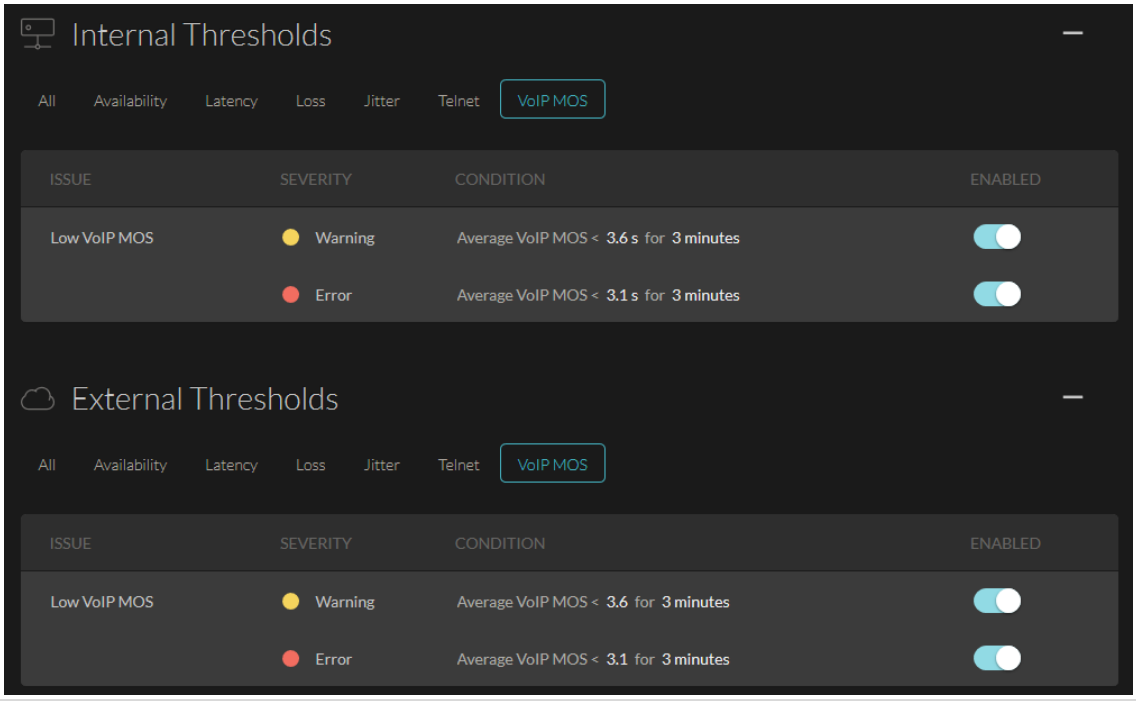
The network threshold are for

- DNS availability and lookup time
- DHCP availability and lookup time
- Captive Portal availability and lookup time



For both internal and external test the threshold that you can set are for

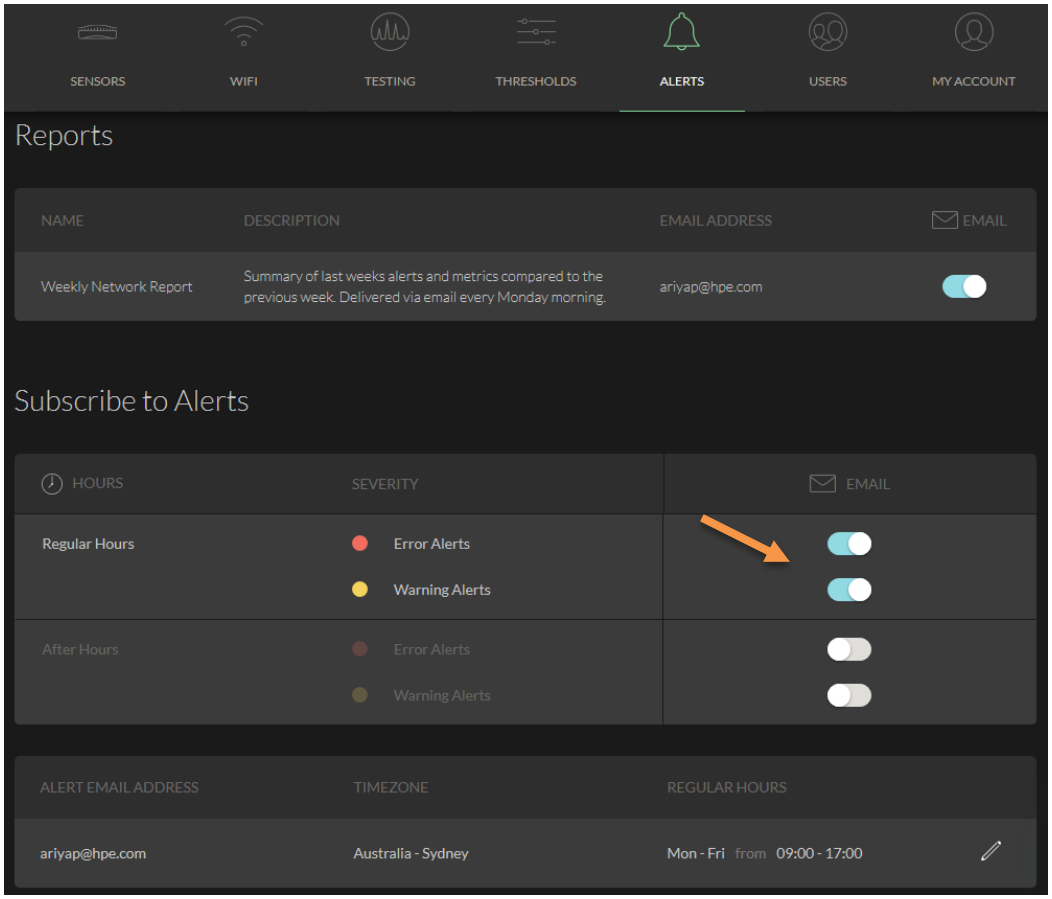
- Availability
- Latency
- Packet Loss
- Jitter
- Telnet
- VoIP MOS



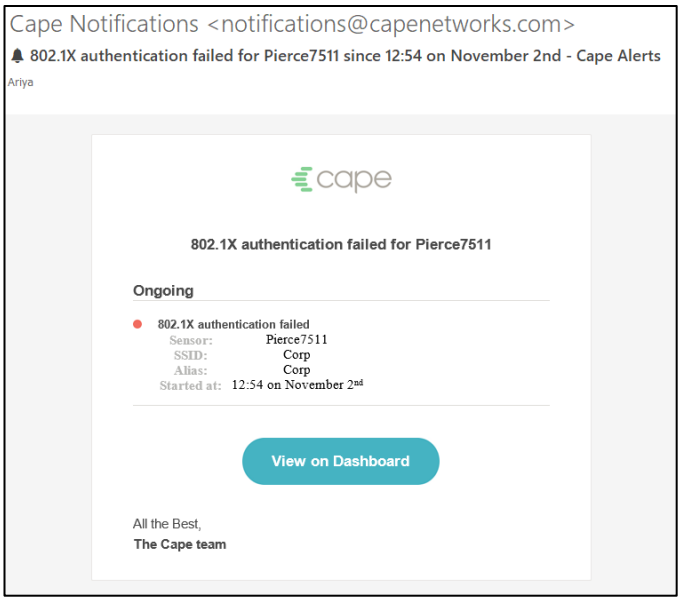
So based on the environment you may want to modify these thresholds.

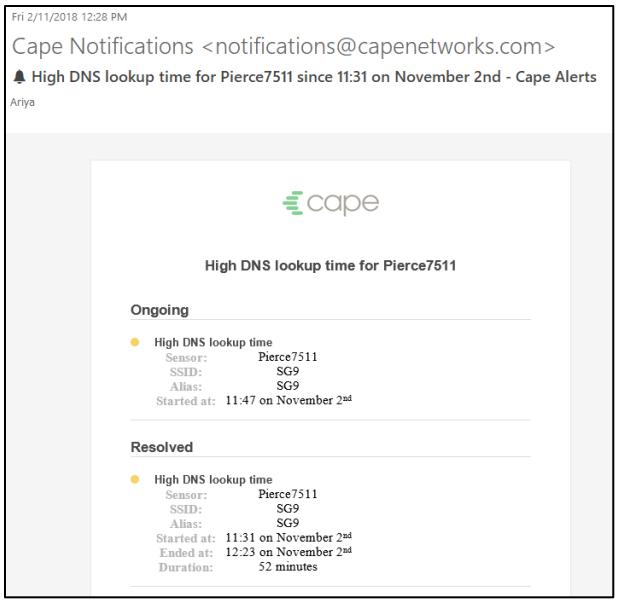
5.6 Alerts and Reporting

With alerts you have a choice of getting these alerts not only to be displayed on the dashboard but also to be emailed during normal hours and after hours.



Here is the sample alert email for a dot1x failure and DNS lookup time.



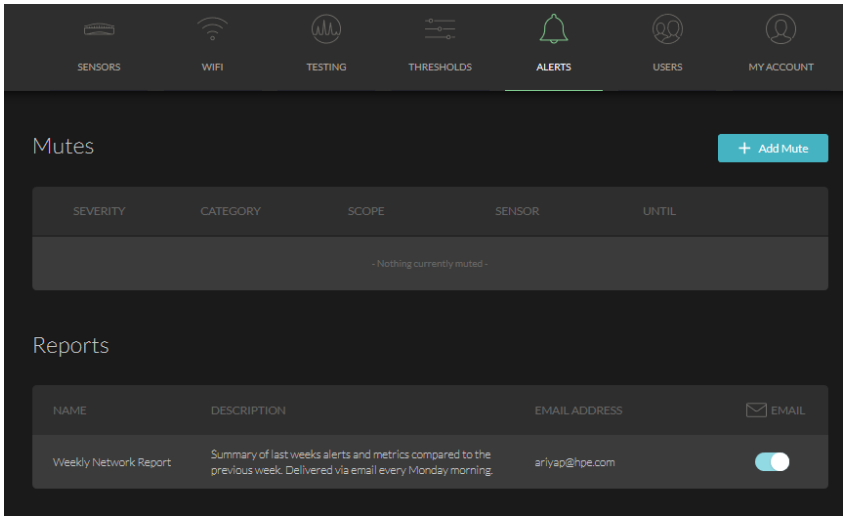


Service Assurance Dashboard provides an automated weekly report from the Service Assurance Sensors and Dashboard. This reports gets emailed to you. The weekly report has the following:

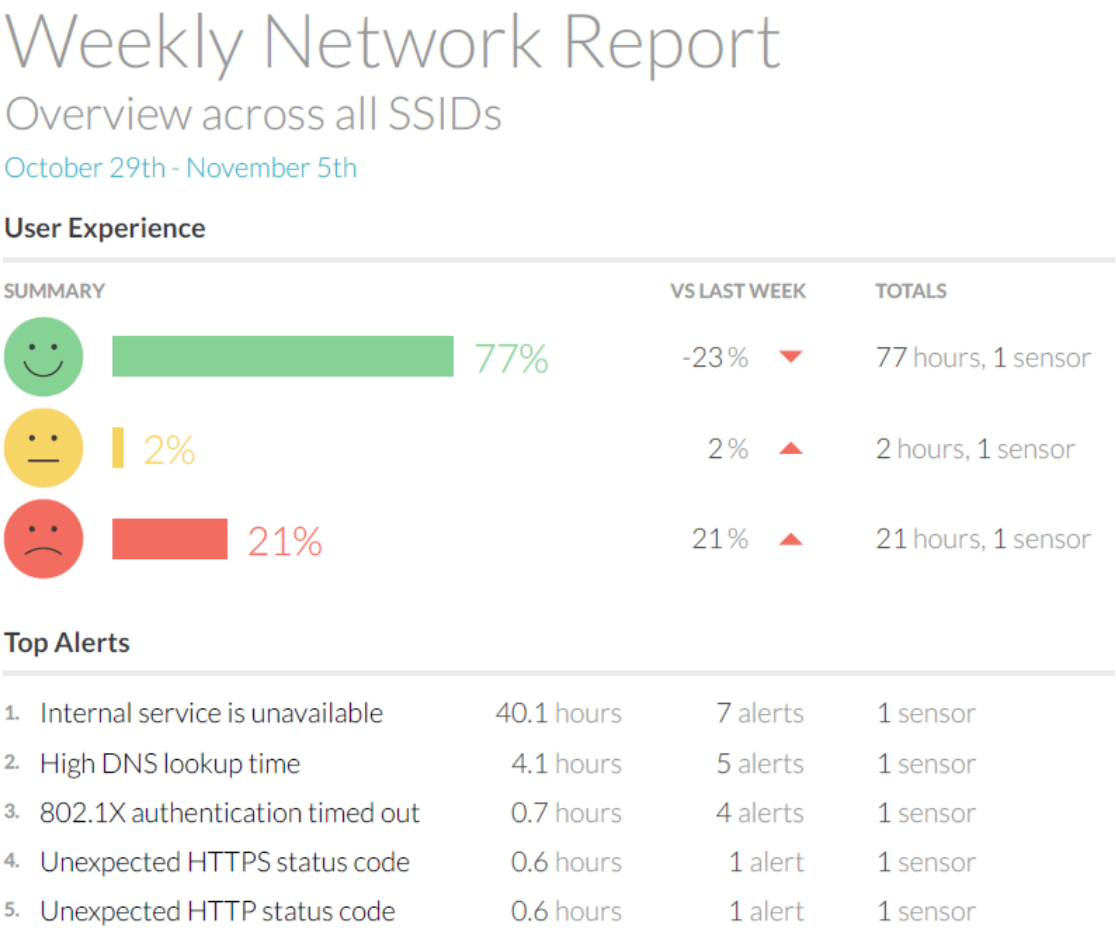
- A traffic light of how well your network is running

- Lists the number of alerts during that period
- Graphically showing the alerts per day
- Lists the worse performing sensor
- Metric on the tests that were run.

This is how to enable the weekly reports



And here is the exact from a weekly report which gets emailed to you in PDF format.



Weekly Network Report

Overview across all SSIDs

October 29th - November 5th

User Experience

SUMMARY		VS LAST WEEK	TOTALS
	77%	-23% ▼	77 hours, 1 sensor
	2%	2% ▲	2 hours, 1 sensor
	21%	21% ▲	21 hours, 1 sensor

Top Alerts

1. Internal service is unavailable	40.1 hours	7 alerts	1 sensor
2. High DNS lookup time	4.1 hours	5 alerts	1 sensor
3. 802.1X authentication timed out	0.7 hours	4 alerts	1 sensor
4. Unexpected HTTPS status code	0.6 hours	1 alert	1 sensor
5. Unexpected HTTP status code	0.6 hours	1 alert	1 sensor

6 School Online Tests

There are many schools and higher education that are moving toward online tests and examinations.

In Australia, National Assessment Program Literacy and Numeracy (NAPLAN) which is a the three-yearly sample assessments in science literacy, civics and citizenship, and information and communication technology (ICT) literacy, is run by Australian Curriculum, Assessment and Reporting Authority (ACARA). NAPLAN test which is for Years 3, 5, 7and 9 is moving online and the schools need to be sure that their infrastructure can handle the volume and latency needed for online examinations.

Service Assurance Sensors can be used to automatically test a school's infrastructure to see if they are ready for NAPLAN. The sensor can check connectivity to an SSID, association time, time it takes for DHCP, DNS and Authentication. Then it can go on to test Captive portal and other gateways and finally can check for web pages loads, throughput, etc. and reports all these through Service Assurance dashboard.

In addition we have enabled the following three specific tests for NAPLAN.

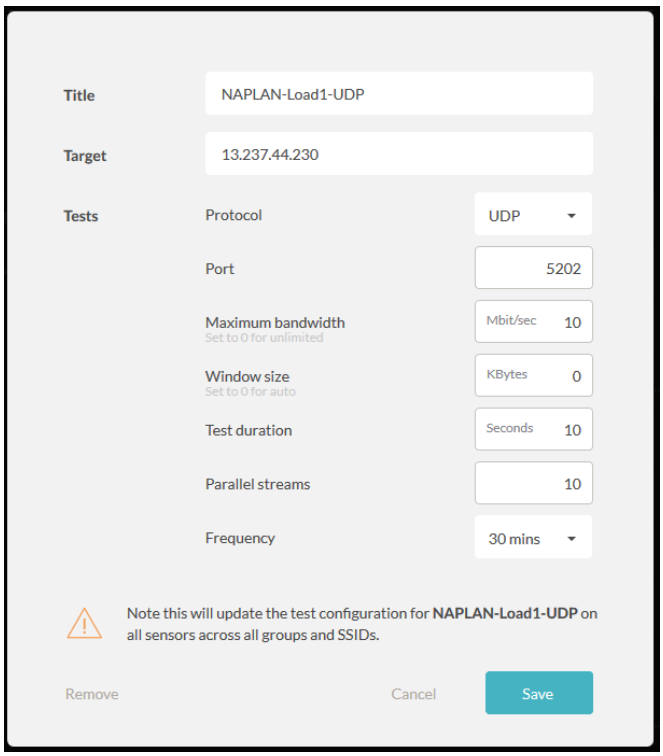
6.1 NAPLAN Load Test

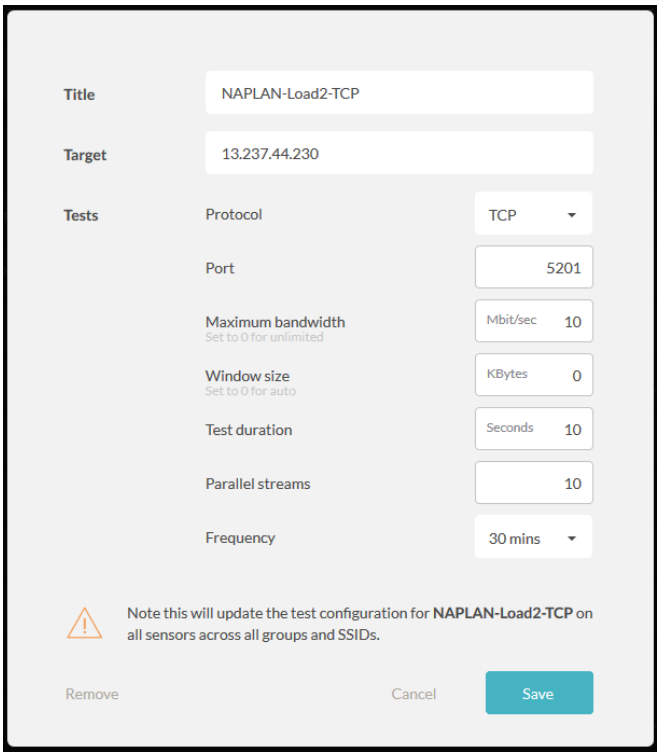
The basis of the load tests provided by Service Assurance Sensors is iPerf. Service Assurance Sensors support both iperf2 and iperf3. iPerf3 is a single thread application while iPerf2 is multi thread application.

You can run NAPLAN load test using either iperf2 or 3. Since iPerf2 is multi-threaded it is more useful for the load testing. Here are the details of iPerf2 tests.

- 13.237.44.230 port 5201 - NAPLAN TCP Load Test
- 13.237.44.230 port 5202 - NAPLAN UDP Load Test

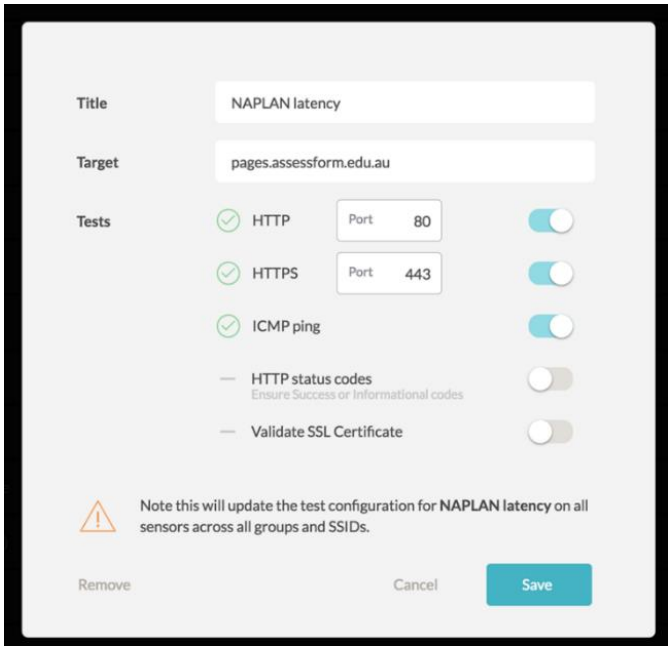
As shown before we'll create a Load test with iperf2 template but this time it will be an external test.

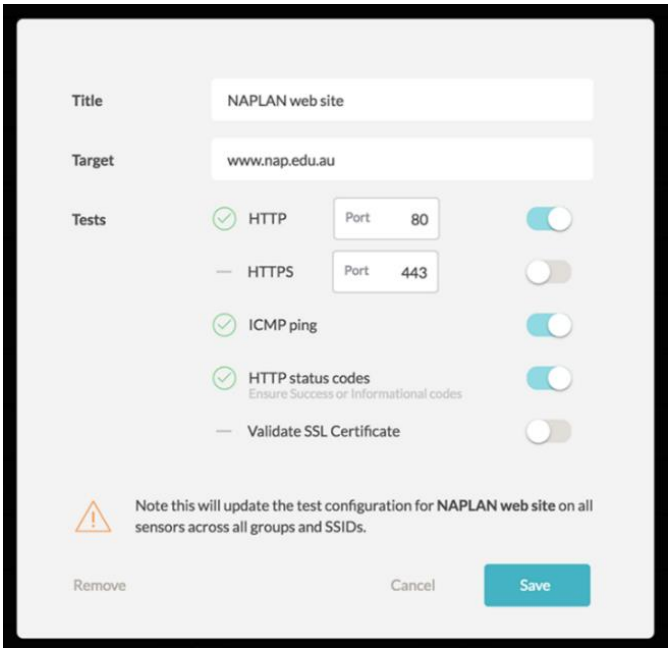




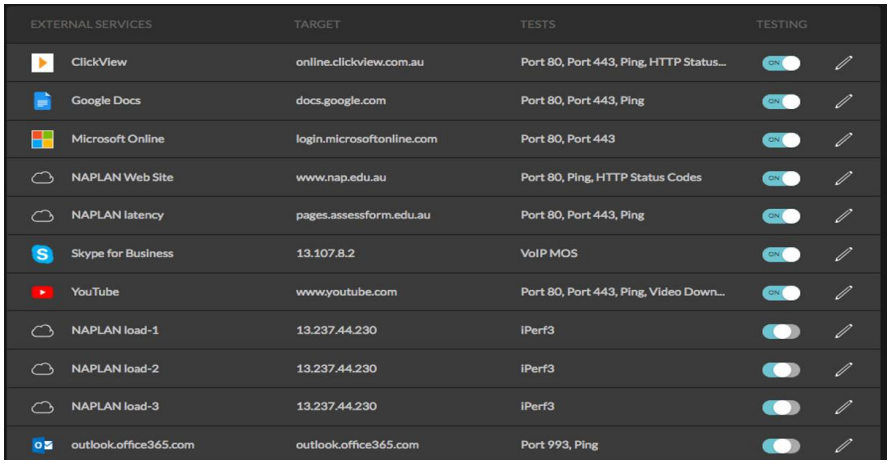
6.2 NAPLAN Latency and Accessibility Test

Here we are adding a tests to be able to time stamp the latency of a particular application access.





And finally here is the rest of the tests that are useful for most of the schools, it includes ClickView, office365, Google docs to mention a few.



EXTERNAL SERVICES	TARGET	TESTS	TESTING
ClickView	online.clickview.com.au	Port 80, Port 443, Ping, HTTP Status...	ON
Google Docs	docs.google.com	Port 80, Port 443, Ping	ON
Microsoft Online	login.microsoftonline.com	Port 80, Port 443	ON
NAPLAN Web Site	www.nap.edu.au	Port 80, Ping, HTTP Status Codes	ON
NAPLAN latency	pages.assessform.edu.au	Port 80, Port 443, Ping	ON
Skype for Business	13.107.8.2	VoIP MOS	ON
YouTube	www.youtube.com	Port 80, Port 443, Ping, Video Down...	ON
NAPLAN load-1	13.237.44.230	iPerf3	
NAPLAN load-2	13.237.44.230	iPerf3	
NAPLAN load-3	13.237.44.230	iPerf3	
outlook.office365.com	outlook.office365.com	Port 993, Ping	

7 Service Assurance Dashboard

7.1 Main Dashboard

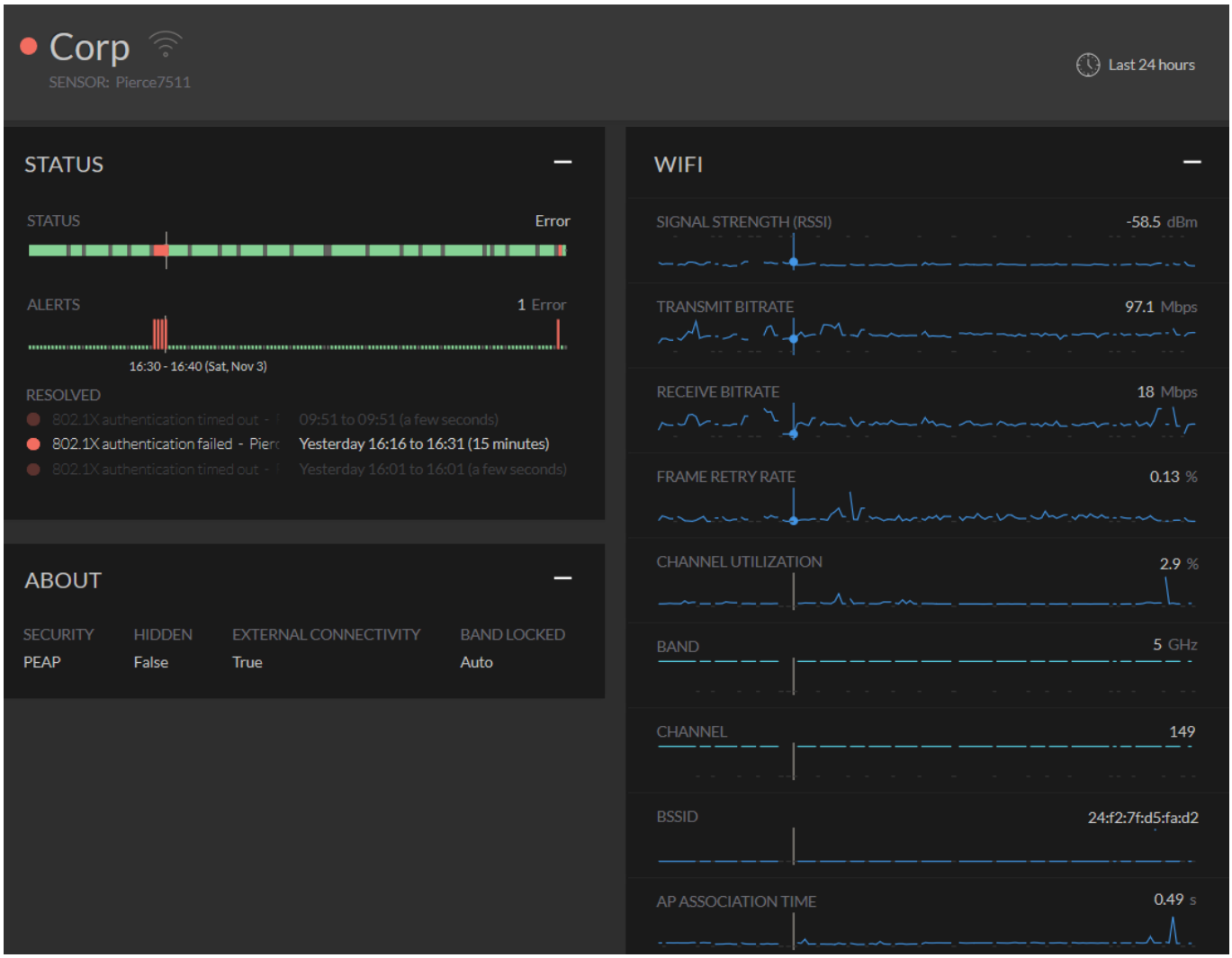
Here is the main dashboard that you can view all your sensors as well as various networks and test that have been configured. The traffic lights indicates that everything is in order and running fine.

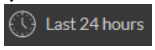
You can hover your mouse over any item and you that gives you a 24 hours view of it.

First you can hover your mouse over the sensor in the overall Experience section

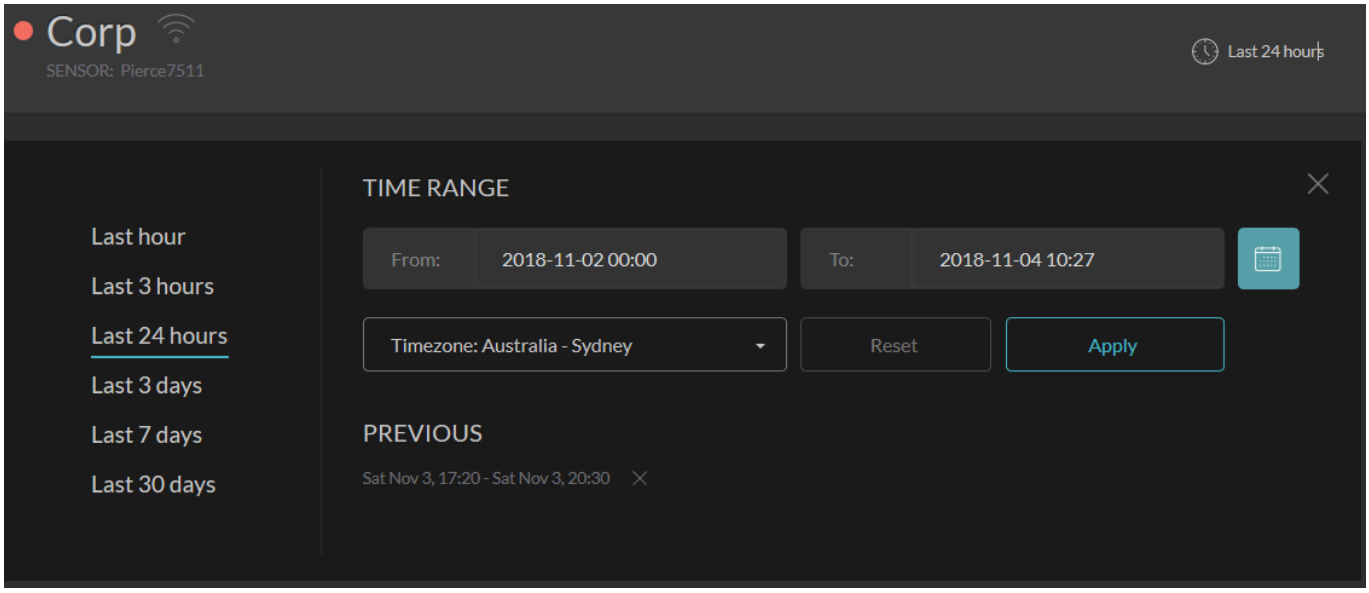
We notice that there are some red lines under the status of 2 SSIDs. You can then hover your mouse over the 2x SSIDs to see if there are more information.

We see that on the Corp SSID there are some red lines. Now we click on the Corp SSID to get even more information. We see some authentication failure and timeout along with relevant wireless stats on the right hand side.

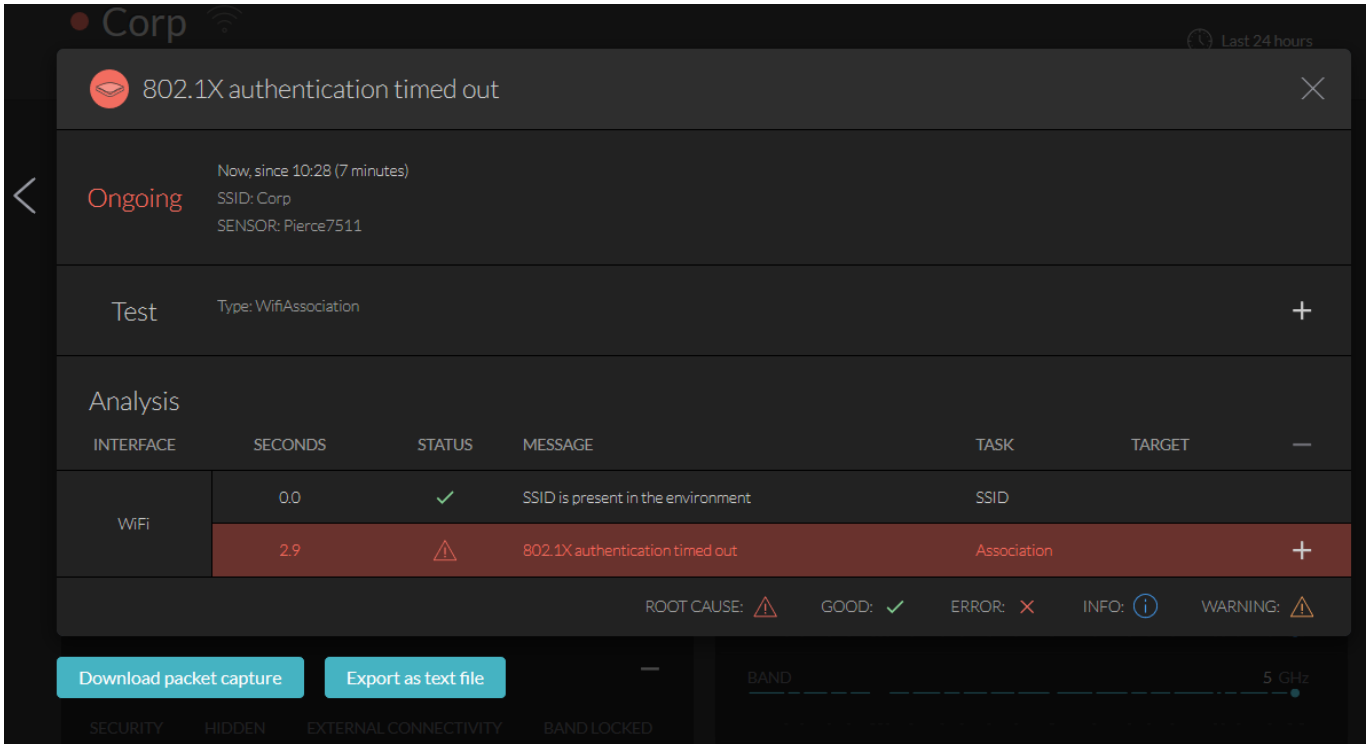


Now as you hover over the one of the red lines that indicate an error, you'll see the corresponding point in time in other graphs. You can change the time filter as well by clicking on the 

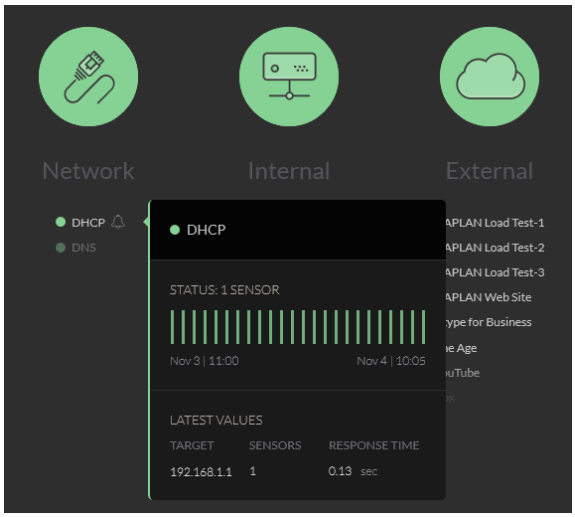
on the top right corner of the dashboard.



Now if we click on the one of the errors we get the following where we can download a pcap and/or export the text file.

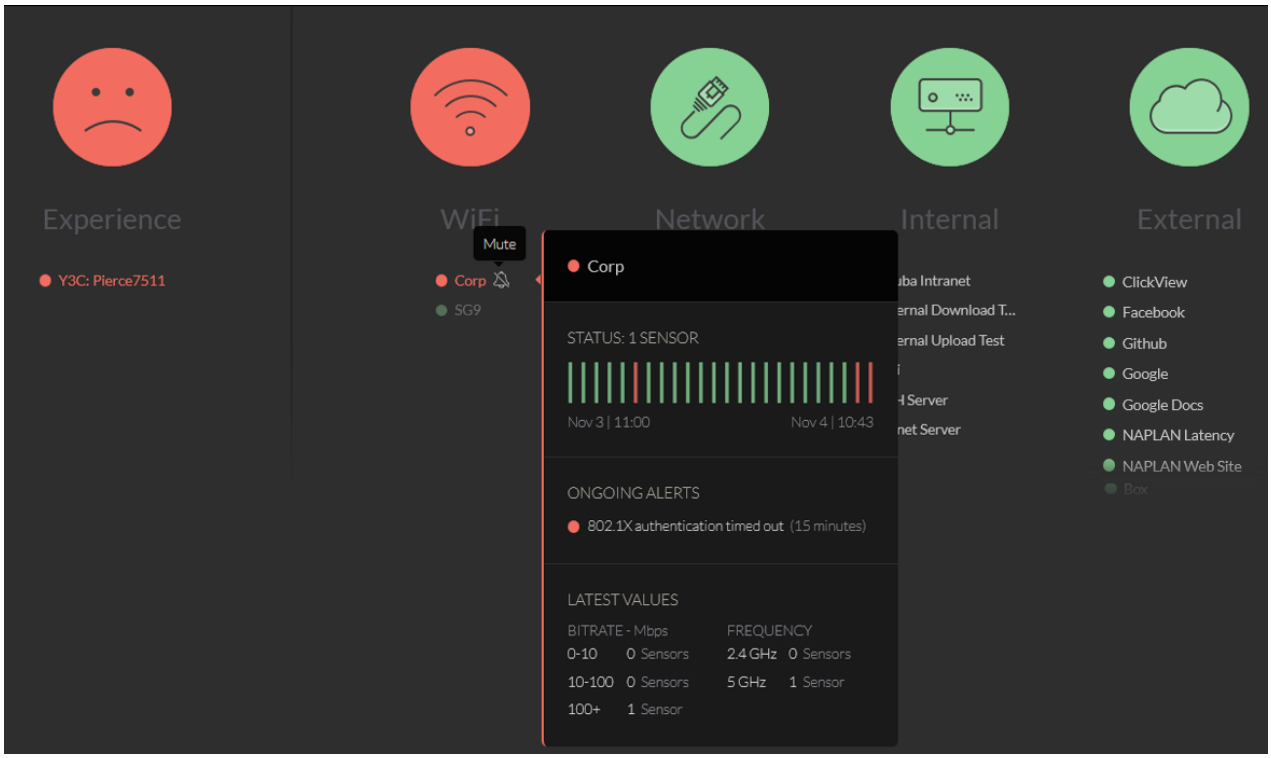


Now going back to the main dashboard and we'll hovering over DHCP and one of the external tests



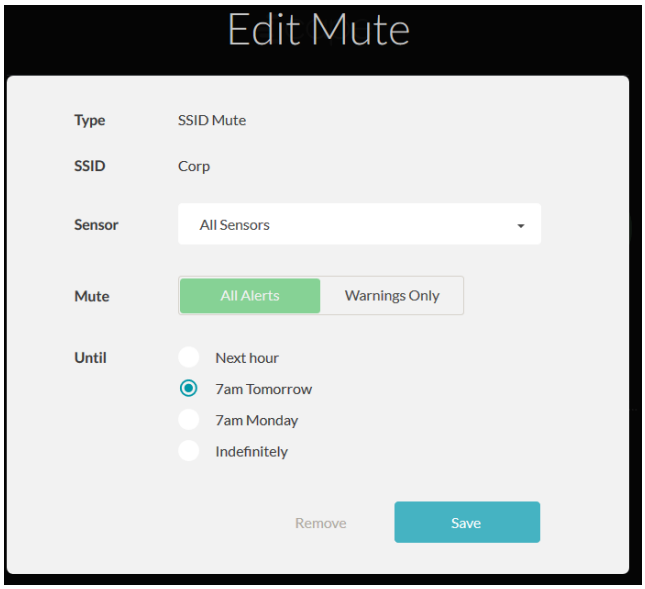
Now if there is an ongoing issue the dashboard could look like this.

Now if we are aware of the problem say in this case with the Corp dot1x SSID we can mute this error so we don't get alerts and get the traffic light back to green.



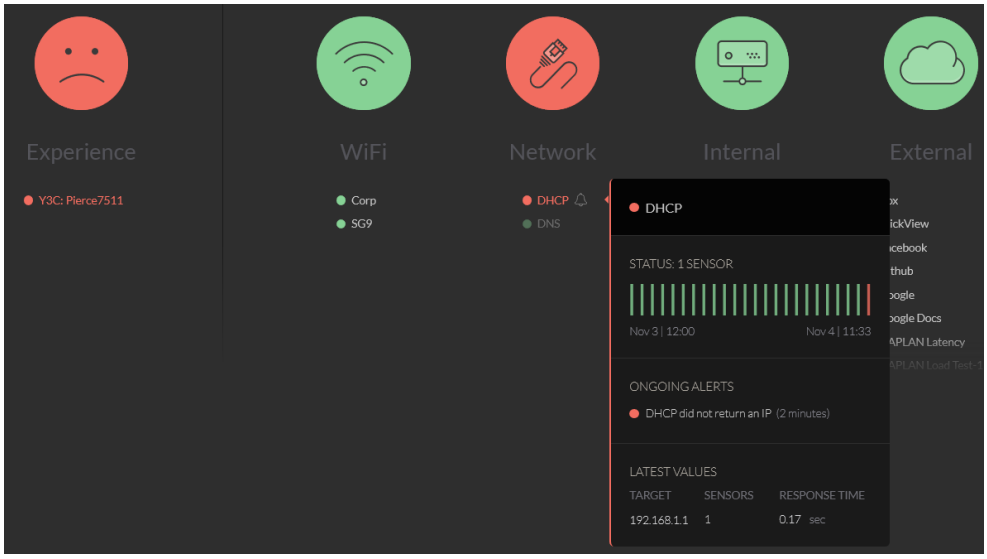
So now if you hover over the "Corp" and click on the bell icon, you get the following with the message at the top saying "Corp has been muted until 07:00 tomorrow across all sensors click to edit"

You can further edit the mute option by again clicking on the bell icon

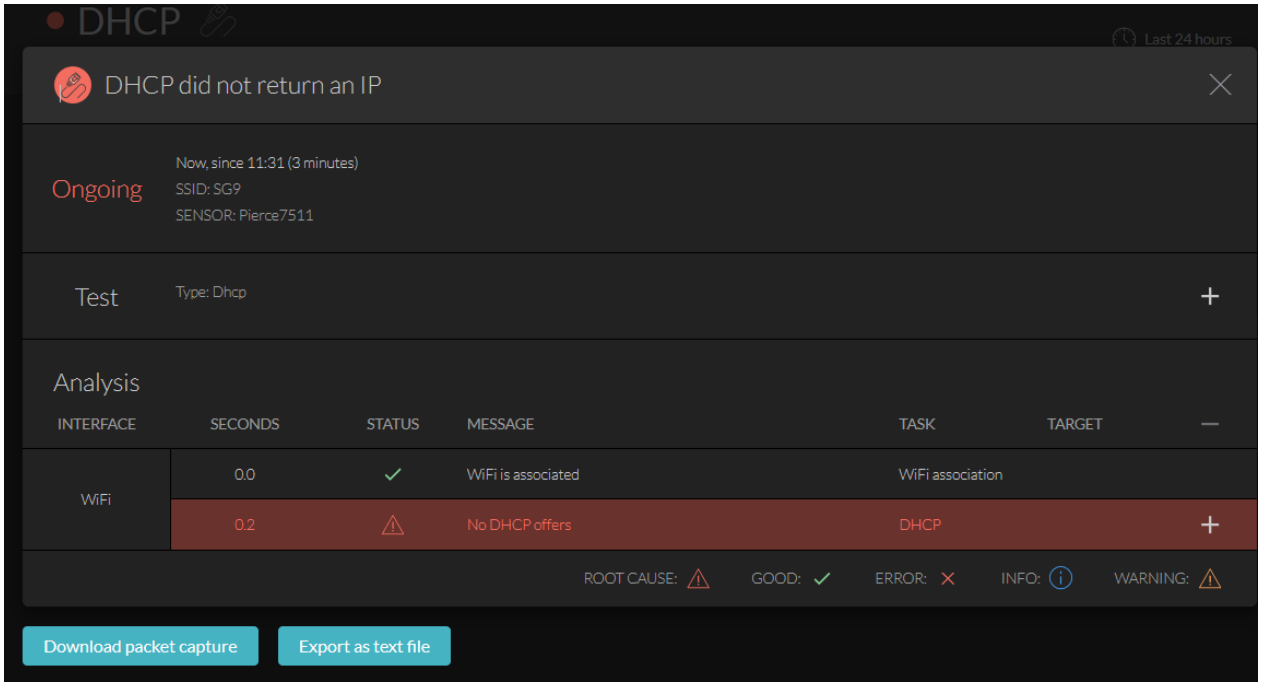


7.2 DHCP timing metrics and Gateway Visibility

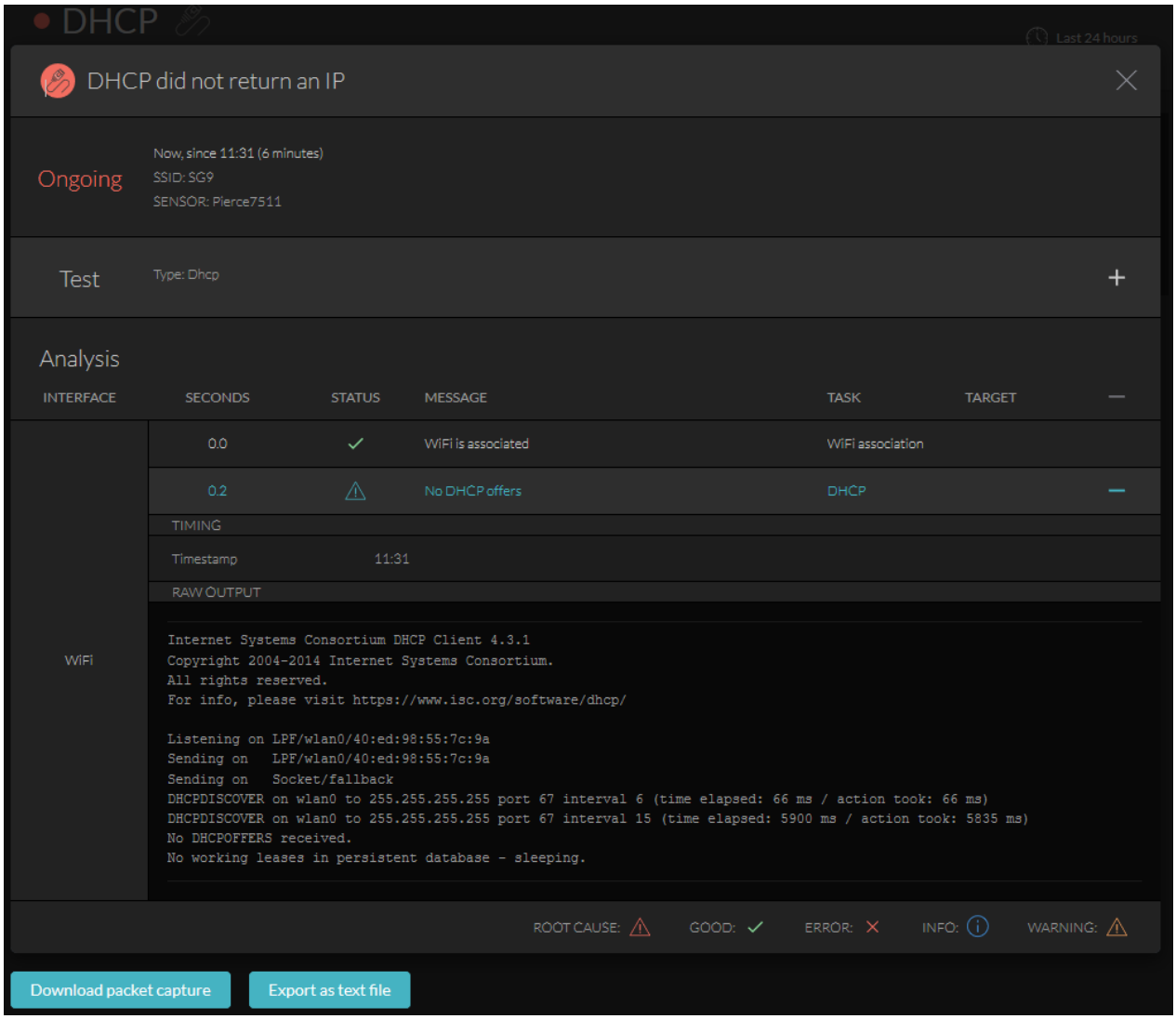
You are able to peek into the DHCP (discover, offer, request, acknowledge) exchanges, whenever there is an issue, to view the breakdown of the transaction times and understand which part of the process is causing the delay or failure.



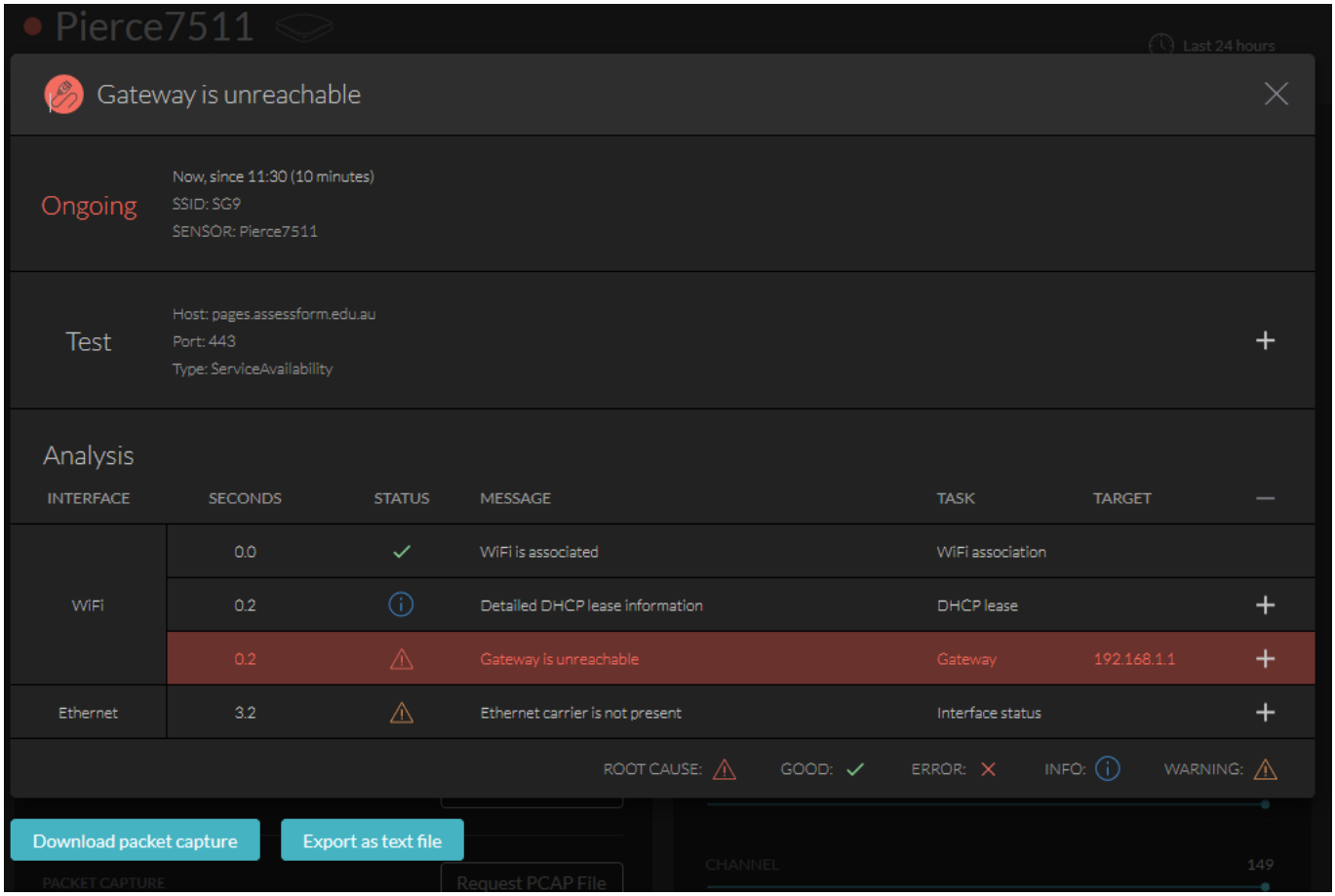
You then click on the DHCP and get the following.



You can now click on the “+” sign for get more info

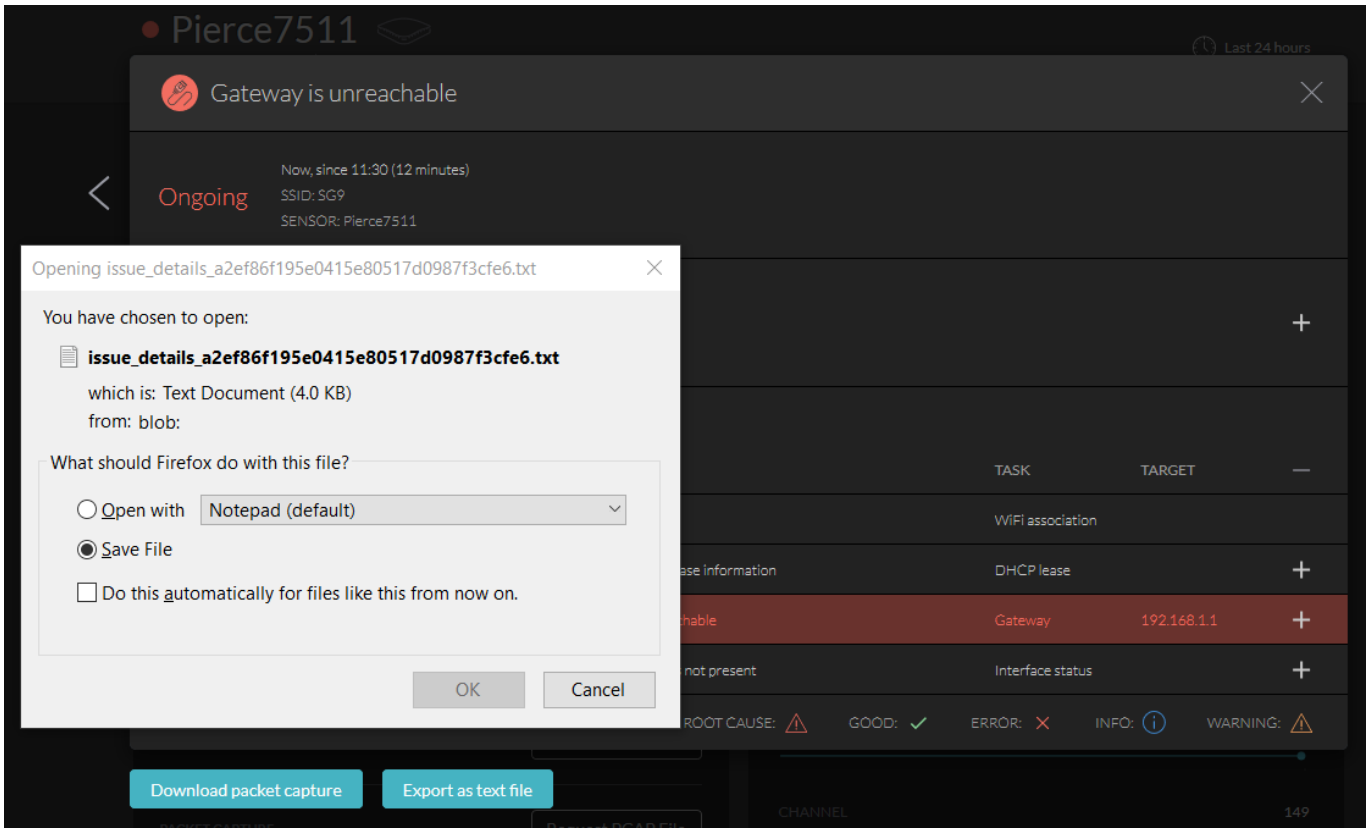


The following is the case where the default gateway is not reachable.



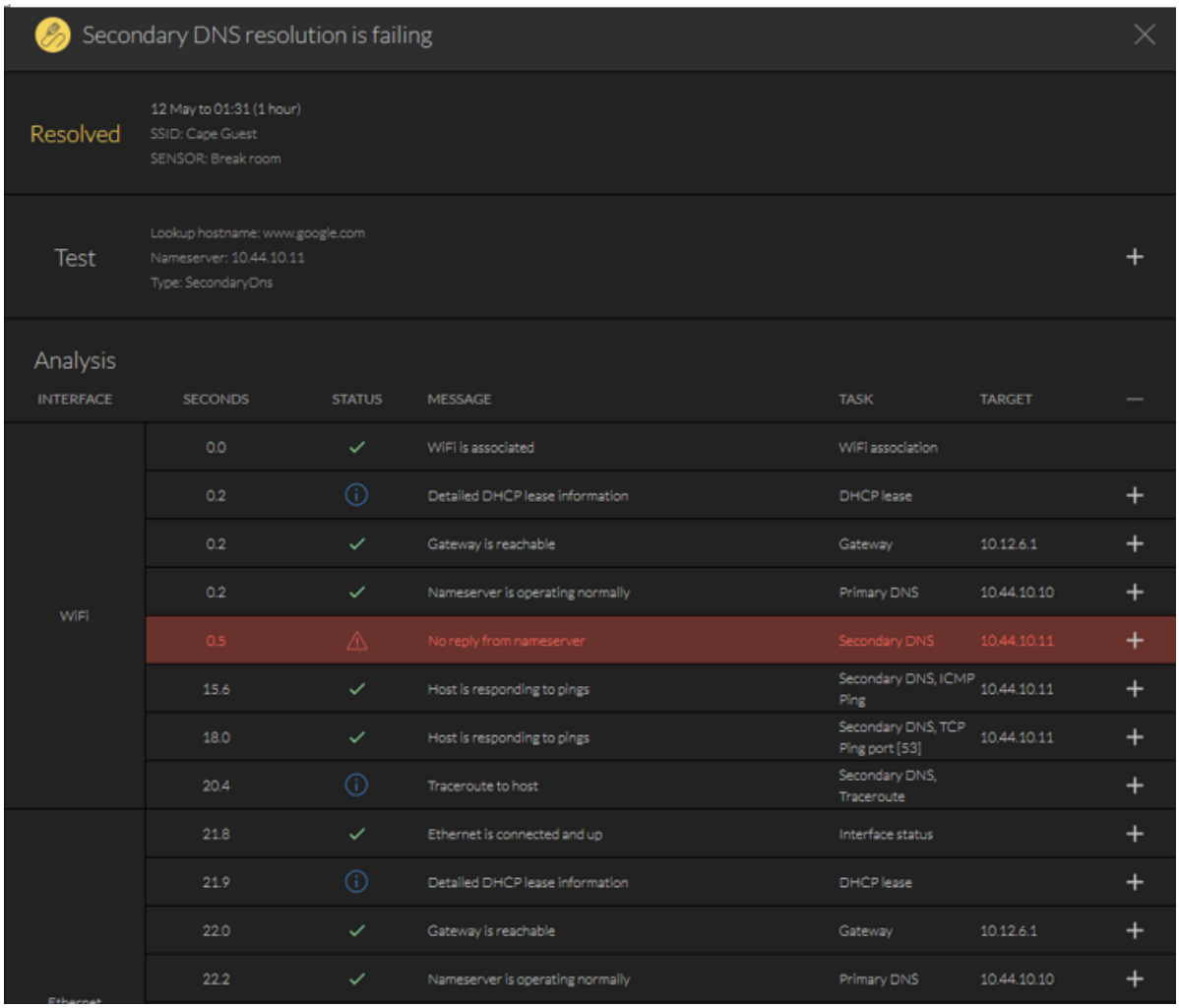
Again you click on the "+" signs to get more information about this error and even download the pcap.

We now click on the "Export as text file" and get this.



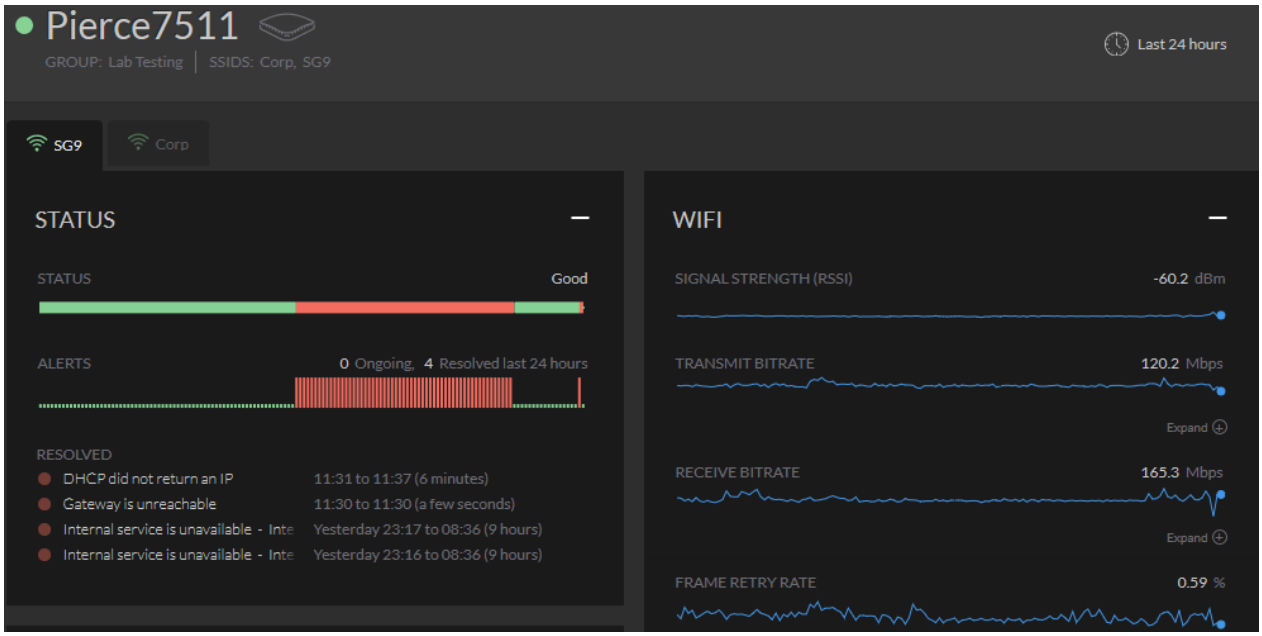
7.3 DNS Issue Visibility

Here is the screenshot showing that the DNS resolution us failing and it clearly displays what DNS was setup and helps in quickly resolving the issue.

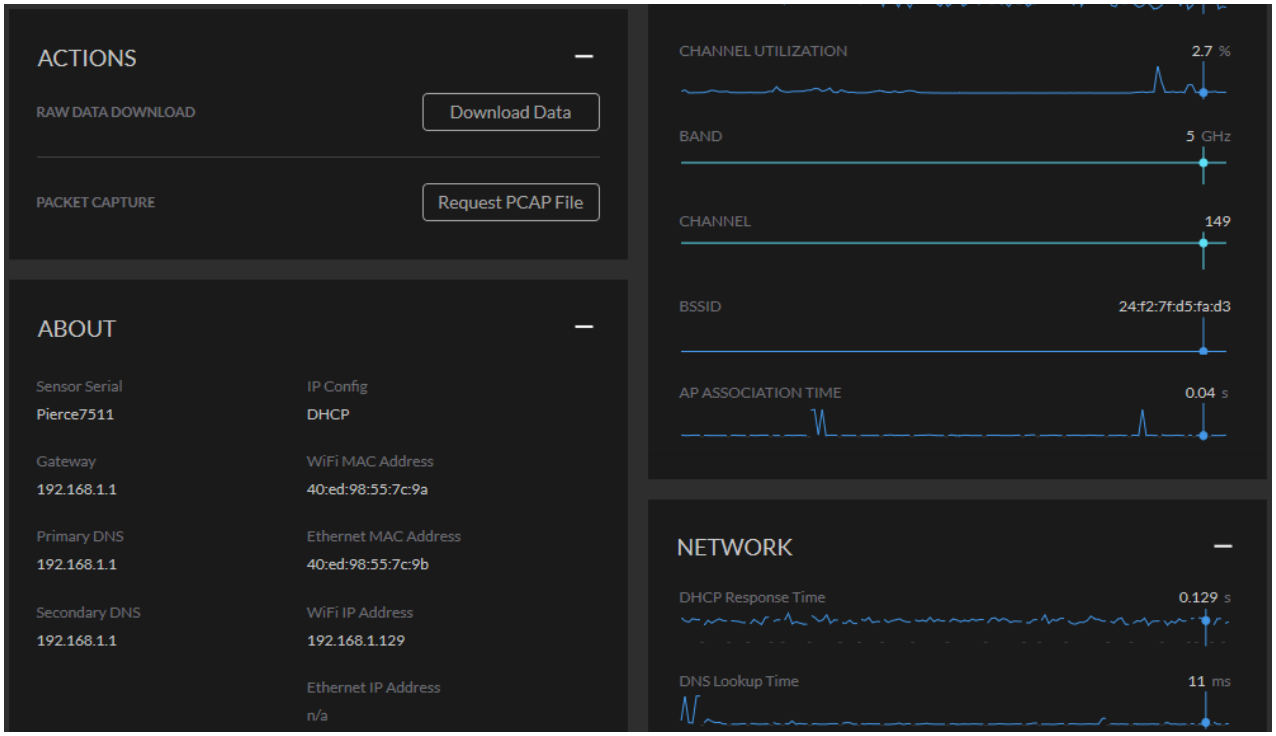


7.4 Sensor Visibility

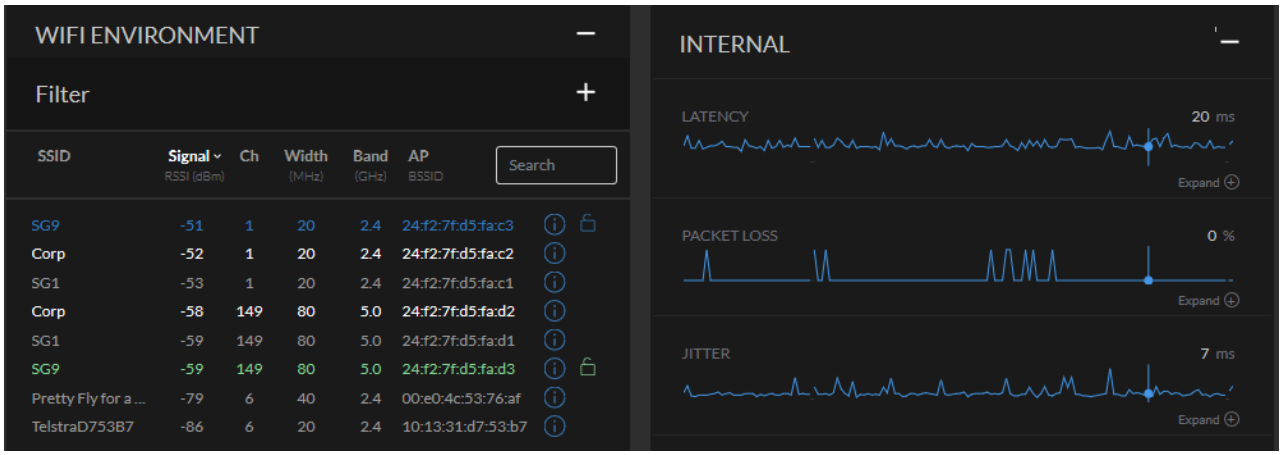
You can view all the information pertaining to a specific sensor by clicking on the sensor name from the main dashboard. At the top you get all the warning and the error with full view of the WiFi metrics.



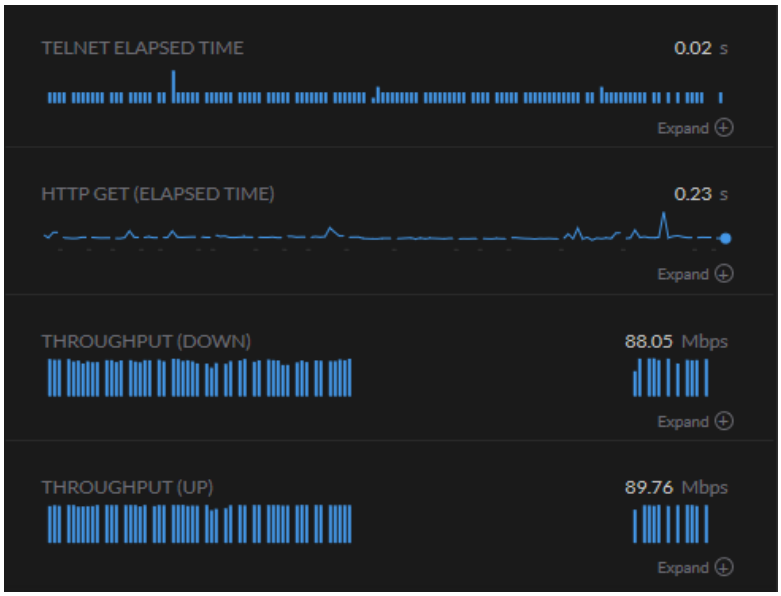
It continues with WiFi metric, the ability to download pcaps and the DHCP and DNS timings.



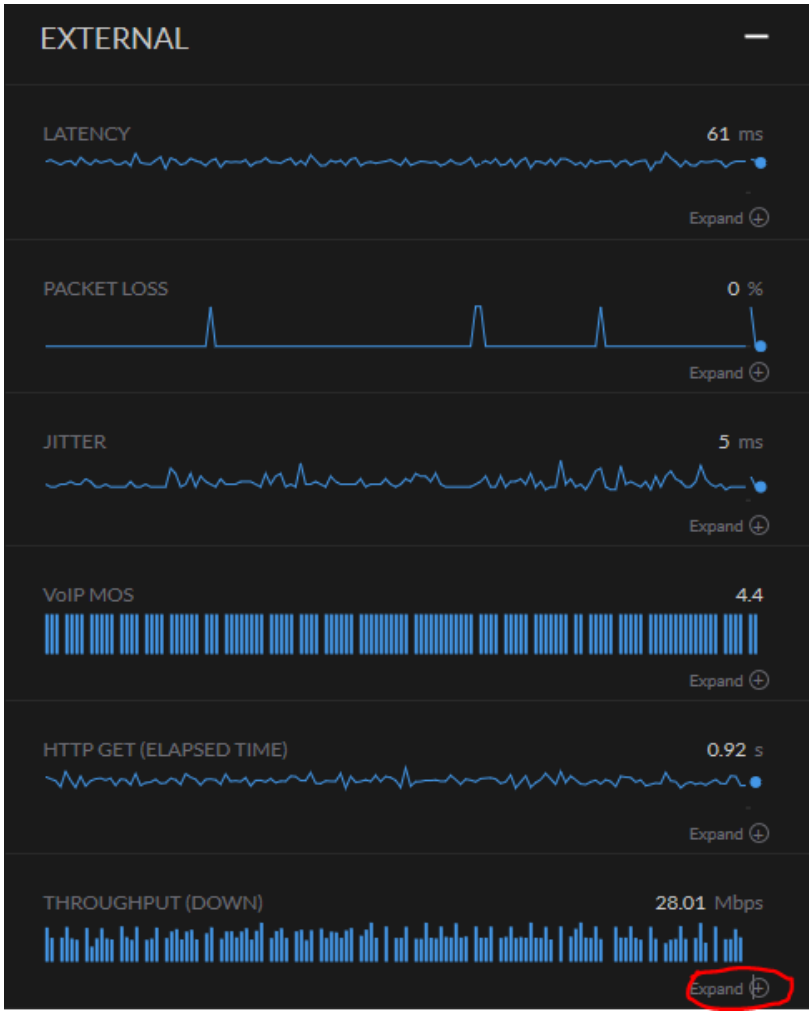
It then continues with WiFi environments where you can see the interference and other SSIDs that are being broadcasted along with Internal tests and their metrics of latency, packet loss and jitter.



It then continues with the remaining metrics of internal tests like telnet and SSH response time along with throughput tests in both direction.



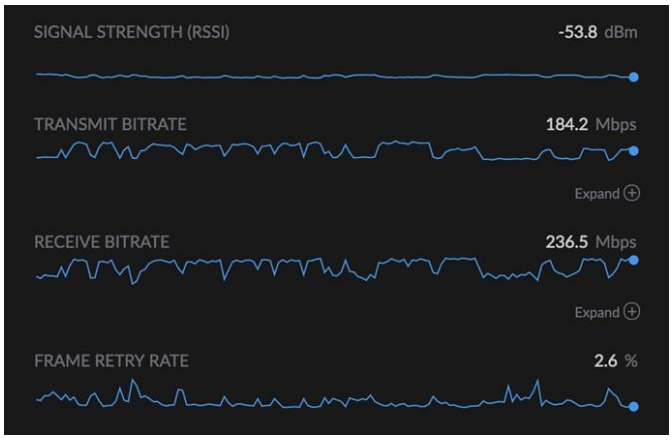
And finally the external tests.

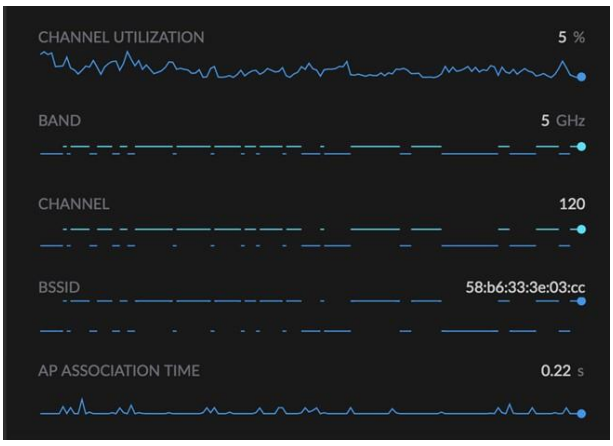


Clicking on the expand button will give you the details of external load tests.

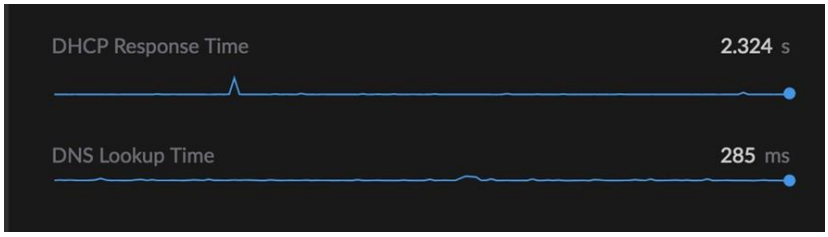
7.5 NAPLAN Metrics Visibility

Here is the screenshot showing some of the NAPLAN related metrics starting with WiFi environment.





DHCP and DNS Response times



Now looking a NAPLAN Latency values

NAPLAN Site reachability

And finally NAPLAN load test