# MANAGED WI-FI CLOUD DASHBOARD USER GUIDE

IT'S HOW WE CONNECT

# WELCOME TO THE MANAGED WI-FI CLOUD DASHBOARD USER GUIDE

This guide will help you navigate and complete critical tasks to benefit your business and provide tips to better utilise the application.

**Please note that for customers with Read-only Access, some options listed in this user guide may be able to be seen and interacted with, but changes made will not be saved.**

## CONVENTIONS USED IN THIS GUIDE

The following typographical conventions are used in this guide for simplicity and readability:

Web addresses, e-mail addresses and hyperlinks are shown in ***bold italics***, for example ***www.telstraenterprise.com.au***.

Button names and titles/features on your computer screen are shown in *italics*.

User input is shown in `typewriter` font.

The **red text** used in images is example text. Any underlined green text, normal green text, blue text or grey text is a matching link on the portal.

# WHAT'S INSIDE

# CHAPTER 1
# GETTING STARTED

## 1.1 EMAIL AND PASSWORD

To log in to the Managed Wi-Fi Cloud dashboard, go to ***https://dashboard.meraki.com***. You will see the following:

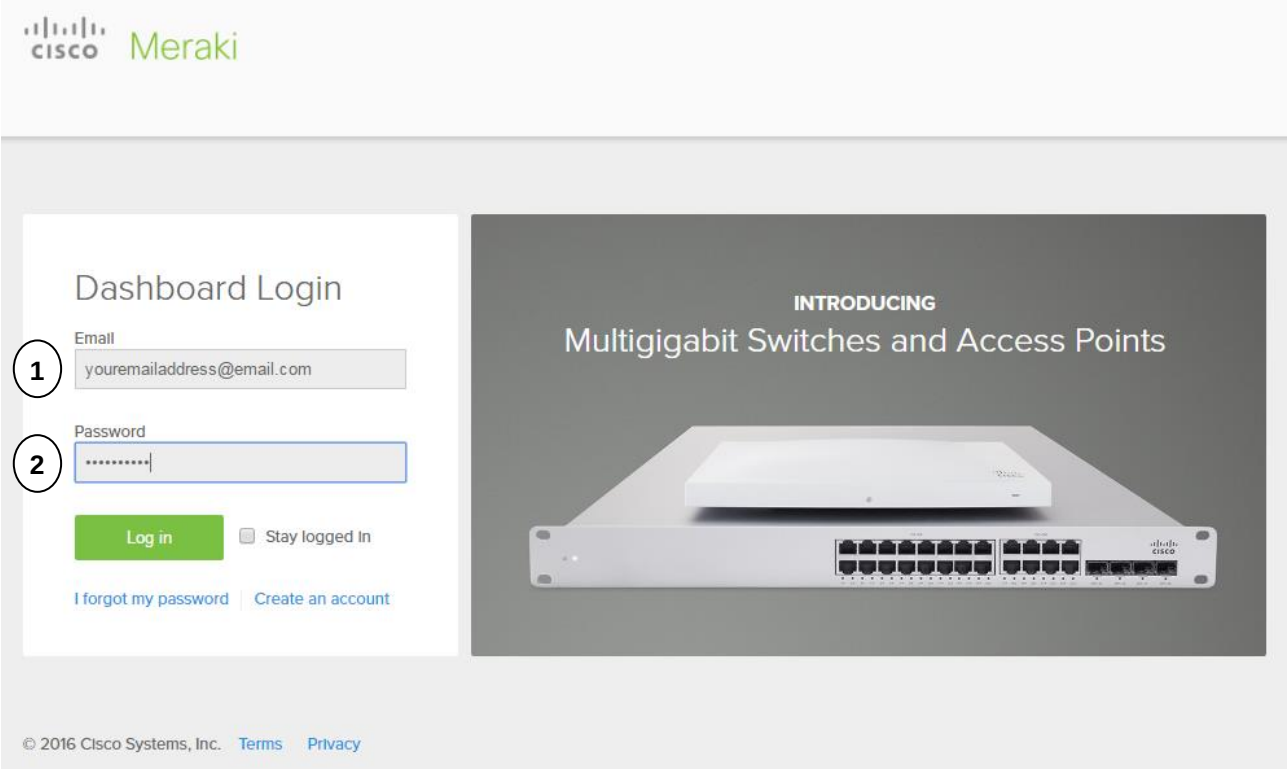



*Figure 1 – Managed Wi-Fi Cloud Dashboard Login Screen*

The first time you sign in to the dashboard, you will be asked to verify your identity. Sign in with:

1. Your **email address**, which is the email you have provided
2. The temporary **password** to log in is provided in the 'Welcome to Meraki' email that we have sent to you. If you forget your password, select I forgot my password, enter your email, and a password reset will be sent to your email address.

## 1.2 MY PROFILE

Click on my profile at the top right-hand side of the dashboard to update your account information, including creating your own password (*Figure 2 – Top section of Meraki Dashboard Home screen*).

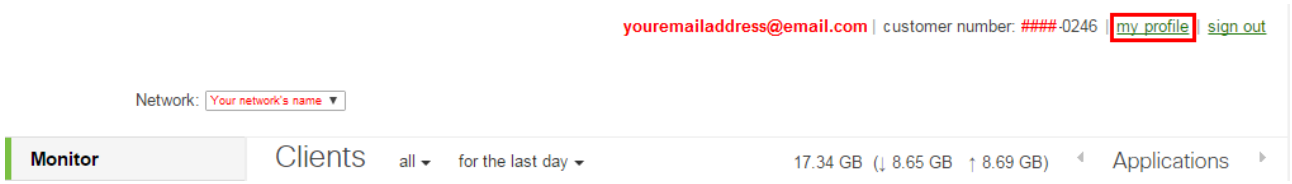



*Figure 2 – Top section of Meraki Dashboard Home screen*

You will be able to see the following, and take the following actions for each:

| HEADING | DESCRIPTION | ACTIONS |
|---|---|---|
| Your recent logins | Shows which IP address you have recently logged in from, where, and when, and your current IP address and location. | 1. Sort ▲ ▼ by **IP Address**<br>2. Sort ▲ ▼ by **Location**<br>3. Sort ▲ ▼ by **Date/Time** |
| Your active sessions | Shows which sessions are still "active" (i.e. not logged out) and their descriptions. | 1. Sort ▲ ▼ by date **Started**<br>2. Sort ▲ ▼ by the access **Location (IP Address)**<br>3. Sort ▲ ▼ by time of expiry (**Expiry In**)<br>4. Sort ▲ ▼ by when session was **Last Active**<br>5. Sort ▲ ▼ by browser/OS (**User Agent**)<br>6. End Sessions that are not currently active<br>7. **Sign out all other sessions** that are not active |
| Your email address | View or change the email address linked to this account | 1. Change your email address |
| Your account | View or change your account details (name, address, phone) | 1. Change your account details |
| Change your password | Change your account password | 1. Change your password |
| Two-factor authentication | View, setup or change your SMS authentication or offline access on a mobile device | 1. Set up SMS authentication<br>2. Set up offline access |
| Color blind assist mode (ON – Red/Green/OFF) | Preview, enable or disable Red/Green colourblind mode | 1. Enable/Disable Red/Green colourblind assist mode<br>2. Preview Red/Green colourblind assist mode (mouse hover) |

## 1.3 NAVIGATION

All your networks, plus an Overview of your networks, can be selected in the Network selection drop-down at the top left. For more information on the Overview, please go to **Chapter 2 – Overview**.

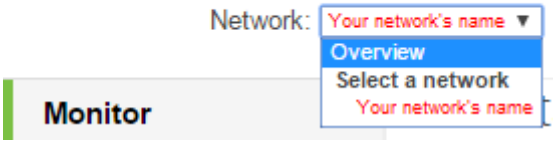



*Figure 3 – Network selection drop-down*

The monitor portal is navigated using the menu options on the left-hand side of the page, underneath the logo and Network selection drop-down.

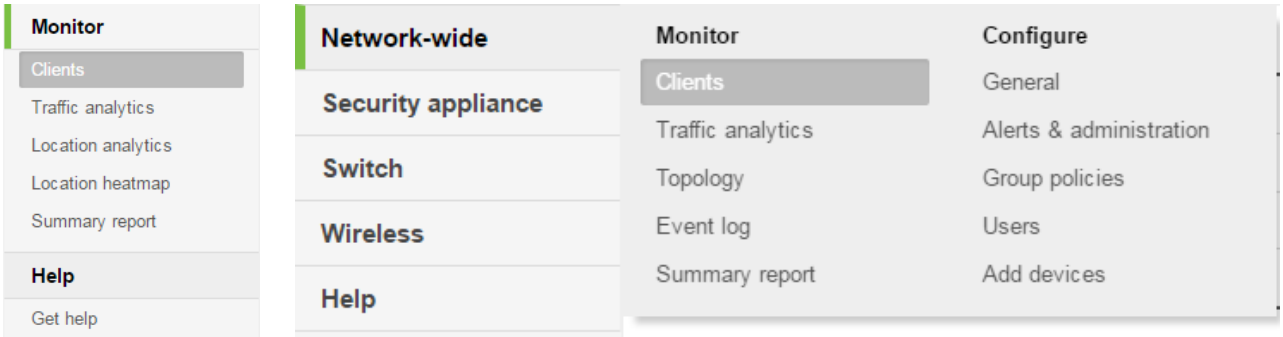



*Figure 4 – Navigation Menu Options & Configurations (hover for extra menu items)*

There are up to five different sections/tabs available in the Navigation Menu:

1. Network-wide OR Monitor
2. Security appliance
3. Switch
4. Wireless
5. Help

Depending on your network's configuration and access type, different sections may be available for different users. The Help section will always be present.

The menu items provided are listed below, please see each individual chapter for details.

**Monitor-only**

- **Chapter 3** – **Clients** – default menu, all your clients for this network are listed here
- **Chapter 4** – **Traffic analytics** – detailed view of how many clients, aggregated usage, application breakdown/ usage
- **Chapter 5** – **Presence analytics** – real-time information on non-associated Wi-Fi clients and intuitive reports on device presence to understand foot traffic behavior
- **Chapter 6** – **Presence heatmap** – a visual indication of coverage based on client connectivity
- **Chapter 7** – **Summary report** – a complete overview of the current network

In Read-Only Access, the **Network-Wide** menu is slightly different. Each Device Type has two sub-menus: **Monitor**, and **Configure**. Up to three device types are available: **Security appliance, Switch,** and **Wireless** access point. The Live Data & Summary page for each device in each Device Type is consistent, and further information can be found in **Chapter 10 – Live Data & Device Summary**.

The following options are available for each sub-menu:

| MENU ITEM | MONITOR | CONFIGURE |
|---|---|---|
| **Chapter 9 – Network-Wide** | Clients<br>Traffic analytics<br>Topology<br>Event log<br>Summary report | General<br>Alerts & administration<br>Group policies<br>Users<br>Add devices |

| | | |
|---|---|---|
| **Chapter 11 – Security appliance** | Appliance status<br>Route table | Addressing & VLANs<br>DHCP<br>Firewall<br>Site-to-site VPN<br>Client VPN<br>Active Directory<br>Traffic shaping<br>Access control<br>Splash page<br>Wireless concentrator |
| **Chapter 12 – Switches** | Switches<br>Switch ports<br>DHCP servers | IPv4 ACL<br>Access policies<br>Port schedules<br>Switch settings |
| **Chapter 13 – Wireless** | Access points<br>Map & floor plans<br>Air Marshal<br>Location analytics<br>Location heatmap<br>PCI report<br>Bluetooth clients<br>RF spectrum | SSIDs<br>Access control<br>Firewall & traffic shaping<br>Splash page<br>SSID availability<br>Bluetooth settings<br>Radio settings |

## 1.4 WHERE TO GET HELP

Hovering over **Help** will reveal the Get help and Firewall info tabs, which leads to the Telstra Managed Wi-Fi Cloud Help page and Firewall information respectively. If you need more help, please contact your Telstra representative, or, for 24 x 7 support, call ***1800 815 851***.

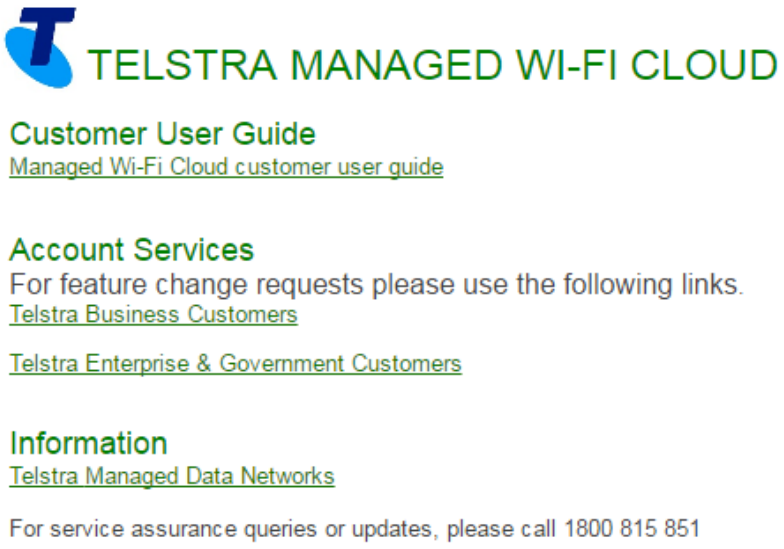



*Figure 5 – Managed Wi-Fi Cloud Help*

Your Firewall information can be found in the Firewall info tab. It can be sorted ▲▼ by any of the seven columns **Source IP**, **Destination IP**, **Ports**, **Protocol**, **Direction**, **Description** and **Devices using this rule**. These rules (plus the unfiltered rules can be downloaded by selecting the **Download…** ▼ button.

## Firewall information

This list is intended to help guide you in creating firewall rules for the Cisco Meraki cloud.

| Source IP ▲ | Destination IP | Ports | Protocol | Direction | Description | Devices using this rule |
|---|---|---|---|---|---|---|
| Your network(s) | Destination IPs/subnets | 1812, 7351 | UDP | outbound | Meraki cloud communication, 802.1X with Meraki RADIUS | Access points, Cameras, MX Security Appliance, Phones, Switches |
| Your network(s) | Destination IPs/subnets | 80, 7752 | TCP | outbound | Backup Meraki cloud communication, Throughput tests live tool | Access points, Cameras, MX Security Appliance, Phones, Switches |
| Your network(s) | Destination IPs/subnets | 80, 443, 7734 | TCP | outbound | Backup configuration downloads, Backup firmware downloads, Splash pages | Access points, Cameras, MX Security Appliance, Phones, Switches |
| Your network(s) | Destination IPs/subnets | 123 | UDP | outbound | NTP time synchronization | Access points, Cameras, MX Security Appliance, Switches |

Download... ▼

*Figure 6 – Managed Wi-Fi Cloud Help (left) and Firewarll information (right)*

# CHAPTER 2
# OVERVIEW

An organisational overview can be displayed that includes site Names, usage per site, clients, tags, network types, bar chart health, number of devices per site, offline devices and percentage of downtime. To access this Overview, select Overview in the Network selection drop-down.

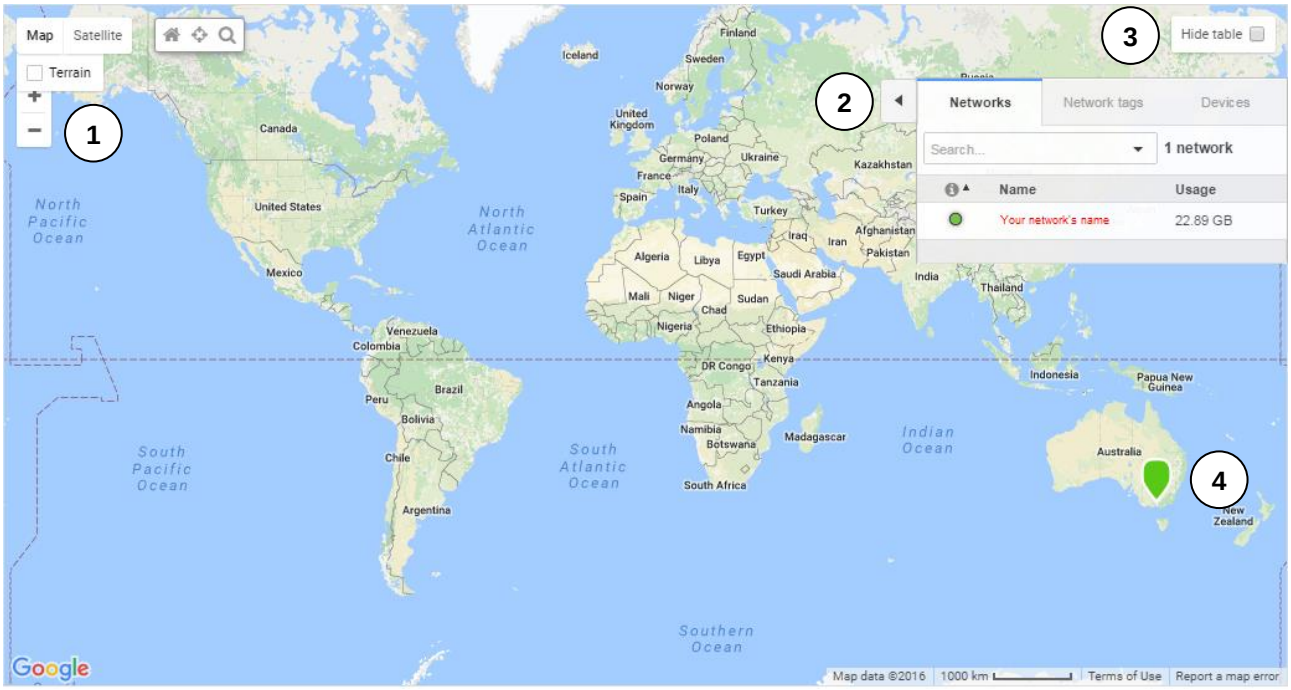



*Figure 7 – Overview*

The default view of the Overview is a map of the world, with markets where your networks are located, and a shortened version of the Network & Devices table.

1. **Google Maps map options**
2. **Networks & Devices table** – table showing the organisational overview for Networks, Network tags, and Devices. The following features are available on both the contracted and expanded versions of the table:

| ACTION | RESULT |
|---|---|
| Selecting ◂ or ▸ | Table to expand or contract respectively |
| Selecting a device line in **Networks** or **Devices** tab | Hovering over line will turn it yellow (Your network's name). Takes you to Clients page – please see **Chapter 3 – Clients** for more information. |
| Sort ▲ ▼ | Sort by the column names in each of the tabs (more options available in expanded table) |

Search

| FILTER | STRING |
|---|---|
| ***Special Commands*** | COMPOUNDED results: (`result1`) **AND** (`result2`) **AND** …<br>ALL results with at least one filter: (`result1`) **OR** (`result2`) **OR** …<br>NOT result: -(`result string`)<br>More than one special command can be used at once. |
| **Description** | Any `string` within the Description box, or **(**`string`**)** within the Search box at the top. |
| **Status** | **(status:**`string`**)** OR **(status:"**`string`**")** |
| **Firmware status** | **(firmware_status:**`string`**)** OR **(firmware_status:"**`string`**")** |
| **Firmware security** | **(firmware_security:**`string`**)** OR **(firmware_security:"**`string`**")** |
| **Network type** | **(type:**`string`**)** OR **(type:"**`string`**")** |
| **Device type** | **(device:**`string`**)** OR **(device:"**`string`**")** |

The `string` is not case sensitive. Not all categories appear on all tabs.

Once an option is selected, or the `string` is entered, then the search will automatically start. If the option is selected from the drop-down list, then it will appear within a blue box – normal x. Select x or delete the matching search string to remove this from your search.

The number of results returned will show as # **matches** in #.

**Please note that the search will be kept when switching to another tab.**

Hovering over ⓘ

Show help/more information about that particular column, e.g.:

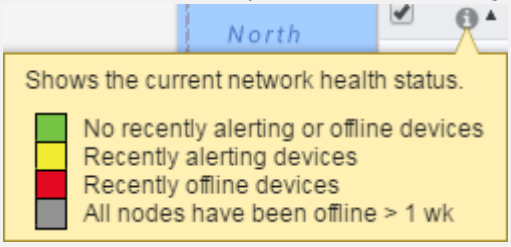



*Figure 8 – Hover-over information for Network Health Indicator*

More options are available in the expanded table.

On the **Expanded** the version of the table, along with extra columns, the following features are *also* available:

| TAB | FEATURES |
|---|---|
| All tabs | 1. Small summary of the number of clients and the amount of traffic last week<br>2. **Select columns** to be displayed in the Client Devices table by selecting the + icon. A checked box means that the column will appear, and an unchecked box, not appear. To change the ordering of the columns, click, hold and drag the column name.<br>3. **Download data** as a .csv file. |
| Networks | 1. **Select/Deselect** networks with the check-box<br>a. **Tag/Untag** networks that are marked with a check<br>b. **Combine/split networks** that are marked with a check (an information box will also appear upon hovering)<br>c. **Delete** networks that are marked with a check |

3. **Show/Hide Network & Devices** table
4. **Network Markers** – shows the location of your networks. The colour used matches the colour listed next to that particular network, under the ⓘ in the Network & Devices table. The marker outline will change from white to black and increase in size when the corresponding network is mouseovered, or when the market itself is mouseovered. In the latter case, a summary will also appear. Selecting the network name will take you to the Clients page – please see **Chapter 3 – Clients** for more information.

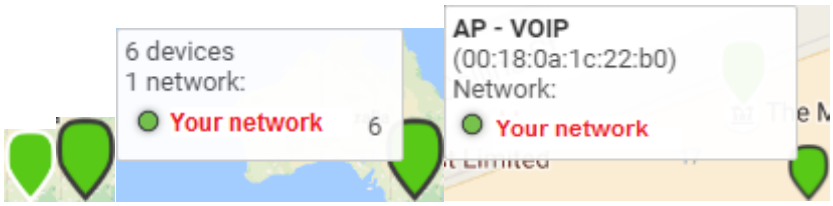



*Figure 9 – Markers: Normal, Outlined, Summary of a group marker (2+ devices), Summary of a singular marker*

If there is a number on the bottom right of the summary (middle-right figure), selecting the marker will zoom in on that network and show each different client/device in that area:


*Figure 10 – Markers: Normal (left), Outlined (middle), Outlined with Summary (right)*

Markers will combine or uncombine depending on the scale of zooming. Larger markers denotes more devices within one area.

# CHAPTER 3
# CLIENTS

Clients are devices that have been attached to your Wi-Fi network. The clients page is the default home screen on the dashboard, it shows how the network is being used by client devices – see **Figure 11 – Clients Page**.

To change between networks, select the Network selection drop-down in the top left.

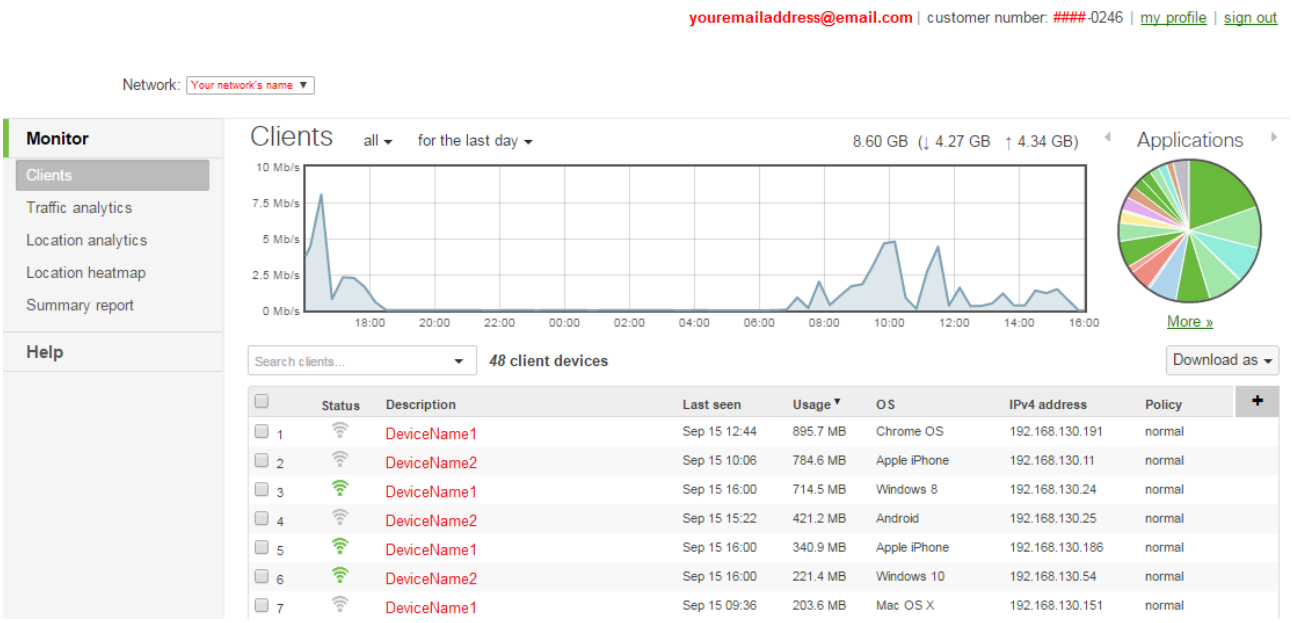



*Figure 11 – Clients Page*

A device can be selected by selecting anywhere on that particular device line (hovering over a line will turn it yellow  ) – please refer to **Section 2.4 – Client Representation** for more information.

## 3.1 TRAFFIC GRAPH

The traffic graph below shows the amount of traffic generated by the clients on the networks within your organisation. The values, time period and data shown depends on the filter(s) applied to it.

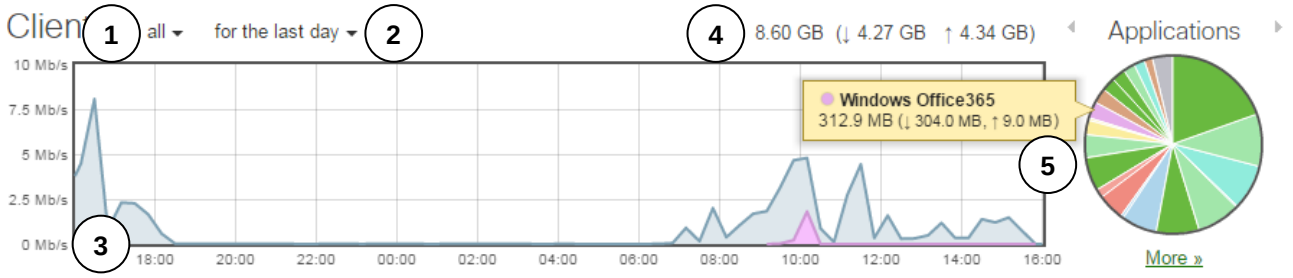



*Figure 12 – Client Traffic Graph*

It has the following features:

1. **Network or Devices filter** – change the network or the type of devices that are displayed on the graph. They are separated into the following categories:

| SECTION | FILTERS |
|---|---|
| 1 – All | 1. All devices (clients) on all networks.<br>2. Only devices (clients) with a policy |
| 2 – Specific Clients | 1. Only security appliances<br>2. Only access points<br>3. Only switches |
| 3 – Specific Network | 1. Only devices on *network_01_name*<br>2. Only devices on *network_02_name*<br>… |

2. **Time filter** – view a specific time period that devices were in use.

| FILTERS |
|---|
| 1. **For the last 2 hours**<br>2. **For the last day**<br>3. **For the last week** (7 days)<br>4. **For the last 30 days** |

3. The numerical value of the **total traffic** is shown at the top right-hand side, separated into ↓ **download** and ↑ **uploaded** values in brackets.
4. The **average speed over time** is shown in the graph. The x-axis (horizontal) shows the time in 24-hour format, and the y-axis (vertical) shows the average speed across all clients at that particular time.
5. A breakdown of the **usage per application, port or HTTP content** over this period of time – this is explained in-depth in **Section 2.2 – Applications, Ports & HTTP content**. Hovering over a section will show the description (name) of the application, colour associated, and the total traffic for that application, separated into ↓ **download** and ↑ **uploaded** values in brackets.

## 3.2 APPLICATIONS, PORTS & HTTP CONTENT

The pie chart shows a breakdown of the traffic and details. Selecting the ◂ left or right ▸ arrows will change the type of content and traffic, between Applications, Ports and HTTP content. Clicking on a sector or More ›› will open up the **Applications/Ports/HTTP content details** drop-down, with the following features:

1. Application details (mouseover)
2. Application usage overlaid over total usage
3. View and **sort** ▲▼ all **Applications details**, including:
   - **Description** – name of application (may include IP address)
   - **Group** – type of data usage
   - **Usage** – amount of traffic in bytes
   - **% Usage** – percentage of traffic
   - **Group usage** – total amount of traffic used by this particular group

- **Group % usage –** percentage of traffic for this particular group

4. Change between **20** and **all** results displayed per page
5. Go to the **previous page**, a specific page number (e.g. 1, 2, 3), or the **next page**
6. ‹‹ Hide **Applications details**

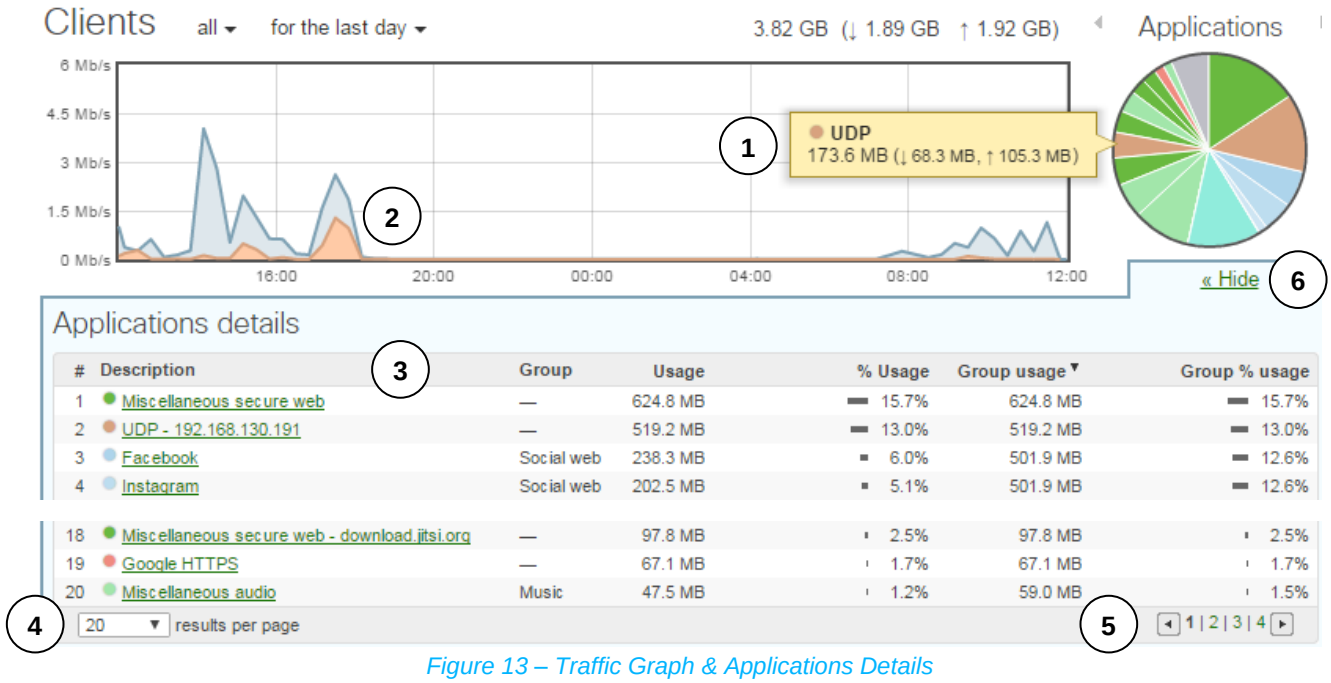



*Figure 13 – Traffic Graph & Applications Details*

An application can be selected by selecting anywhere on that particular device line (hovering over a line will turn it yellow 2 YouTube), and take you to a page called **Rule details: Applications – *ApplicationName***:

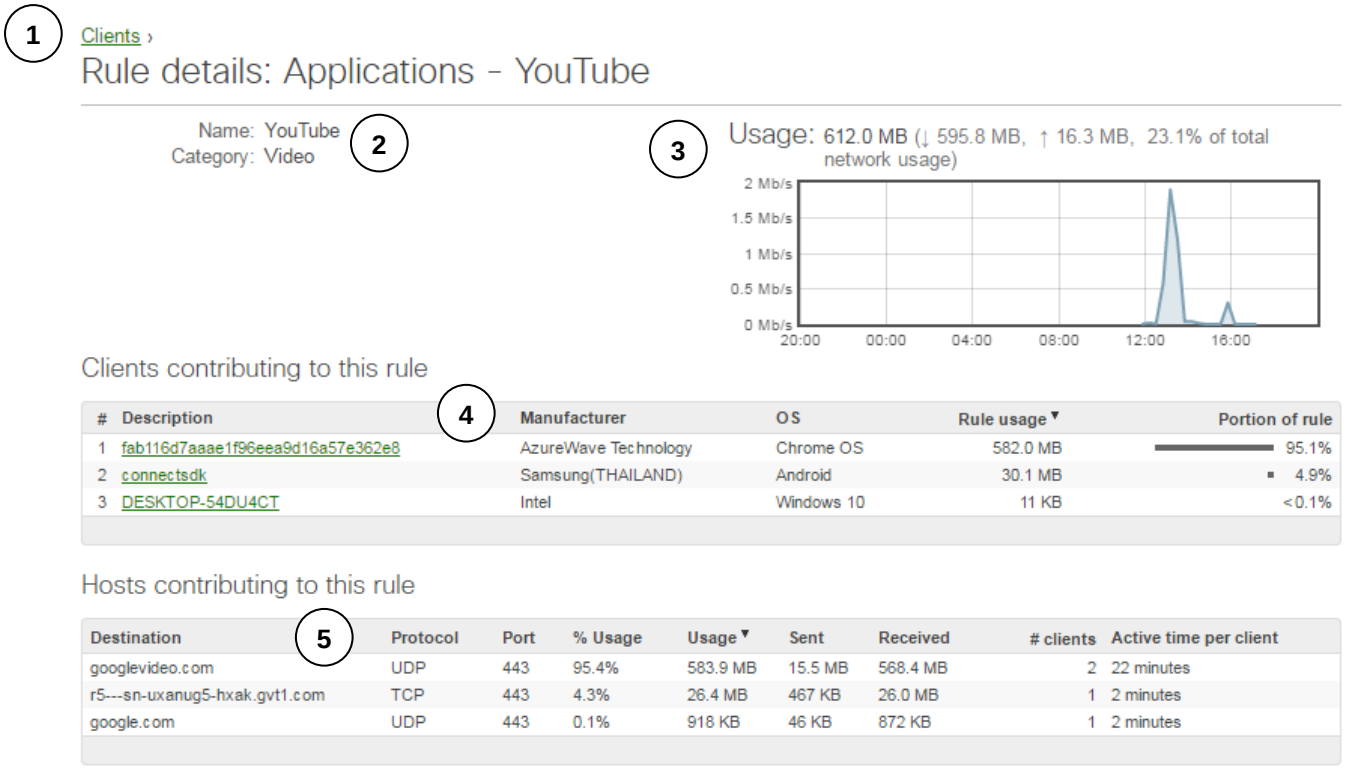



*Figure 14 – Rule details (Applications)*

1. **Breadcrumb Trail** – clicking a green link will take you back to that page
2. **Application name and category**
3. **Usage over time** graph – the total traffic for this specific application, separated into ↓ **download** and ↑ **uploaded** values, and **percentage of total network usage** in brackets.
4. View and **sort** ▲▼ all **Clients contributing to this rule**, by:
   - **Description** – name of application (may include IP address)
   - **Manufacturer** – of device
   - **OS** – operating system/device that the client has connected with
   - **% Usage** – percentage of traffic
   - **Rule usage** – total amount of traffic used by this particular group
   - **Portion of rule –** percentage of traffic for this particular group
5. View and **sort** ▲▼ all **Hosts contributing to this rule**, by:
   - **Destination** – of pinged website
   - **Protocol** – network protocol used to contact website
   - **Port** – network port used to contact website
   - **Usage** – amount of traffic in bytes
   - **% Usage** – percentage of traffic
   - **Sent** – amount of traffic sent to destination (uploaded)
   - **Received** – amount of traffic received to destination (downloaded)
   - **# clients** – number of the clients that contacted this host
   - **Active time per client –** average amount of time spent at host by each client

   An individual device can be selected by selecting its device name under the Description, and take you to the device's individual page – please refer to **Section 2.6 – Client Representation** for more information.

## 3.3 CLIENT DEVICES

Beneath the **Traffic Graph** is the **Client section**, which shows the users that are currently connected to the network:

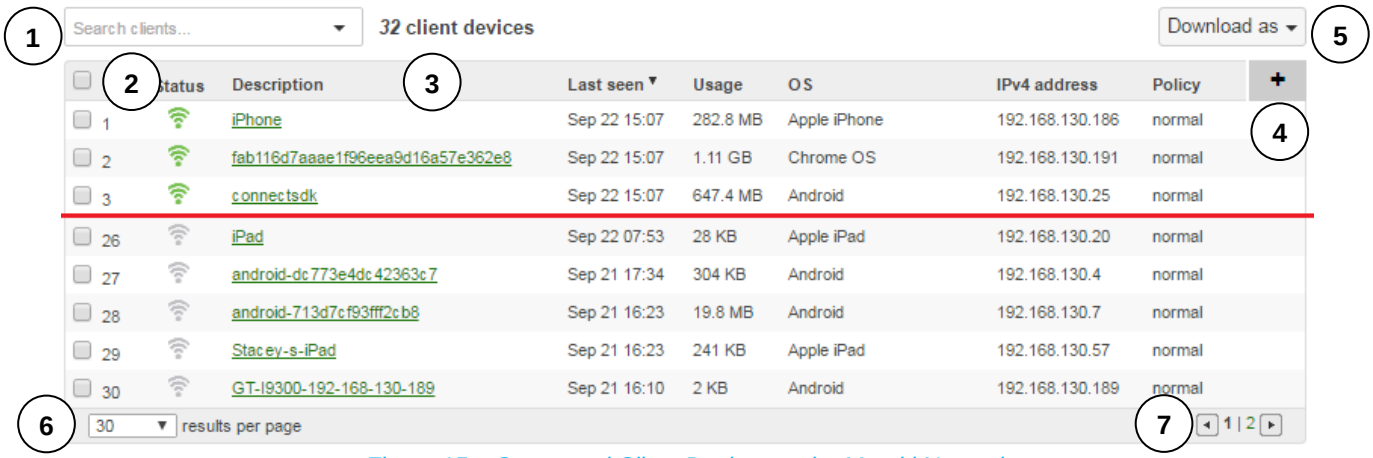



*Figure 15 – Connected Client Devices to the Meraki Network*

The following is provided in the Client Devices section:

1. **Search** and **total number of clients**. This number changes depending on the filters from the Client section above, and updates in real time as a search is applied.

    - Selecting the Search box (Search clients…) allows you to type in characters. To filter by a certain types of **directly**, or multiple filters, the following strings can be used:

| FILTER | STRING |
|---|---|
| ***Special Commands*** | • COMPOUNDED results: (result1) **AND** (result2) **AND** …<br>• ALL results with at least one filter: (result1) **OR** (result2) **OR** …<br>• NOT result: -(result string)<br>• More than one special command can be used at once. |
| **Status** | Wireless – **is:wireless**<br>Wired – **is:wired**<br>Online – **is:online**<br>Offline – **is:offline** |
| **OS** | **(os:**`string`**)** OR **(os:"**`string`**")** |
| **Connected to** | **(on:**`string`**)** OR **(on:"**`string`**")** |
| **VLAN** | **(vlan:**`string`**)** OR **(vlan:"**`string`**")** |
| **Policy** | **(policy:**`string`**)** OR **(policy:"**`string`**")** |

    The `string` is not case sensitive.

    - Selecting ▼ will cause the same filters to appear. These can be used to filter directly by:

        i. Checking/Unchecking the **Status**

        ii. Selecting the text box under any of **OS**, **Connected to**, **VLAN**, or **Policy**, a drop-down list with all possible options to appear.

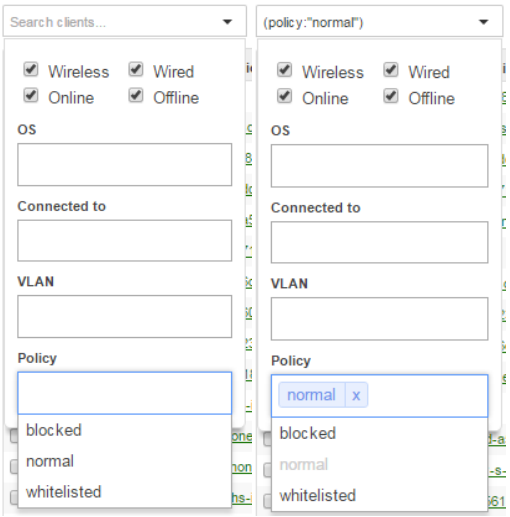



*Figure 16 – Client Devices search, before "normal" Policy (left) and after (right)*

Typing directly into this box is also possible. Once an option is selected, or the string is entered, then the search will automatically start. If the option is selected from the drop-down list, then it will appear within a blue box – normal x. Select x or delete the matching search string to remove this from your search.

2. **Check box** – select one or multiple devices
3. View and **sort** ▲▼ all columns. The default colums are:
    - **Status** – shows green for currently connected and grey for not connected

| STATUS | WIRED | WIRELESS |
|---|---|---|
| Online | | |
| Offline | | |

    - **Description** – name of application (may include IP address)
    - **Last Seen** – when a client connection was last on the network
    - **Usage** – amount of traffic in bytes
    - **OS** – operating system/device that the client has connected with
    - **IPv4 Address** – IP address the client has used for the connection
    - **Policy** – policy used for the client (if there are pre-configured policies in the system)
4. **Select columns** to be displayed in the Client Devices table by selecting the + icon. A checked box means that the column will appear, and an unchecked box, not appear. To change the ordering of the columns, click, hold and drag the column name.

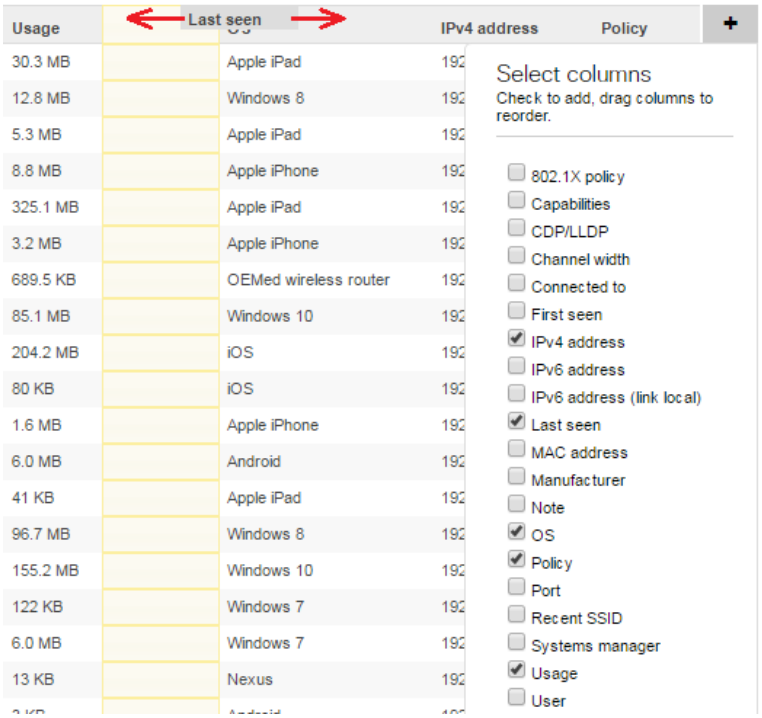



*Figure 17 – Selecting & moving columns*

5. **Download data** – as either a .csv or an .xml file.

6. Change between **30** and **all** results displayed per page
7. Go to the ◂ **previous page**, a specific page number (e.g. 1, 2, 3), or the **next page** ▸

## 3.4 CLIENT REPORTS

Select one of the clients from the client device menu to show the specific details for that device only.

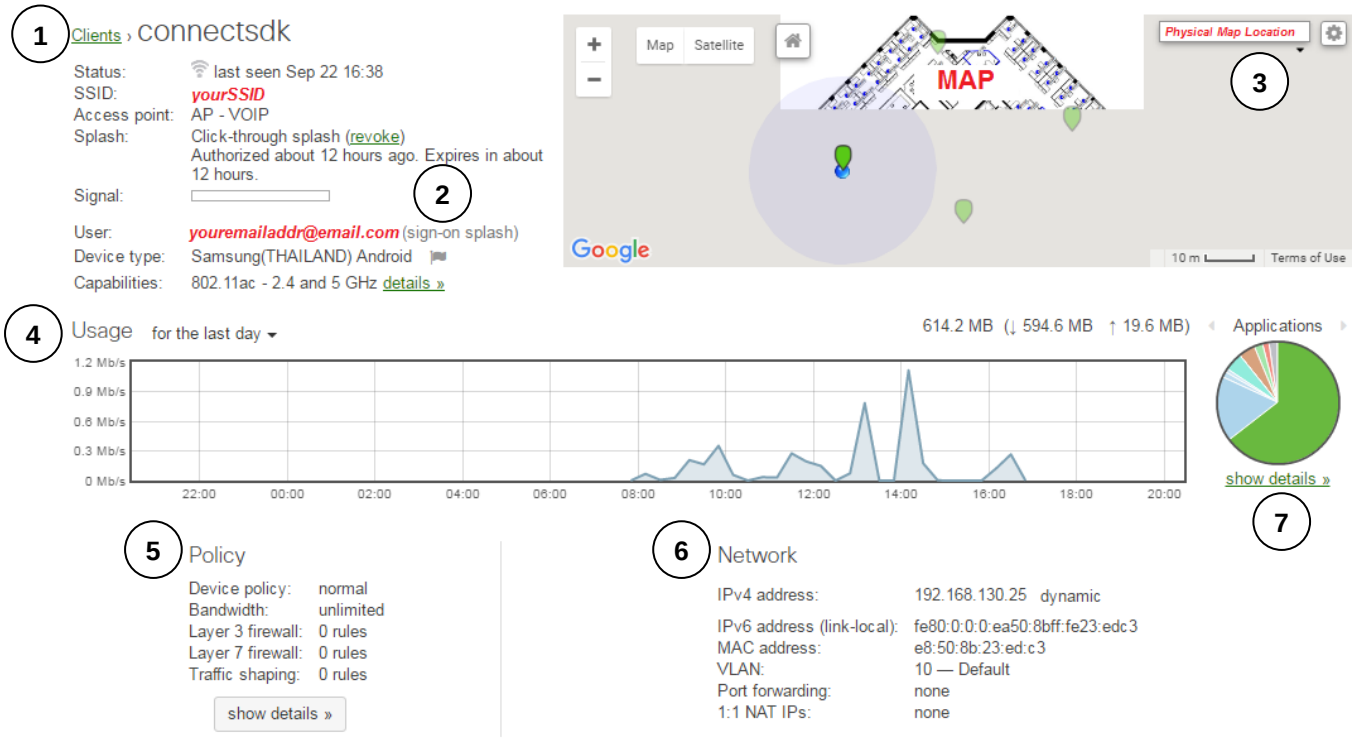



*Figure 18 – Selecting & moving columns*

1. **Breadcrumb Trail** – clicking a green link will take you back to that page
2. **Device Details** – of this particular device and its current status
   a. Selecting revoke will revoke the click-through splash.
   b. Selecting details ›› will show the channel width, maximum bitrate and the spatial stream information.
3. **Access Point Map** – shows which access point the device is connected to by a blue dot on the map. The map has normal Google Maps map options, as well as a drop-down list to select different. If it is a wireless device and a floorplan has been associated with the network, the map will show an **approximate** location for the device (accuracy dependant on wireless installation).
4. **Usage over time** graph – the total traffic for this specific application, separated into ↓ **download** and ↑ **uploaded** values, and **percentage of total network usage** in brackets. Its pie chart works the same way as the larger All Clients pie chart (see **Section 2.1 – Traffic Graph** and **Section 2.2 – Applications, Ports and HTTP content**), and selecting show details ›› will show the individual drop-down list for this device.
5. **Policies** – associated with this device. Selecting how details ›› will open an overlay with more detailed information on the rules.
6. **Network** – details about how the device is connected to the network

# CHAPTER 4
# TRAFFIC ANALYTICS

The Traffic Analytics page includes analysis of clients (devices), usage and applications.

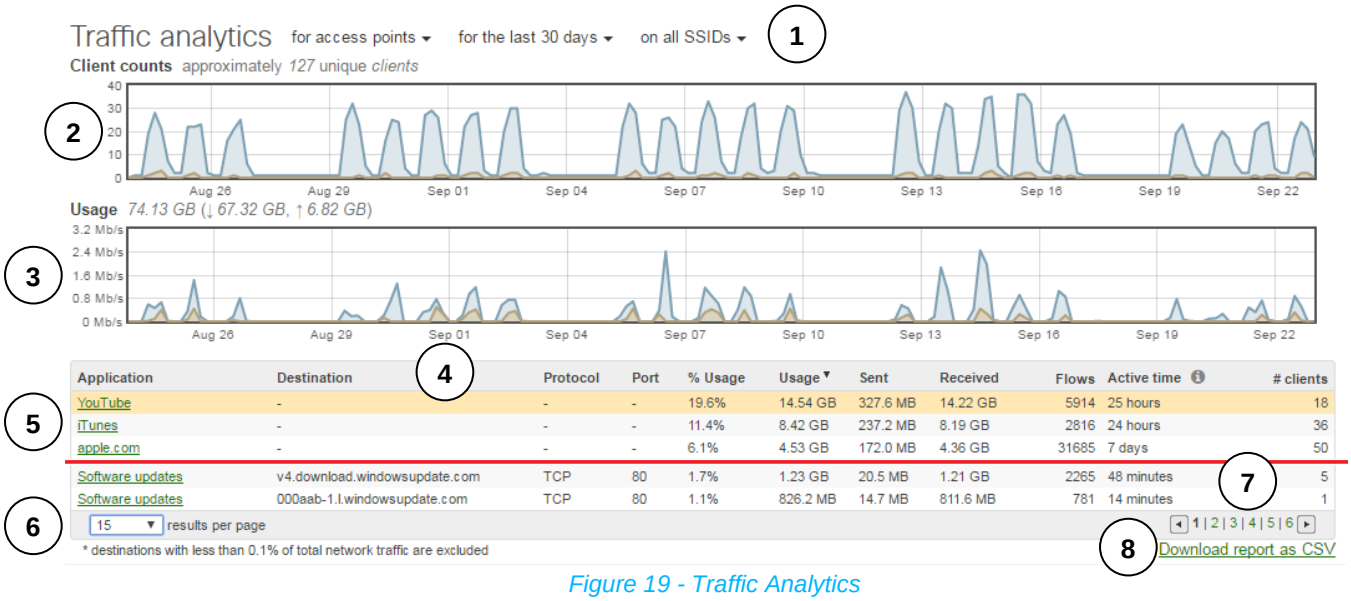



*Figure 19 - Traffic Analytics*

It has the following features:

1. **Three Filters** – change the type of device, time period and/or SSID broadcast by the clients. After selecting a filter, the information below it will automatically update.

| FILTER TYPES | FILTERS |
|---|---|
| For client type | 1. For security appliances<br>2. For access points<br>3. For switches |
| For time period | 1. For the last 2 hours<br>2. For the last day<br>3. For the last week<br>4. For the last 30 days |
| By SSID | 1. All SSIDs<br>2. SSID: *SSID_01_name*<br>3. SSID: *SSID_02_name*<br>…<br>If the network is disabled, then (disabled) will appear next to the SSID. |

2. **Client Count –** graph of number of clients connected to the network(s) filtered against the selected time period. It also displays the approximate *number* of unique *clients* that connected over this period of time.

3. **Usage/Traffic** – graph of the amount of traffic against the selected time period. The numerical value of the **total traffic** is shown on its right, separated into ↓ **download** and ↑ **uploaded**.
4. View and **sort** ▲▼ all **Applications details**, including:
    - **Application –** name of application (may include IP address)
    - **Destination** – website pinged
    - **Protocol** – network protocol used to contact website
    - **Port** – network port used to contact website
    - **% Usage** – percentage of traffic
    - **Usage** – amount of traffic in bytes
    - **Sent** – amount of traffic sent to destination (uploaded)
    - **Received** – amount of traffic received to destination (downloaded)
    - **Flows** – number of counts of connection to data source have taken place
    - **Active time** – across all clients using this application
    - **# clients** – number of the clients that contacted this host
5. **Individual Application** – can be selected by selecting anywhere on that particular device link – please refer to **Section 2.2 – Application, Ports & HTTP content** for more information. Hovering over a line will turn it yellow 

, and the amount of data and devices will be shown above as a brown overlay over the normal number of client and usage/traffic graphs.
6. Change between **20** and **all** results displayed per page
7. Go to the ◂ **previous page**, a specific page number (e.g. 1, 2, 3), or the **next page** ▸

a. Selecting revoke will revoke the click-through splash.

b. Selecting details ›› will show the channel width, maximum bitrate and the spatial stream information.

8. Download report as CSV file

# CHAPTER 5
# LOCATION ANALYTICS

The Managed Wi-Fi Cloud dashboard provides real-time information relating to Wi-Fi clients on the network and intuitive reporting on device presence. Retail and enterprise customers can use this information to better understand foot traffic across their sites.

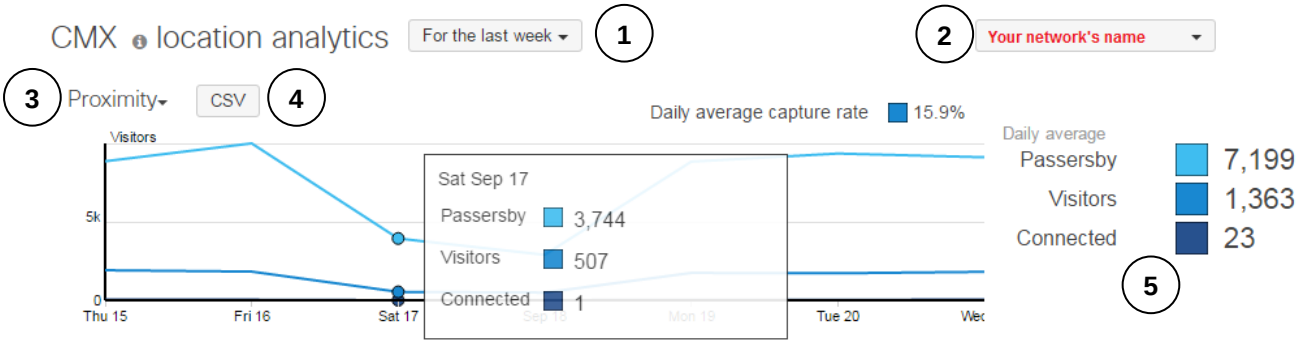



*Figure 20 - Traffic Analytics*

It has the following features:

1. **Time Filter** – change the time period from which the data is taken.

| FILTERS |
|---|
| 1. **For the last day**<br>2. **For the last week** (7 days)<br>3. **For the last month** (30 days)<br>4. **Custom range**: selectable *from* and *to* dates |

2. **Network Filter** – filter by either networks or nodes. Networks can be filtered by either a specific tag (please see **Chapter 2 – Overview** for how to tag networks), or by a network name. Nodes can be filtered by either all nodes, or nodes with a tag.
3. **Graph selection** – there are **six** graphs, three of which can be displayed at any one time.
    - **Proximity Rate** – please see **Section 5.1 – Proximity Rate** for more information.
    - **Capture Rate** – please see **Section 5.2 – Capture Rate** for more information.
    - **Engagement** – please see **Section 5.3 – Engagement** for more information.
    - **Median visit length** – please see **Section 5.4 – Median visit length** for more information.
    - **Loyalty** – please see **Section 5.5 – Loyalty** for more information.
    - **Repeat visitor rate** – please see **Section 5.6 – Repeat visitor rate** for more information.

Each graph comes in “pairs”; when the drop-down list is selected, the currently selected graph is greyed out. Each graph also shows extra information when mouseovered.

4. **Download** data as a .csv file
5. **Graph Statistics** – hovering over the coloured squares will change the thickness of the border in line graphs, or add a black outline in bar graphs.

For more information, hover over the ⓘ icon and follow the link.

## 5.1 PROXIMITY RATE

This graph displays three different types of visitors:

1. **Passersby** – the number of devices with Wi-Fi network search 'on', that have been identified by your network over a period of time
2. **Visitors** – the number of devices which have connected for at least 5 minutes
3. **Connected** – the number of devices that are actually connected

The Daily average capture rate is determined by the number of visitors, divided by the sum of the number of passersby and visitors.

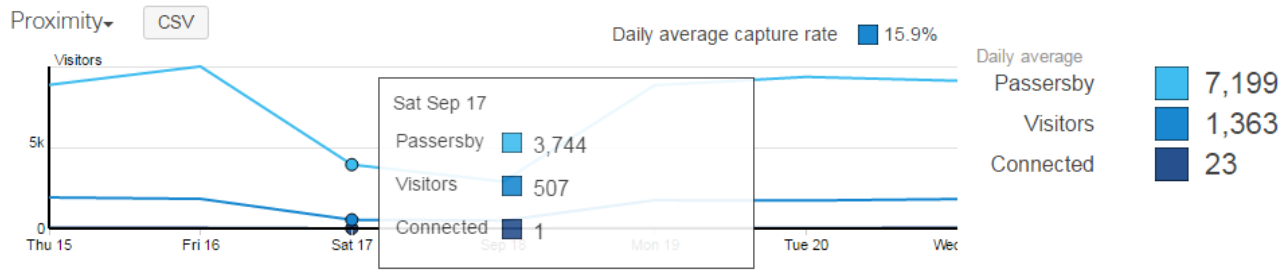



*Figure 21 – Proximity Rate Graph*

## 5.2 CAPTURE RATE

This graph shows the change in the daily average capture rate from the **Proximity Rate** over time.

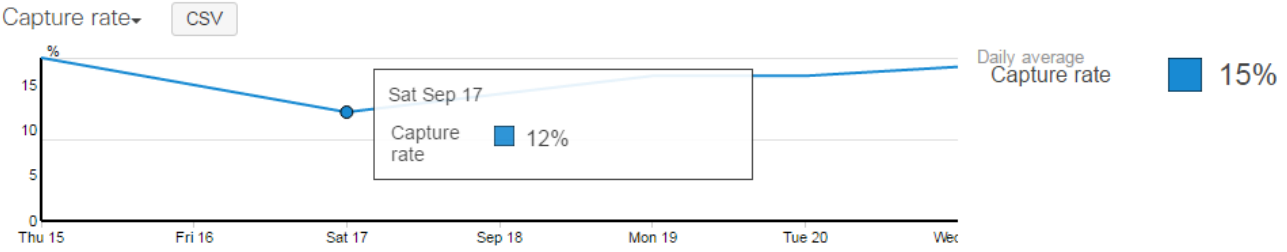



*Figure 22 – Capture Rate Graph*

## 5.3 ENGAGEMENT

This graph displays the number of unique visitors to your network by the duration of their longest visit. A single visitor who leaves and returns multiple times will only be counted once.

The Daily average visits is the average of all the total visits over the selected time period.

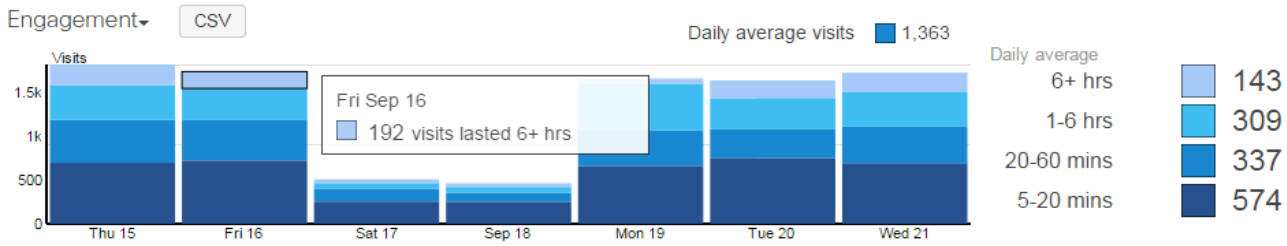



*Figure 23 – Engagement Graph*

## 5.4 MEDIAN VISIT LENGTH

This graph shows the change in the daily average median visit rate from **Engagement** over time.

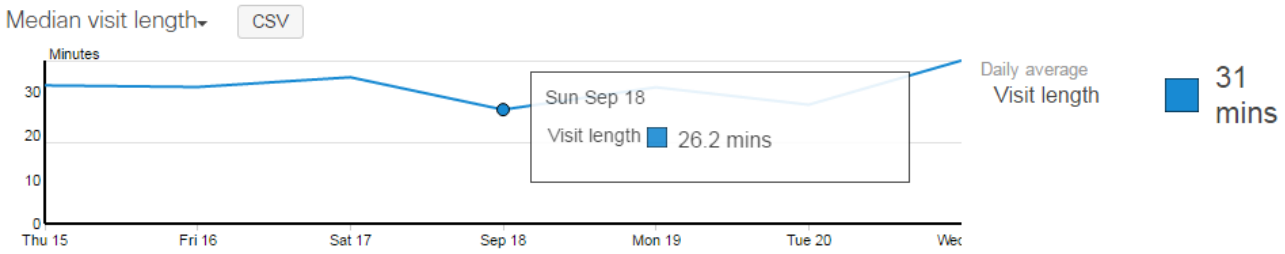



*Figure 24 – Median Visit Length Graph*

## 5.5 LOYALTY

This graph shows visitors based on how frequently they return. For example, a weekly visitor is someone who returned between 2 and 6 times in the last month.

The Daily average repeat rate is determined by the number of non-First time users, divided by ALL users.

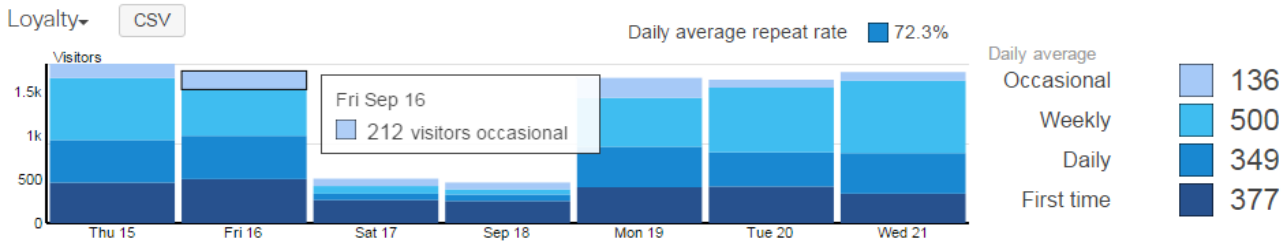



*Figure 25 – Loyalty Graph*

## 5.6 REPEAT VISITOR RATE

This graph shows the change in the daily average median visit rate from **Loyalty** over time.

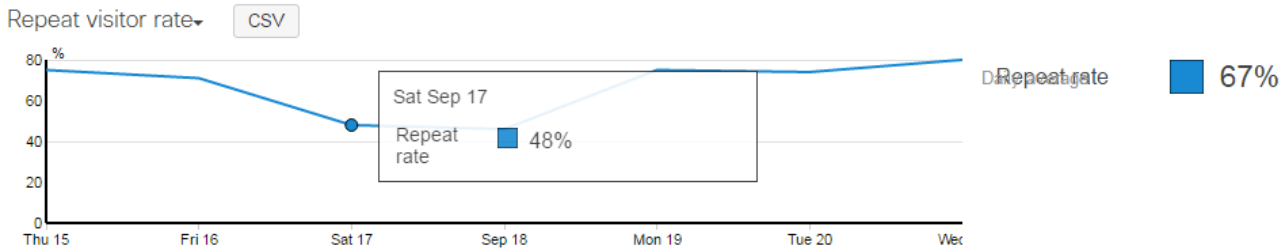



*Figure 26 – Repeat Visitor Rate Graph*

# CHAPTER 6
# LOCATION HEATMAP

The presence heat map provides a visual representation of coverage based on client connectivity.

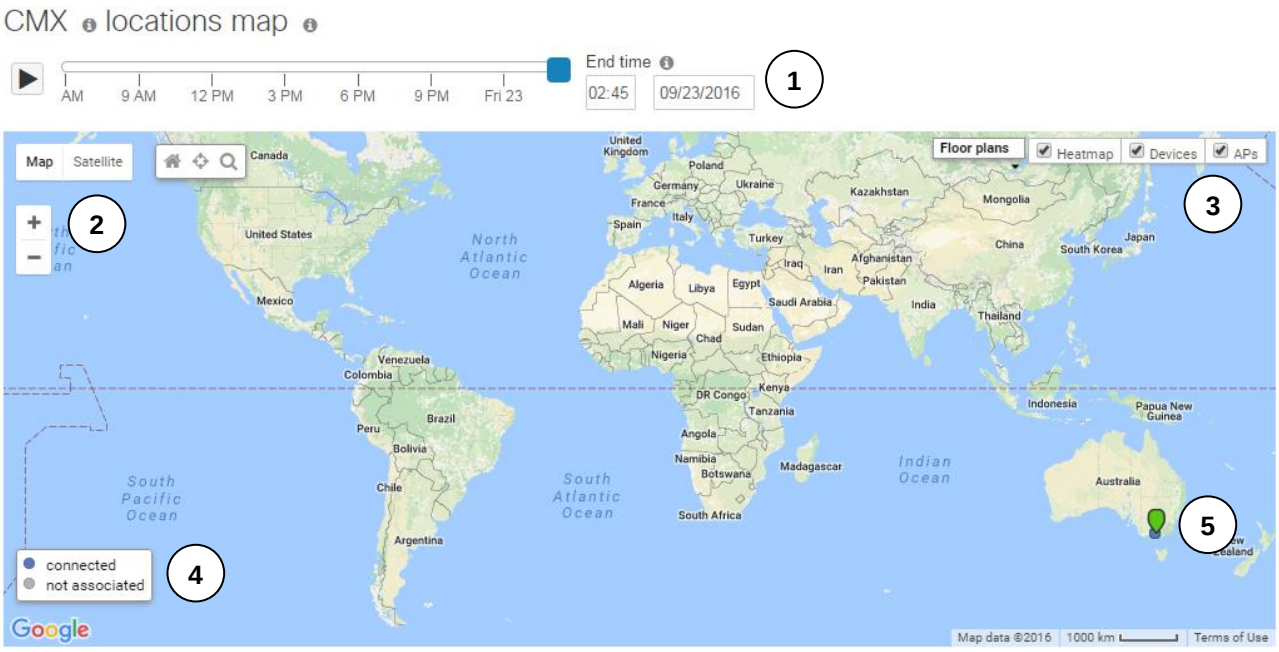



*Figure 27 – Locations Heatmap default view*

1. **Time Filter** – change the time period from which the data is taken by moving the blue marker, or view the connection over time as an animation, by selecting the play button. End times can be adjusted by clicking on the input box and selecting an option. The start time can be changed by moving the blue marker; otherwise, it will start at the beginning.
2. **Google Maps map options**
3. **Show/Hide** the **Heatmap**, **Devices (clients)**, and/or **Access Points**
4. **Device Key** – blue denotes a connected device, and grey denotes a disconnected device
5. **Access Point** marker

Zooming in to a point (or multiple points) result in the following:


*Figure 28 - Access Point and Device Location Heatmap*

For more information, hover over the information icons and follow the links.

# CHAPTER 7
# SUMMARY REPORT

The summary report gives a complete overview of the current network and includes information about the traffic and its details, top APs (usage, model), SSIDs, clients (usage, number) and OS.

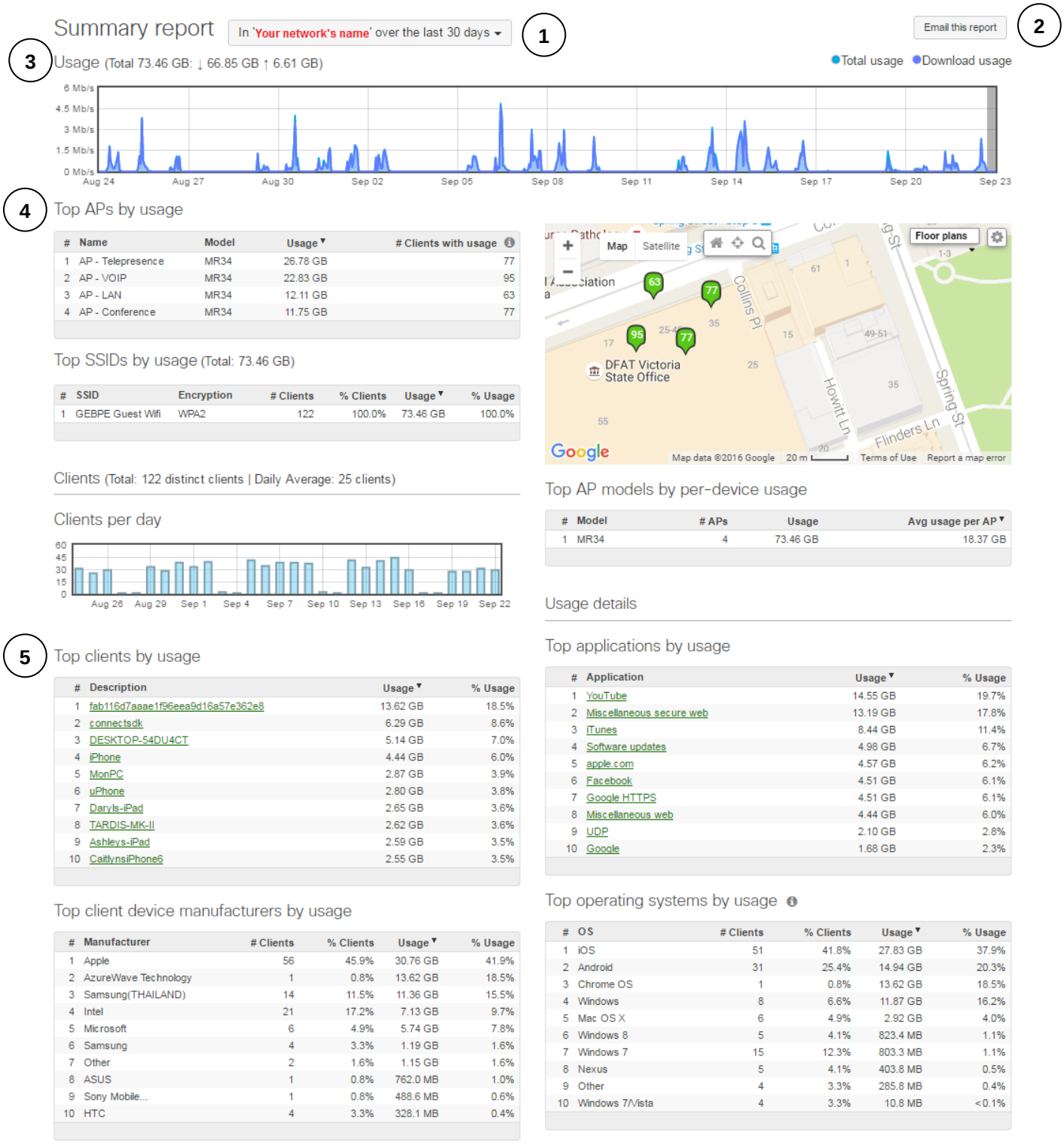



*Figure 29 – Summary Report for your network*

Reports can also be tailored based on the following options:

1. **Time & Device type Filters** – change the data displayed on the page by:
   - **Device type** – on that particular network, or networks tagged with a specific tag
   - **Number of devices shown**
   - **Number of results per table** – either 1, 5, 10, 20 or 50
   - **Time period** – over the last day, week, month (30 days) or over a custom range (*from* `date` *to* `date`)

   The report **will not** update unless the Update button is clicked.
2. **Email report**
3. The **traffic** graph for all the traffic in the network with the filters applied. numerical value of the **total traffic** is shown at the top right-hand side, separated into ↓ **download** and ↑ **uploaded** values in brackets. The graph also displays the download usage ● over the total usage ●.
4. Midsection Results – depends on the filtered device type in the report. All tables can be sorted ▲▼ and all maps have the usual Google Map map options.The above figure shows the results for applications and wireless devices, and is the default screen. Below is the alternate screen for ports:

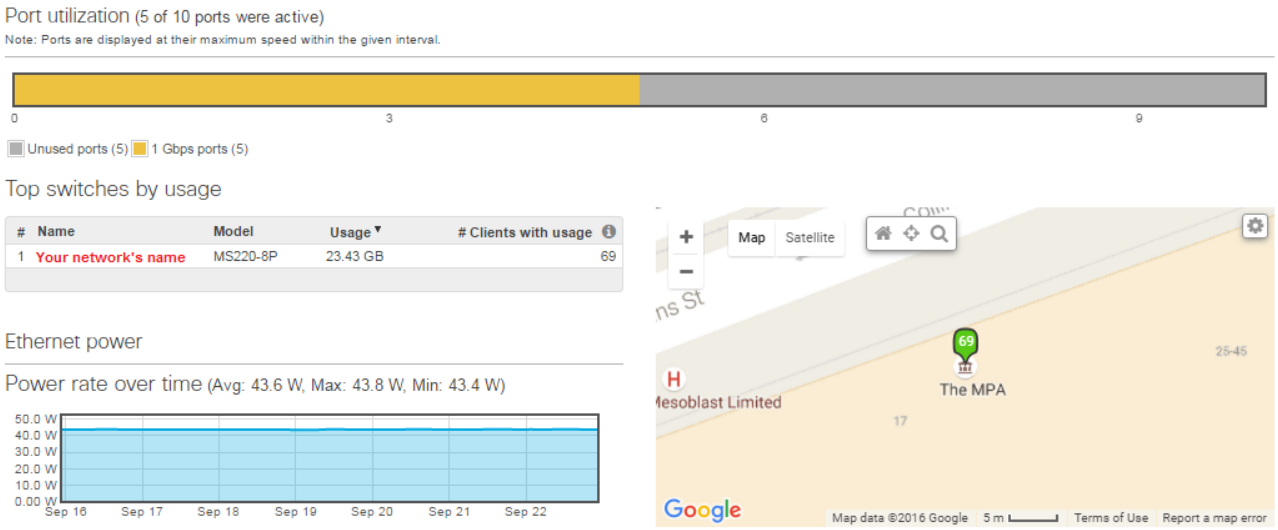



*Figure 30 – Summary Report Midsection for ports*

5. **Top clients and applications by usage** – All tables can be sorted ▲▼ by columns

For more information, hover over the ⓘ icon and follow the links.

# CHAPTER 8
# GUEST AMBASSADOR

The Managed Wi-Fi Cloud dashboard enables you to quickly and easily get guests online, and at the same time, control who is on your network. With Monitor Role acces to the Managed Wi-Fi Cloud dashboard you can create “guest ambassadors”. A guest ambassador can create guest user accounts but cannot otherwise modify the system. A guest ambassador can create guest users for specific wireless SSIDs.

A guest ambassador who logs into the Managed Wi-Fi Cloud dashboard can access the “Guest Management Dashboard”, which only allows the creation of user accounts on SSIDs that are configured to use the Managed Wi-Fi Cloud hosted authentication server. The guest ambassador can add, edit, and remove user accounts, and can specify expiration times for user accounts (e.g. to expire in one day).

## 8.1 CREATING GUEST USERS

Choose the SSID (network) name that you would like to add the user to by selecting the correct option in the “SSID” box at the top left-hand side of the page.

Select “Add new user” from the right-hand side of the page and enter the required details:

1. **Name**
2. **Email Address**
3. **Password** – can be entered manually or a random generation
4. **Check the box** to email the details to the guest user
5. **Select “Yes” or “No”** for authorised. If “Yes”, then an expiry time can be set on the account.

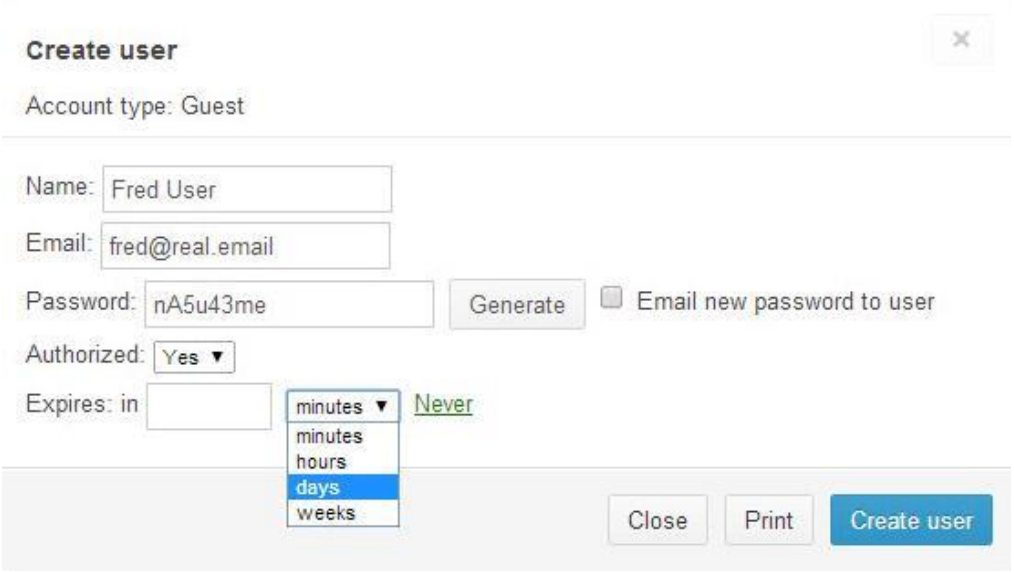



*Figure 31 – Create Guest Ambassador*

Once “Create User” is pressed the new user will be added to the list of current users – this will allow for the details to be verified – if changes are required, selecting the user will open the details for modification. If all details are correct select “Save Changes”

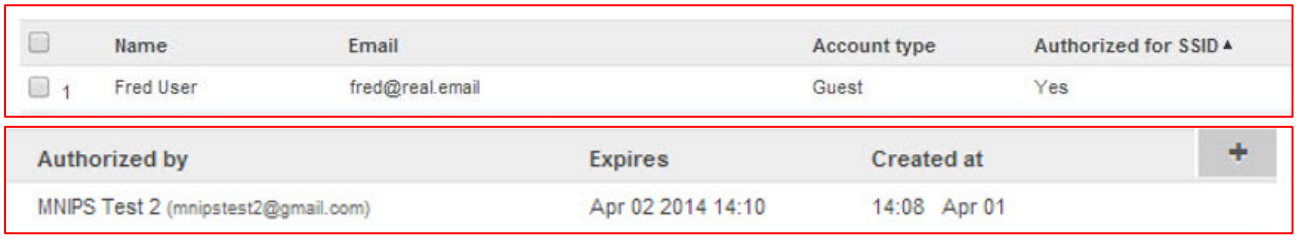



*Figure 32 – Adding and editing User Details*

## 8.2 AUTHORISING USERS

Users can be authorised and revoked by using the option on the top left-hand side of the page – select the users to which you want to make changes and then the option required.

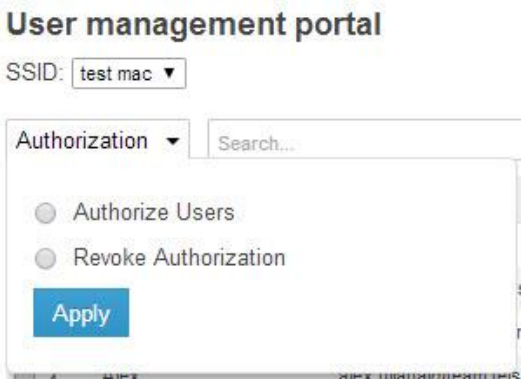



*Figure 33 – User Management*

After making the changes – select “Save Changes” in the yellow bar at the bottom of the screen.

## 8.3 DELETING USERS

Guest Ambassadors cannot delete users from the system – this can only be done by an authorised Administrator – if a user should no longer be active on the system they can be revoked in the **User management portal**, until an authorised person can remove their details from the system.

# CHAPTER 9
# NETWORK-WIDE

This section describes the **Network-Wide** menu item and sub-menu items. This menu may not be available in all access types.

## 9.1 MONITOR > CLIENTS

Please see **Chapter 3 – Clients**.

## 9.2 MONITOR > TRAFFIC ANALYTICS

Please see **Chapter 4 – Traffic Analytics**.

## 9.3 MONITOR > TOPOLOGY

A topology of all devices on this network can be seen here. The more devices there are, the larger the topology diagram will be. The following functions can be carried out:

1. **Expand/Collapse** – the diagram and access points
2. Turn on/off **device labels**
3. **Search** through devices – works in the same way as previously described in **Chapter 2 – Overview > Search** and **Chapter 3.3 – Clients > Client Devices > Search**.
4. Search directly by **online devices** – select ■ x online
5. **Devices & Link information** – hover over the ⓘ icon

Online devices are represented by a green shape ■, and offline as a grey outline shape ◇.

This topology can also be downloaded as an .svg image or printed.

## 9.4 MONITOR > EVENT LOG

Shows list of events, which can be sorted by ‹‹ newer (earlier page), or older ›› (next page). This data be filtered by the given fields, as well as for device type (access points, security appliances, and switches). It can also be downloaded as a .csv file.

## 9.5 MONITOR > SUMMARY REPORT

Please see **Chapter 7 – Summary Report**.

## 9.6 CONFIGURE SUB-MENU

The Configure sub-menu under **Network-Wide** are all in-depth configuration pages. Below is a short description of each page and their function.

| MENU ITEM | BRIEF DESCRIPTION |
|---|---|
| General | General network information, configuration methods and firmware. Customisation options available. |

| | |
|---|---|
| Alerts & administration | Administration and linked accounts, email alerts, and client monitoring options |
| Group policies | View, add, remove and edit group policies linked to this network |
| Users | User database |
| Add devices | Add new Cisco Meraki devices by claiming them and adding them to your network’s inventory |

# CHAPTER 10
# LIVE DATA & DEVICE SUMMARY

The Live Data & Summary for each device can be found, for each individual device, in the following areas:

1. Security > Monitor > Appliance status
2. Switch > Monitor > Switches > Select a switch device (row will be highlighted in yellow, e.g. Your network's name)
3. Switch > Monitor > DHCP servers > Select a switch device
4. Wireless > Monitor > Access points > Select a wireless access point (row will be highlighted in yellow, e.g. Your network's name)
5. Wireless > Monitor > Wireless & floor plans > Hover over an AP, and select the network name
6. Wireless > Monitor > Air Marshal > Map > Hover over an AP, and select the network name
7. Wireless > Monitor > Location heatmap > Hover over an AP, and select the network name


*Figure 34 – Hover-over Access Point network names map (5,6)*

The Live Data & Summary page has the following features in common:

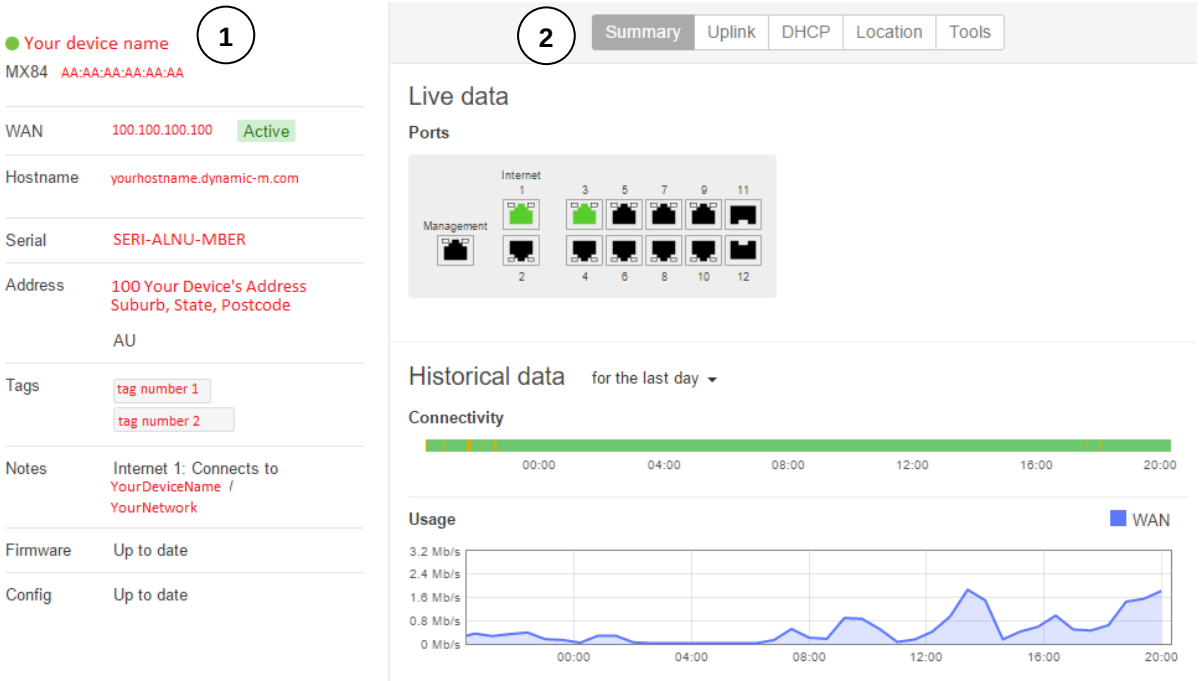



*Figure 35 – Live Data and Summary Page*

1. **Device Details** – shows name, device type/family, MAC, and other details and tags

2. **Summary screen** – shows device ports, historical and live data, and clients, depending on device type, and links to device type specific pages

The **summary screen pages** differ depending on the device type, however the **historical data** under the **Summary page** is present on all three devices types. It displays the overall connectivity of the device, as well as the WAN usage in Mb/s. The time period displayed can be changed to any of the following:

| FILTERS |
| --- |
| 1. **For the last 2 hours**<br>2. **For the last day**<br>3. **For the last week** (7 days)<br>4. **For the last month** (30 days) |

Hovering over a section of connectivity will show the connectivity information for that particular segment, and includes a time and a short explanation if it is disconnected (yellow). If the port is connected, the segment will be green.

Hovering over any part of the Usage graph will show the WAN usage at that point in time.

## 10.1 SWITCH SUMMARY PAGES

<table>
<tr><th>PAGE</th><th>DESCRIPTION & FEATURES</th></tr>
<tr><td>Summary</td><td>Also includes Live data – ports. Hovering over a port will show its connectivity information
<table>
<tr><th>ICON/FEATURE</th><th>DESCRIPTION</th></tr>
<tr><td>Green icon</td><td>Connected port</td></tr>
<tr><td>Black icon</td><td>Disconnected port</td></tr>
<tr><td>  </td><td>Ethernet port</td></tr>
<tr><td>  </td><td>SFP port</td></tr>
</table></td></tr>
<tr><td>Uplink</td><td>Displays information about connectivity and traffic related to the uplink of this device.<br>• Configuration information – shows expanded device/IP information<br>• Live data – Real-time data of current uplink and HTTP traffic for this device<br>○ Hovering over any section of either graph will show the usage at that time<br>○ Play/Pause live data updating<br>• Historical data – Shows the total WAN latency and data loss over the chosen period of time<br>Time period displayed can be changed to any of the following:
<table>
<tr><th>FILTERS</th></tr>
<tr><td>For the last 2 hours</td></tr>
</table></td></tr>
</table>

| | |
|---|---|
| | **For the last day**<br>**For the last week** (7 days)<br>**For the last month** (30 days)<br>○ Destination IP can be changed<br>○ Hovering over any section of either graph will show the usage at that point in time<br>▪ Latency: *x* ms at *time*<br>▪ Loss: *x* % of traffic lost at *time* |
| DHCP | Displays all IP addresses and subnets used by the Dynamic Host Configuration Portal.<br>• DHCP subnets – shows subnets relating to each VLAN<br>○ Can be sorted ▲▼ by each column<br>• All DHCP leases<br>○ Can be sorted ▲▼ by each column<br>○ Text search/filtering by Subnet, VLAN, IP, MAC<br>○ Selecting a client will take you to its client page – please see **Chapter 3 – Clients** for more information.<br>○ Number of results per page can be change<br>○ Previous/next page (and skip page) links |
| Location | Shows location of device on Google Maps display. Selecting the icon or the device name after hovering over will take you back to the summary page. The usual Google Maps options are available. |
| Tools | Tools used to test functionality of device. Tools available:<br>• **Ping** – see if device is still active, or if device can reach a certain website (type website into input box)<br>• **Blink LEDs** – selecting "Run" will start the LED blinking sequence (only useful if device is nearby)<br>• **Throughput** – measure current throughput to ***meraki.com***<br>• **Traceroute** – measure route in IP addresses from a user-input website, over any of the listed uplink ports<br>• **DNS lookup** – domain name system lookup to a user-input website<br>All tools/processes can be rerun ↻ or cancelled/closed × by selecting the relevant icon once it appears. |

## 10.2 SECURITY APPLIANCE SUMMARY PAGES

| PAGE | DESCRIPTION & FEATURES |
|---|---|
| Summary | Also includes:<br>• **Ports & Port configuration** – hovering over a port will show its connectivity information and a short summary<br>○ Selecting a port will take you to the Ports page, with that port already selected |

| ICON/FEATURE | DESCRIPTION |
|---|---|
| Green icon | Connected port |

| | |
|---|---|
| Black icon | Disconnected port |
|  | Ethernet port |
|  | SFP port |
| Blue arrow  | Uplink port, connected, no Power over Ethernet |
| Lightning bolt  | Power over Ethernet |

- **Clients** – on this particular switch
  - Can be sorted ▲▼ by each column
  - Text search/filtering by Subnet, VLAN, IP, MAC
  - Selecting a client will take you to the client page – please see **Chapter 3 – Clients** for more information.
  - Number of results per page can be change
  - Previous/next page (and skip page) links

Uplink

Displays information about the selected port.

- **Main page** (no ports selected) – shows a summary table of all the ports
  - Hovering over a port will show its connectivity information and a short summary
  - Selecting Configure ports on this switch will take you to a table that allows for editing (with write-access only)
  - Hovering over a row will change its colour to yellow, e.g. 
  - Selecting a row will take you to that port
  - Selecting a CDP/LLDP will take you to that device's summary page
- **Individual Port** – click on a port
  - Navigation

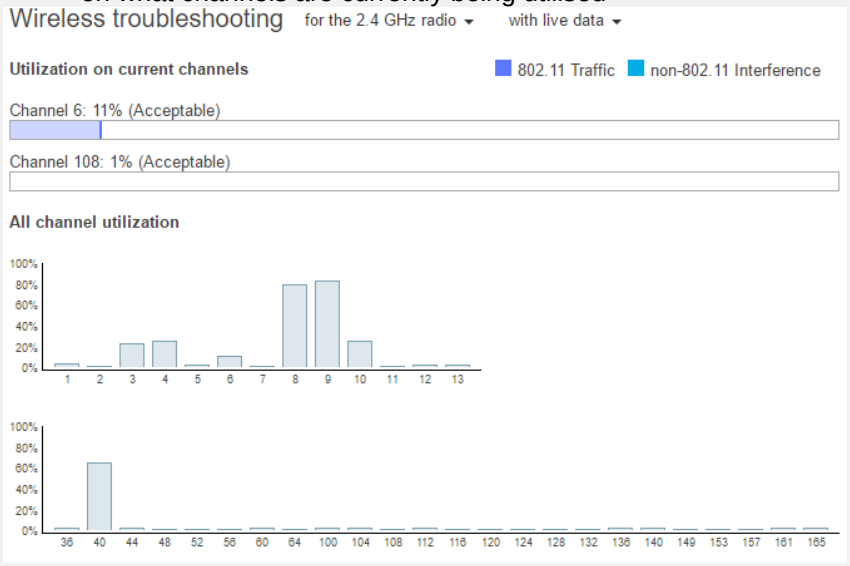
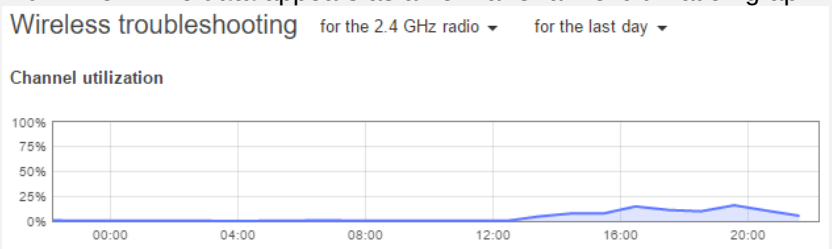
| ICON | FUNCTION |
|---|---|
|  | Go back to Main Ports page |
|  | Go to previously numbered port (will be greyed out if first port) |
|  | Go to next numbered port (will be greyed out if last port) |

  - Current port will be in full colour, other ports will be greyed out
  - **Configuration** – of port
  - Connectivity **Status** of port – includes linked device(s), PoE usage, etc.
  - **Current clients** – number and information about clients currently attached to this device, updating in real time
    1. Selecting the client will you to its client page – please see **Chapter 3 – Clients** for more information.
    2. Pinging a client will take you to the device page tools
  - **Troubleshooting** tests – press ▶ to run troubleshooting function, or select Run a packet capture on this port

| | |
|---|---|
| | ○ **Packet** information – real-time updates |
| Power | Displays Power supply and Power over Ethernet information. |
| Event log | Shows list of events, which can be sorted by **newest**, **newer** (earlier page), or **older** (next page). |
| Location | Shows location of device on Google Maps display. Selecting the icon or the device name after hovering over will take you back to the summary page. The usual Google Maps options are available. |
| Tools | Tools used to test functionality of device. Tools available:<br>• **Ping** – see if device is still active, or if device can reach a certain website (type website into input box)<br>• **Blink LEDs** – selecting "Run" will start the LED blinking sequence (only useful if device is nearby)<br>• **Throughput** – measure current throughput to ***meraki.com***<br>• **Traceroute** – measure route in IP addresses from a user-input website, over any of the listed uplink ports<br>• **DNS lookup** – domain name system lookup to a user-input website<br>All tools/processes can be rerun or cancelled/closed by selecting the relevant icon once it appears. |

## 10.3 WIRELESS SUMMARY PAGES

| PAGE | DESCRIPTION & FEATURES |
|---|---|
| Summary | Also includes:<br>• **Uplink traffic graph** – with total traffic, and downlink ↓, and uplink ↑ in brackets.<br>• **Current clients** – number and information about clients currently attached to this device, updating in real time<br>○ Selecting the client will you to its client page – please see **Chapter 3 – Clients** for more information.<br>○ Pinging a client will take you to the device page tools<br>• **Clients** – on this particular switch<br>○ Can be sorted by each column<br>○ Text search/filtering by Subnet, VLAN, IP, MAC<br>○ Selecting a client will take you to the client page – please see **Chapter 3 – Clients** for more information.<br>○ Number of results per page can be change<br>○ Previous/next page (and skip page) links |
| Event log | Shows list of events, which can be sorted by **newest**, **newer** (earlier page), or **older** (next page). |
| Location | Shows location of device on Google Maps display. Selecting the icon or the device name after hovering over will take you back to the summary page. The usual Google Maps options are available. |
| Tools | Tools used to test functionality of device. Tools available: |

| | |
|---|---|
| | • **Ping** – see if device is still active, or if device can reach a certain website (type website into input box)<br>• **Blink LEDs** – selecting “Run” will start the LED blinking sequence (only useful if device is nearby)<br>• **Throughput** – measure current throughput to ***meraki.com***<br>• **Traceroute** – measure route in IP addresses from a user-input website, over any of the listed uplink ports<br>• **DNS lookup** – domain name system lookup to a user-input website<br>All tools/processes can be rerun or cancelled/closed by selecting the relevant icon once it appears. |
| LAN | Shows VLAN connections and requests.<br>• Filter by VLANs that are tagged with a specific tag, or untagged<br>• Shows number of unanswered requests<br>• Display request type (DNS, DHCP, ARP)<br>  ○ Unanswered requests will also appear on these buttons |
| RF | Shows wireless troubleshooting and channel utilization information in the form of a graph.<br>• Graphs can be filtered by frequency band (2.4GHz, 5GHz) and time period<br>  ○ **Live data** appears differently than other time periods, and shows graphs on what channels are currently being utilised<br>  <br><br>*Figure 36 – Live Data Channel Utilization Graph*<br>  ○ **Non-Live data** appears as a normal Channel ultilization graph<br>  <br><br>*Figure 37 – Non-Live Data Channel Utilization Graph*<br>• **Mesh routes** – used in the selected time period and frequency<br>• **Mesh neighbours** – to this device in the selected time period and frequency |

we

# CHAPTER 11
# SECURITY APPLIANCE

This section describes the **Security Appliance** menu item and sub-menu items. This menu may not be available in all access or network types, and is dependent on the type of devices that you have in your network.

## 11.1 MONITOR > APPLIANCE STATUS

Please see **Chapter 10 – Live Data & Device Summary**.

## 11.2 MONITOR > ROUTE TABLE

This page displays the route table and the status of the subnets that are routed to. Hovering over the icon listed in the Status column will give a description of the status.

## 11.3 CONFIGURE SUB-MENU

The Configure sub-menu under **Security appliance** are all in-depth configuration pages. Below is a short description of each page and their function.

| MENU ITEM | BRIEF DESCRIPTION |
|---|---|
| Addressing & VLANs | Network addressing modes, routing configuration, dynamic DNS and warm spare (redundancy) back-up configuration options |
| DHCP | In-depth VLAN details and configuration |
| Firewall | Layer 3 and Layer 7 Firewall policies/protocols and routing/forwarding rules regarding IP addresses |
| Site-to-site VPN | Off/Hub (Mesh)/Spoke options |
| Client VPN | Enable/Disable |
| Active Directory | Authenticate/Do not authenticate |
| Traffic shaping | Traffic shaping rules and options |
| Access control | Access controls allowed to specified VLAN by an outsider (via Splash page). None, Click-through and Sign-on options available. |
| Splash page | Detailed splash page options. Splash page is only displayed if not disabled in Access control. |
| Wireless concentrator | Teleworker VPN/L3 roaming options |

# CHAPTER 12
# SWITCHES

This section describes the **Switches** menu item and sub-menu items. This menu may not be available in all access or network types, and is dependent on the type of devices that you have in your network.

## 12.1 MONITOR > SWITCHES

Please see **Chapter 10 – Live Data & Device Summary**.

## 12.2 MONITOR > SWITCH PORTS

This page displays the ports on the switch, which may be modified if user has write-access. For more detail, please see Please see **Chapter 10.1 – Live Data & Device Summary > Switches > Ports**.

## 12.3 MONITOR > DHCP SERVERS

This page displays possible options for the DHCP servers. Different servers can be allowed and/or blocked, and the list of servers for a certain time period can be viewed. Email alerts can also be set up.

The table displayed can have its selected time period changed to:

| FILTERS |
| --- |
| 1. **For the last 2 hours**<br>2. **For the last day**<br>3. **For the last week** (7 days)<br>4. **For the last month** (30 days) |

The table can also be selected and sorted ▲▼, and new columns can be added with the + icon. Column orders can be changed by dragging and dropping. The following features are also available:

1. Selecting the device name will take you to the Live Data & Summary – please see **Chapter 10 – Live Data & Device Summary** for more information.
2. View most recent packet
3. Hovering over the status in the Policy column will show the other option allow/block – selecting this will allow/block the policy as specified

## 12.4 CONFIGURE SUB-MENU

The Configure sub-menu under **Switches** are all in-depth configuration pages. Below is a short description of each page and their function.

| MENU ITEM | BRIEF DESCRIPTION |
| --- | --- |
| IPv4 ACL | IPv4 Access Control List allows the addition or removal or any user-defined rules. Dashboard service rules are also available for viewing and cam be sorted ▲▼. |
| Access policies | Access policies for defined devices on this network |

| | |
|---|---|
| Port schedules | Time zone settings for ports |
| Switch settings | Switch management and configuration options, including VLAN, STP, QoS, MTU and port mirroring. |

# CHAPTER 13
# WIRELESS

This section describes the **Wireless** menu item and sub-menu items. This menu may not be available in all access or network types, and is dependent on the type of devices that you have in your network.

## 13.1 MONITOR > ACCESS POINTS

Please see **Chapter 10 – Live Data & Device Summary**.

## 13.2 MONITOR > MAP & FLOOR PLANS

Please see **Chapter 10 – Live Data & Device Summary**.

## 13.3 MONITOR > AIR MARSHAL

Please see **Chapter 10 – Live Data & Device Summary** for map functions.

This page displays a list of “rogue” devices that have connected to your wireless access points. As with all other tables, it can be sorted ▲▼, and columns can be added or removed with the + icon. Column orders can be changed by dragging and dropping.

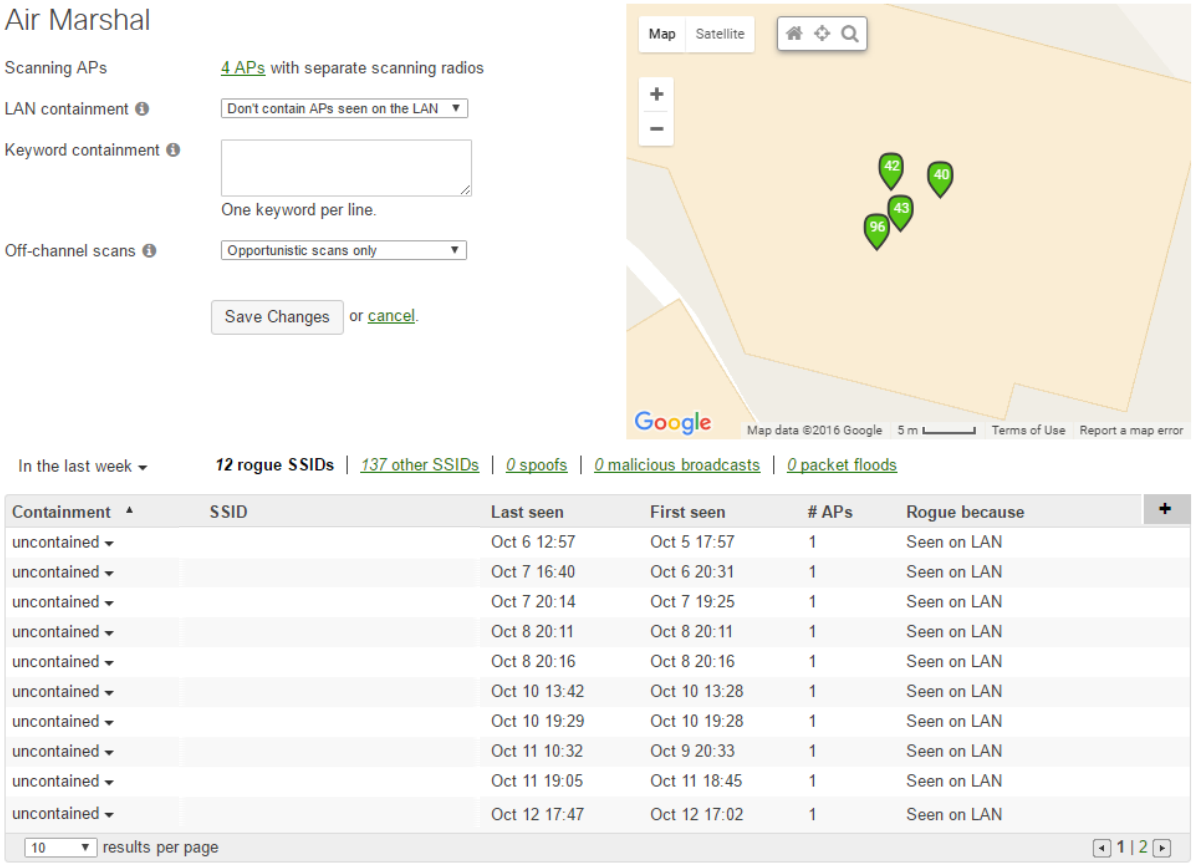



*Figure 38 – Air Marshal page*

## 13.4 MONITOR > LOCATION ANALYTICS

Please see **Chapter 5 – Location Analytics**.

## 13.5 MONITOR > LOCATION HEATMAP

Please see **Chapter 6 – Location Heatmap**.

## 13.6 MONITOR > PCI REPORT

The PCI DSS Wireless LAN Compliance report can be run here. Reports can also be saved and viewed later.

## 13.7 MONITOR > BLUETOOTH CLIENTS

Any connected Bluetooth clients have recently been connected can be found here. The selectable time periods are:

**FILTERS**

1. **For the last two hours**
2. **For the last day**
3. **For the last week** (7 days)

## 13.8 MONITOR > RF SPECTRUM

The frequency spectrum that is used by your Wireless devices can be seen here, as well as the average channel utilisation. The access points can also be searched through by name, and tables sorted ▲ ▼. Either the 2.4GHz or 5GHz spectrum can be selected, and the information displayed will update accordingly.

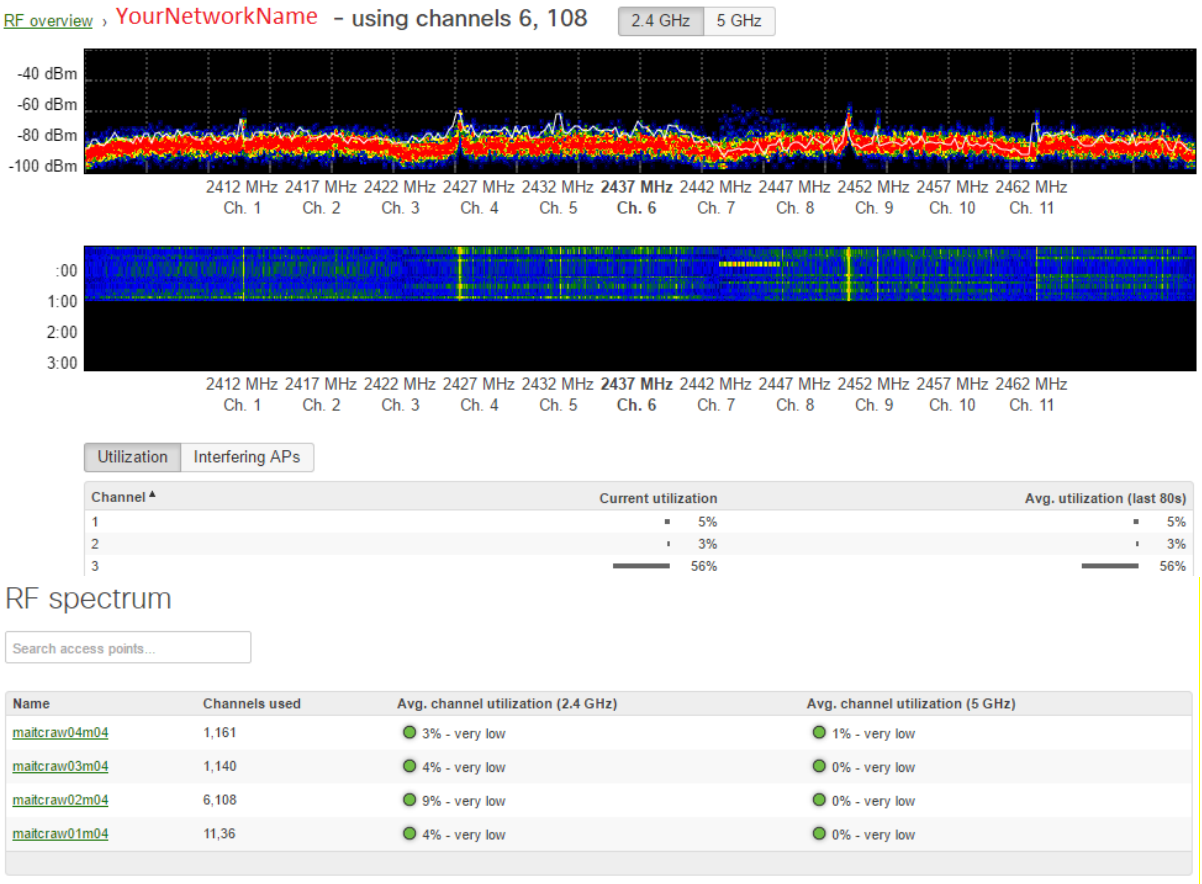



*Figure 39 – RF spectrum usage graphs and tables*

## 13.9 CONFIGURE SUB-MENU

The Configure sub-menu under **Wireless** are all in-depth configuration pages. Below is a short description of each page and their function.

| MENU ITEM | BRIEF DESCRIPTION |
|---|---|
| SSIDs | In-depth SSID information for all access points |
| Access control | Access controls allowed to specified VLAN by an outsider (via Splash page). None, Click-through and Sign-on options available. Normal wireless access point options are also available:<br>• Network access and association/authentication<br>• Addressing and IP management<br>• Frequency spectrum and bitrate |
| Firewall & traffic shaping | Layer 3 and Layer 7 Firewall policies/protocols and routing/forwarding rules regarding IP addresses and traffic shaping rules. |
| Splash page | Detailed splash page options. Splash page is only displayed if not disabled in Access control. |
| SSID availability | Visibility of SSID, and availability of this SSID to each AP |
| Bluetooth settings | Enable/disable advertising and/or scanning functionality |
| Radio settings | In-depth frequency and channel usage and configuration |

# CHAPTER 14
# FREQUENTLY ASKED QUESTIONS

Q. Why can't I see all of the networks associated with my business?

A. *Monitor access can be provided on Managed Wi-Fi Cloud on a per network basis only, not for a complete organisation. To have additional network access provided please log a change request with Telstra.*

Q. Can the Guest Ambassador create users on the correct network?

A. *Guest Ambassador access can be provided on Managed Wi-Fi Cloud on a per-network basis only, not for a complete organisation. To have additional network access provided please log a change request with Telstra.*

Q. Can the Guest Ambassador delete users on a network?

A. *Guest Ambassador access can only create, authorise and de-authorise users – if users need to be removed from the system it needs to be done via a administrator for the network please log a change request with Telstra.*

Q. How do I apply a policy to users on a network?

A. *Policies require specific details to be supplied before being put in place – please log a change request with Telstra.*

Q. I want to add another monitor user or guest ambassador – how do I do this?

A. *Please log a change request with Telstra.*

Q. Can I determine the location of a client?

A. *Selecting the client from the "clients" page will open another window – if you have had a floorplan loaded in the system it will show an approximate location – if you have no floorplan it will show which device the client is connected which may help in determining the location (see Appendix A for device naming).*

Q. Some clients have names under the description others not – why is this?

A. This is dependant on the device type and how it connects to the network – typically Android devices will not display a name whereas Windows and Apple devices will.

# APPENDIX A
# DEVICE NAMING CONVENTION

Telstra's device naming convention is as follows:

**AAABCCCDEEFGG**

| | |
|---|---|
| AAA | Customer network abbreviation |
| B | State the device is located |
| CCC | Site Location of the device |
| D | Type of device |
| EE | Numerical count at this site |
| F | Manufacturer of device |
| GG | Product Code of device |

As an example, below are the details for a fictional router at a fictional company *ABC Company*:

Company: ABC
Device located: Victoria
Site Location: Melbourne Data Centre
Type of Device: Router
Numerical Count at this site: 01
Manufacturer of the Device: Meraki
Product Code: MR32

This device would be named in MDN Online Reporting as **abcvmdcw01m32**. In the below table this device name is expanded to show where each piece of information exists.

| FORMAT | CODE | DETAILS |
|---|---|---|
| AAA | **abc** | ABC Company |
| B | **v** | Victoria |
| CCC | **mdc** | Melbourne Data Centre |
| D | **w** | Wireless device |
| EE | **1** | 01 device at this site |
| F | **M** | Meraki |
| GG | **32** | MR32 |

For support, please contact your Telstra representative or for 24x7 support, call ***1800 815 851***.

IT'S HOW WE CONNECT