FlashStart® cloud

Quickstart **Guide**

English

Rev. 3.3 - April 2017

Welcome to FlashStart !

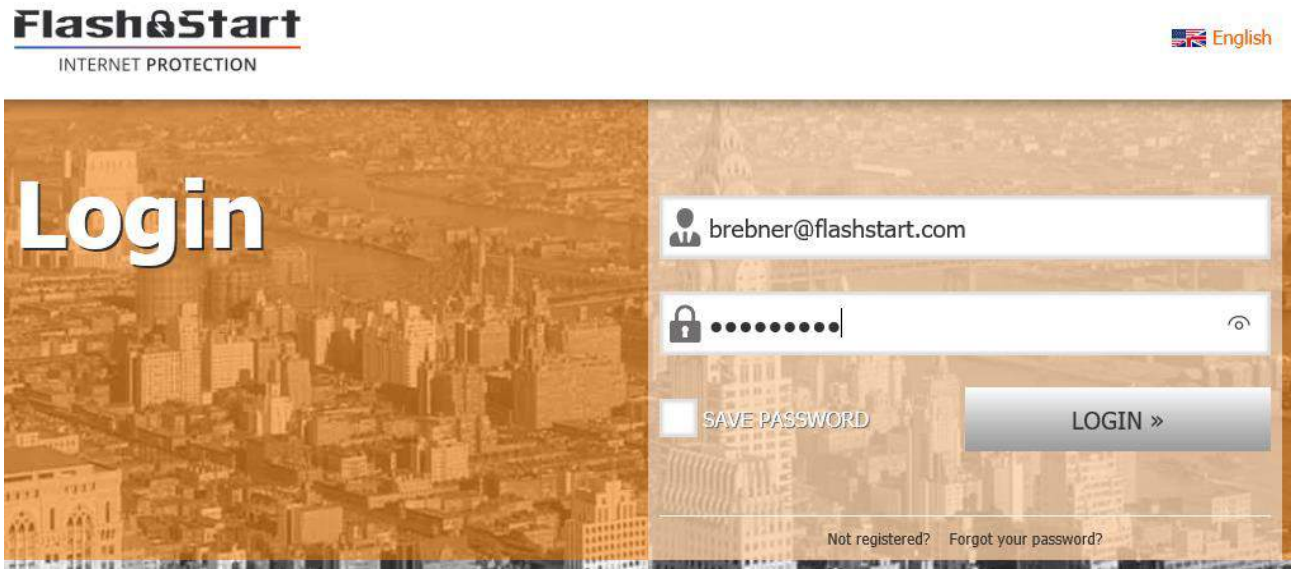
We designed FlashStart to be easy to setup and configure: it should take no more than 15 minutes. This Quick Start Guide takes you through the initial configuration process and explains how to operate the FlashStart 'dashboard'. We hope you find our interface intuitive. If we fall short of your expectations in any way then drop us a line at ‘ can-i-get-this@flashstart.com ’ and we’ll get back to you fast !

Very best wishes

The FlashStart Team

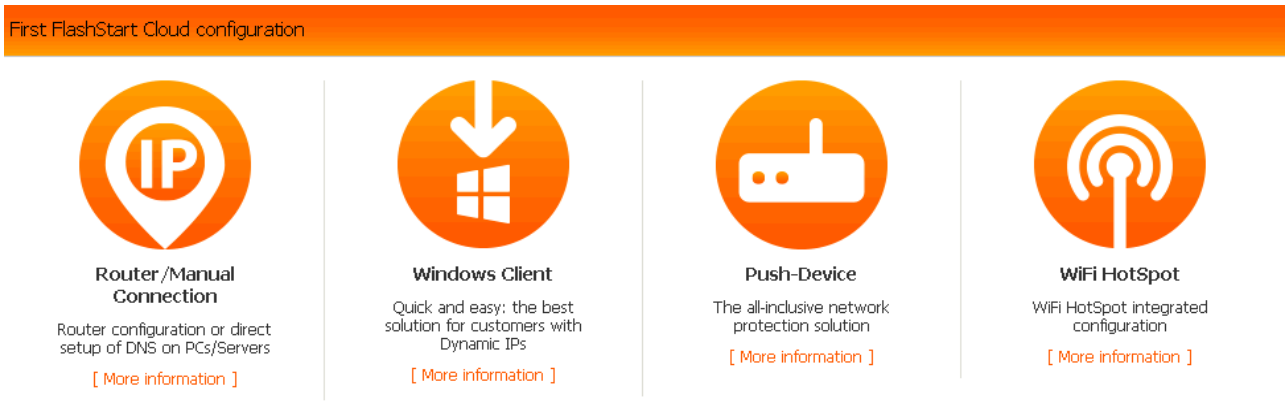
GET LOGGED IN

At the moment **before login** you have the option of selecting your preferred language. Click on it - we currently support German, Italian, French and Spanish, and shortly to be added are Portuguese and Russian.



CONNECT YOUR NETWORK TO THE FLASHSTART CLOUD

Choose one of the following options to quickly integrate your network with the FlashStart Cloud. We will explain more advanced connection options later in the Network section of this guide.



Router / Manual connection:
You can manually configure automatic access to the FlashStart Cloud using static or dynamic IP addressing. To do this, click the icon and follow the set up procedures

Windows Client:
Installing a simple Windows Client is the best option when using a dynamic IP network connection.

Push-Device:
Use this option is you have bought the “all-in-one” bridge option to automatically redirect DNS request to Cloud filtered DNS

WiFi HotSpot:
Use this icon to set up a wifi hotspot. FlashStart is compatible with all access technologies.
You can find example configurations here http://www.flashstart.com/cloud/how-to-activate-flashstart-cloud/router-hotspot-wifi/hotspot-wifi/

After configuration please click on the Tools icon ( ), select "First configuration" and select your **local time zone**.

SECURE64 DNS CONNECTION

Please use the following reserved cloud access points for the trial – you can select either IPv4 or IPv6.

» 45.76.84.187 (IPv4) - 2001:19f0:6c01:25d:f5:3:1:1 (IPv6)
» 188.94.192.215 (IPv4)

DNS access points are available in different countries and regions to guarantee an excellent redundancy and failover.

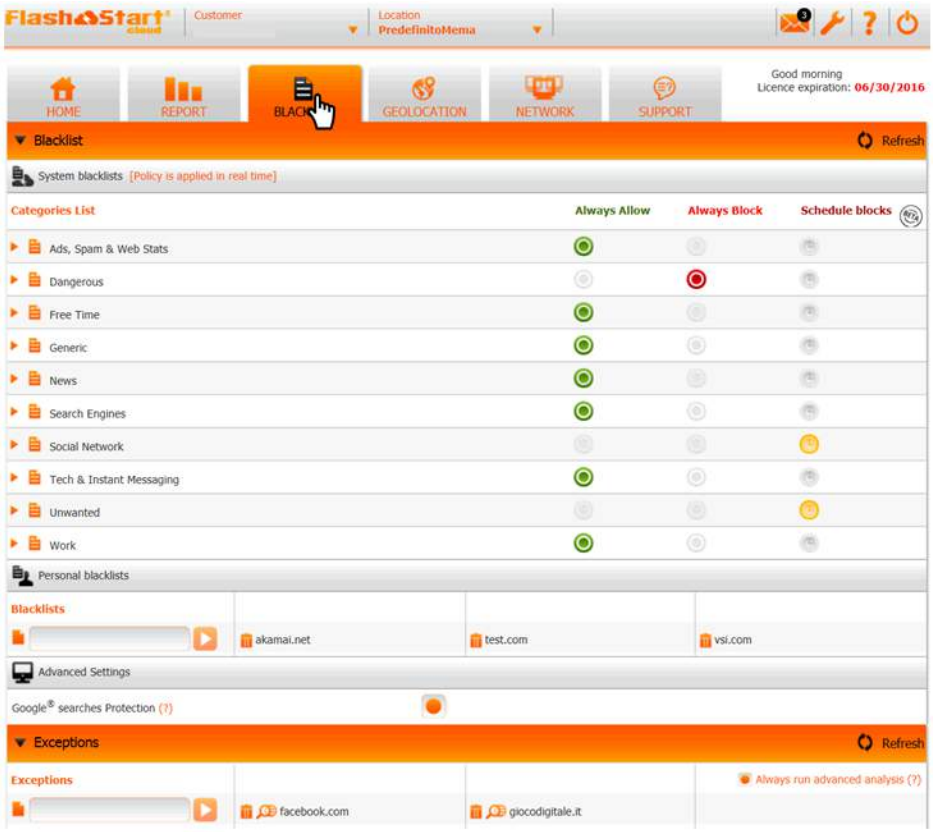
Congratulations - you are now integrated with the FlashStart Cloud.

We’ll now help you to configure FlashStart to help you monitor, block, report and generally create the surfing experience you desire. The best place to start is in the Blacklist tab.

BLACKLISTS

You will immediately see tools to help you with the white-listing and black-listing process. What you will not see are any features to set up **Malware mitigation**. The process of Malware mitigation (protection against Ransomware, Viruses, Botnets etc) is automatic. You can't switch this off, there is nothing to configure, but you can run reports on this (see report section). Don't let this worry you as the sites we are protecting you from are dynamically updated with the very latest threat information.

In the screen shot below you can see 10 macro-categories under the heading 'Category Lists'. There are more than 50 detailed categories and by clicking on the macro-category header (eg 'Ads, Spam, and Web stats) you can see the detailed categories.



» You can allow or block the entire macro-category of specific categories very easily by selecting the 'Always Allow' , 'Always Block' or 'Schedule Blocks' options. It's that simple.

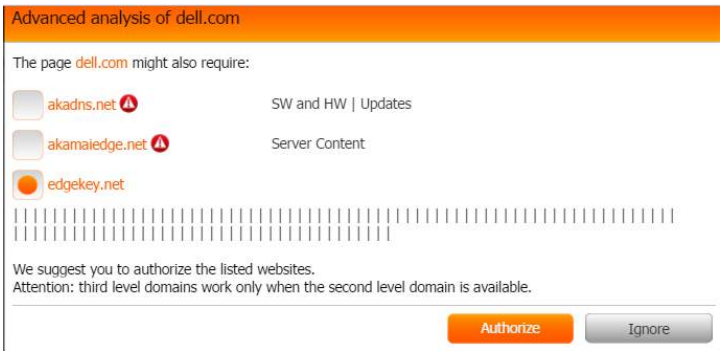
» If you click 'Schedule Blocks' you will see that a calendar appears. You can allow any category or macro-category to be blocked at certain times of day, or days of the week. It's intended to provide access to fun things during break times or even to permit entirely different policies to be run at different times of the day (e.g. a school being used for adult education on Tuesday evenings from 7pm – 9pm).

» New sites are always appearing on the Internet. The FlashStart promise for new site monitoring means that any site which you might find new and open to you will be categorized within 24 hours of your visit.

» When a user experiences a block he/she will receive an 'Access Denied' message, like the one below. As you can see, there is also an 'Ask for the unblock' link to request permission to access the blocked web site. The administrator will receive an immediate message to consider any unblock request.

» It is also possible to block specific domains included in allowed categories or - vice versa - to 'permit' specific domains which may be included in a blocked category.

» To block a specific domain, insert it in the text field below the item **"Personal blacklists"**, then press the play button on the right-hand side of the text field you have just filled in. You will also see that FlashStart uses an advanced DNS parsing capability to recommend other blocking actions (e.g. to block dell.com you need also to block akadns.net and others shown below). With this feature you can block all the back-door paths (.com, .net, .de, .es, etc and CDN's). You can enable / disable this feature by ticking the "Always run advanced analysis" box.



» To allow a blocked domain, you have to fill in the text field under "Exceptions List" with the name of the website (WITHOUT the prefixes http/https or www, e.g. facebook.com).

» You can also **enable Google searches** and **images protection**. Turn on Google "Safe Search" to limit search results and avoid pornography and other unwanted content.

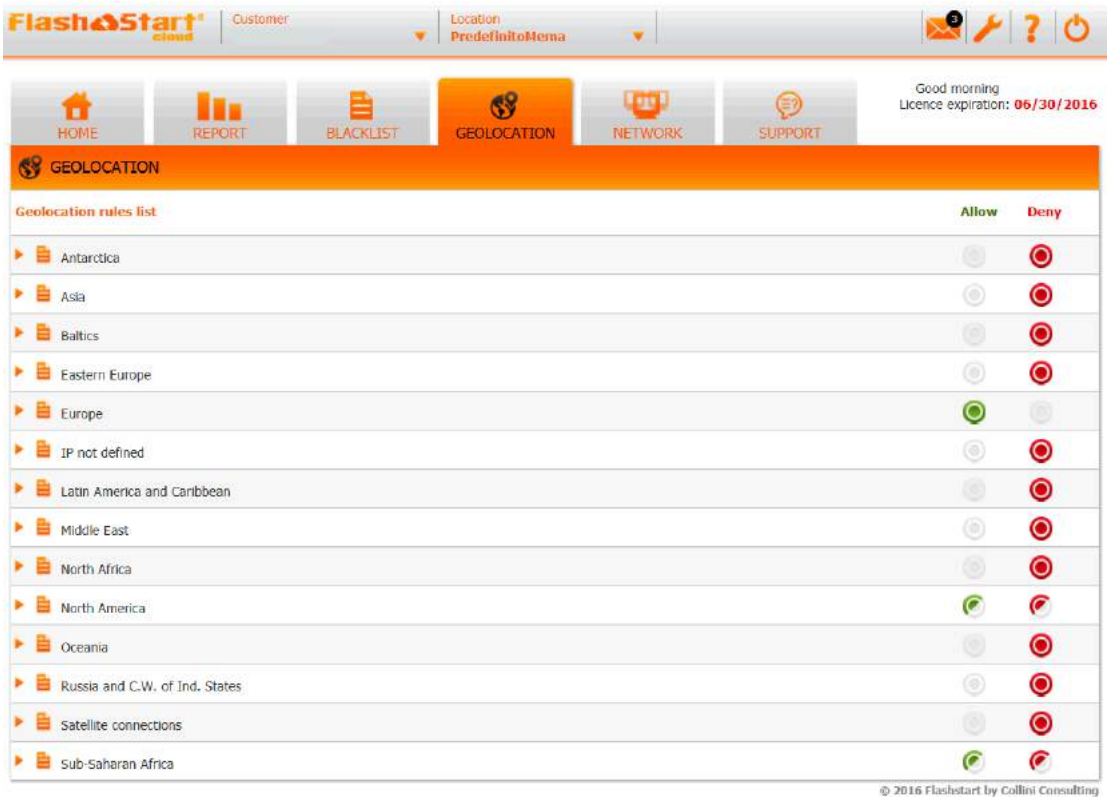
» To enable this option, just select the checkbox on the left-hand side of the item "Google Searches Protection".

When starting out don't over-think what needs to be blocked. Start with blocking the basics, let it run for a few days or a week and then add more rules.

» If you want to know if a **domain is already contained in a blacklist** you can easily find out by using the 'search in lists' feature within the tools drop down menu. See the example below for linkedin.com:

GEOLOCATION

Now select the Geolocation tab. Here you can **block network** connections which originate from a specific country.



» The concept is very similar to that for blacklisting. If you click on any of the macro-regions, a comprehensive list of countries will appear. You just click 'allow' or 'deny' to control access to regions or countries.

As a general rule it's normally a good idea to block any contact with a location identifying itself as "IP Not Defined" or as a "Satellite Connection". These are both widely used for 'bad stuff'.

You can introduce Geo access rules as required, but remember that many technical support centres are based in parts of Asia.

REPORT

As you might expect, this is the part of the dashboard where you can set up reports.

If you click on the drop-down menu on the left, you can select which kind of requests you want to report on.
The main choices are:

» Blocked/allowed requests **by category**: shows blocked/allowed requests to websites by category (Detail)
» Blocked/allowed requests **by macro-category**: shows blocked/allowed requests at a summary level
» Requests grouped **by time slot**: shows the volume of DNS requests over hours in the day (hour trending)
» Requests grouped **by day**: shows the volume of DNS requests over a period of time
» **Blocked undesired requests**: shows attempts to access blocked websites
» **Dangerous requests transited**: shows accesses to unblocked websites which might be considered dangerous
» **Allowed geolocation** requests: shows a world map with the number of requests grouped by geographic area
» **Blocked malware** and threats: shows the number of malware and threats blocked by FlashStart
» **Blocked websites**: shows the blocked websites with the highest number of access attempts.

Scheduling Reports

To create a regular automatic email report click the 'schedule report' button 

» The various drop-down menus allow you to set up email, select reports, intervals (up to 6 months of data), time window for the report (eg 9am – 5pm) and day when the report is sent out.

Ad-hoc Reports

The calendar, clock and search buttons give you control over ad-hoc reports:

» Set the date range, set the time window for consideration (eg 9am – 5pm) and the hit the 'search' button.

» **Tick the details box** on the top right hand side and you will be provided with a tabular results format and additional data.

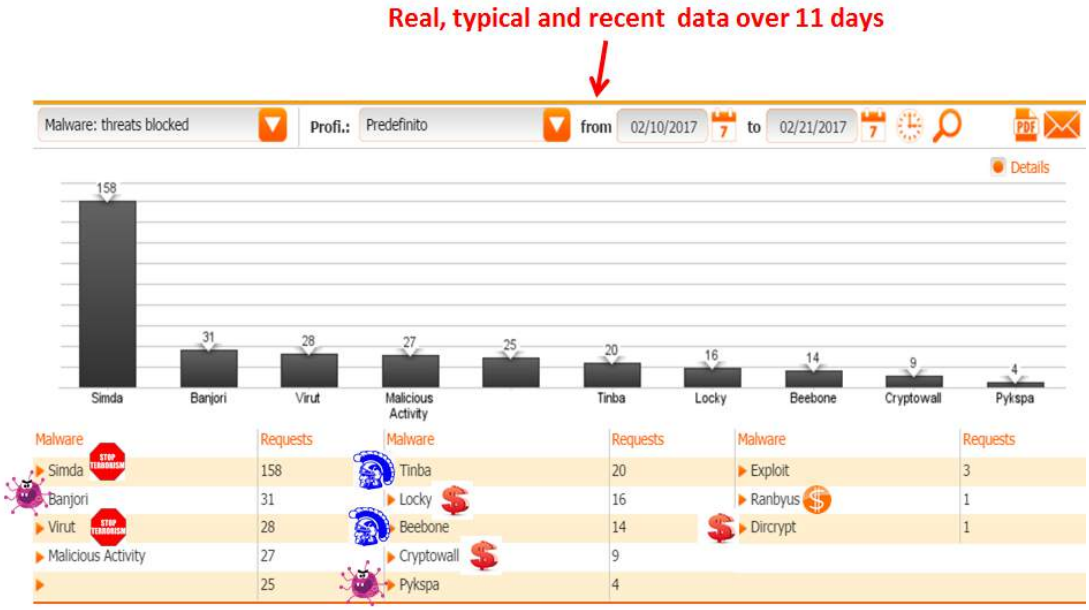
» Create a PDF to **print** the report or send an **email** by selecting the appropriate icons 

If you don't find the report you need – don't panic. Email us here can-I-get-this@flashstart.com

Malware Mitigation

FlashStart has an an advanced, integrated malware filter to protect you from a wide range of threats, including ransomware, botnets, viruses and trojans. This is not an open-source list, but a specialized commercially-sourced real-time feed with a high-quality reputation.

Ransomware is a serious threat for 2017. Such malicious applications will encrypt your data and request payment of money to unencrypt your data. Even if you back-up your data, do consider that some of these ransomware applications immediately download data to help gain fraudulent access to your bank and your customer's bank, steal identity information etc. We recommend creating a malware report regularly looking for peaks in incidents which might suggest more than just a 'normal' risk.



Botnet – uses a device, unknown to the user, for a cyber attack
Virus – infects the device for malicious reasons
Trojan – Remain dormant for a while, malicious attack follows
Ransomware – will steal data and demand a ransom
Payment System – specialist theft malware targeting payment applications

Regulatory and Industry Body Compliance

FlashStart will also filter according to various national and regional regulatory and industry standards. These are all automatically enabled and include compliancy with many national school regulations, anti-terrorism feeds and privacy compliance considerations. If you need the latest information then please contact support@flashstart.com and mention your country and what you require.

NETWORK

In this section the three types of possible connection: push device, static and dynamic ip networks are all reviewed.

» In some situations a customer requests FlashStart to supply a **Push Device** which is a small hardware bridge acting as a "DNS mandatory redirector". If you have not requested this, then please ignore these comments. The function of the Push Device is to re-route DNS queries to the FlashStart Cloud filtered DNS. Using a Push Device, there is no need to change the DNS settings in the existing router or access device. The Push Device is a chargeable option to assist the operations of a network administrator.

Follow the hardware installation guidelines supplied with the Push Device and then open the Network tab.

Push Device Settings

The terms and settings you can see in the above screen shot are explained below:

» Push Device: display unit names. By clicking on the pencil, it is possible to change labels.
» Serial: displays serial factory number of the unit
» Profile: shows configuration profile assigned to the unit
» Status: shows a green dot if the unit is correctly synced with our servers or a red dot otherwise.
» Last sync.: the last time your unit has been synced with our servers.
» IP: the network public IP at a certain moment
» Unfiltered IP: manages internal LAN's PC IPs filter exclusions
» Blocked IP: manages internal LAN's PC IPs blocked (to stop navigation for certain users)
» Advanced: allows the communication port to be changed (53 or 5353). Useful when a LAN is behind a router that acts as a DNS proxy-redirector (such as Vodafone ADSL Station, etc.)
» Wifi: shows and manages Push Device W filtered connection

So now let's configure the Push Device for Static IP or Dynamic IP usage:

» **Static IP** is the simplest to configure;
» **Dynamic IP**: This is the most common connection offered by low-cost access device and router. In this type of configuration, the public IP address issued by the ISP will change from time-to-time;

Static IP Set Up

This section explains the set up for public IPs:

In detail:
» Node: remote Wan IP address filtered by FlashStart Cloud DNS
» Profile: shows configuration profile assigned to the unit
» Status: shows a green dot if the unit is correctly synced with our servers or a red dot otherwise.
» Last login: the last time the IP has been synced with our servers.

Public dynamic IP (DynamicDNS) Set Up
» User: shows username/email address for dynamic DNS synchronization
» Profile: shows configuration profile assigned to the unit
» IP: the network public IP in a certain moment
» Status: shows a green dot if the unit is correctly synced with our servers or a red dot otherwise.
» Last synchronization: the last time the Dynamic DNS credential has been synced with our servers.

Above the Network tab you will also see you two drop-down menus that have not been introduced yet: customer and profile.

» The customer drop-down menu allows different activated networks to be viewed fast and efficiently. This is so-named because many resellers of FlashStart Internet filtering manage multiple end users.

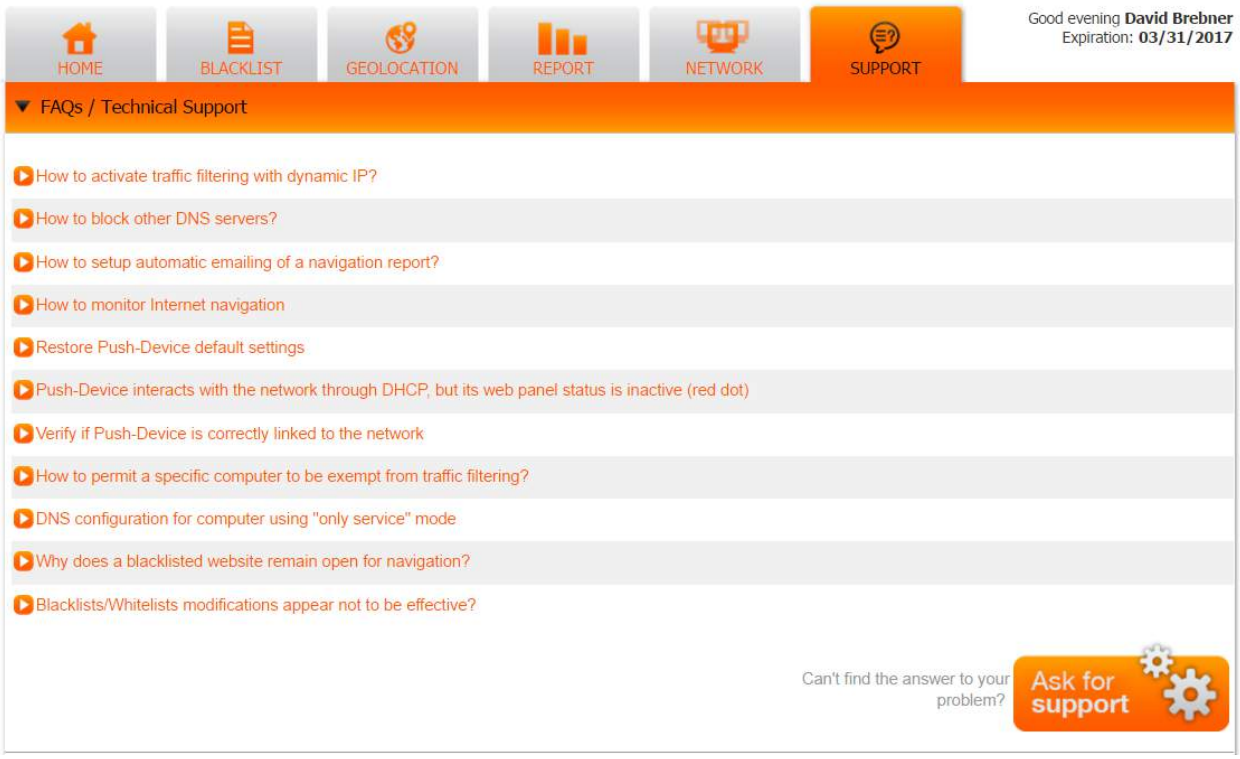
» Profiling is very useful in allowing different user filtering policies to be implemented on the same public IP. This is done using different ports other than the conventional DNS port 53 for to create multiple profiles. As an example: a company wishes to block social network access on its employee LAN but to allow social network access on the Wifi guest network. After creating two profiles (LAN employee and Wifi guests), the administrator should set up Router to forward DNS connection to different DNS ports (53, 110 etc.) according to the querying network.

HOME

The' home' tab is a summary tab and brings together useful reports at a glance.

SUPPORT

Lastly, the 'support' tab:



This panel allows you to **check the FAQs** and to ask for additional support when you require it.

» To read the answer to a specific FAQ, just click on it.

» If you don't find an answer to your problem, or if one of the FAQs is not sufficiently comprehensive, you can click on "Ask for support" to contact us directly. In that case, you just need to describe your problem and you will be contacted back from one of our experts as soon as possible.

» FlashStart use a professional trouble ticketing system. The support capability follows industry best practice and offers a specialized integration lab for access point and router manufacturers.