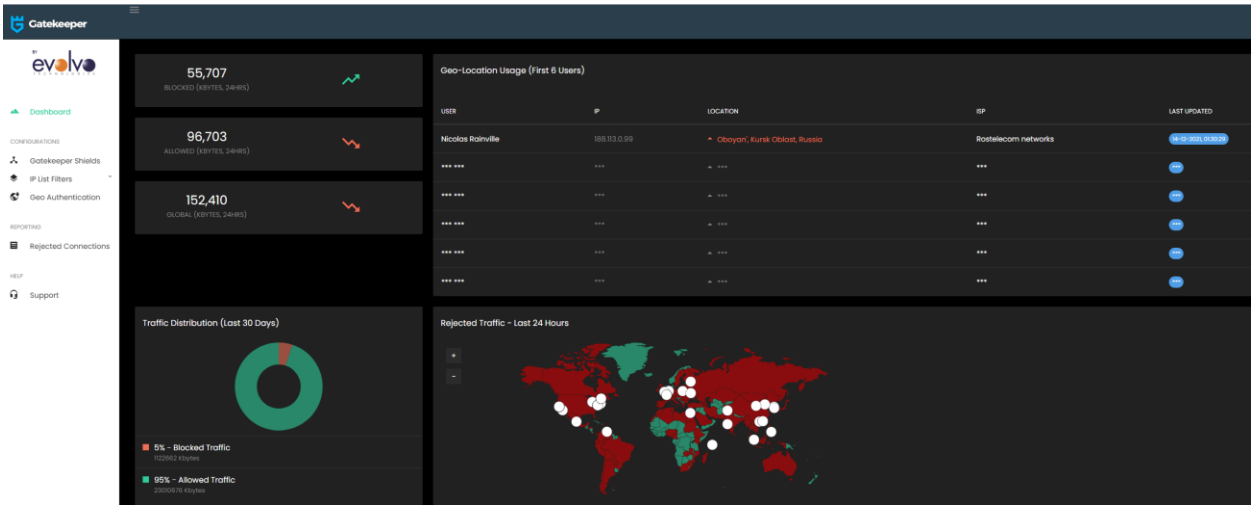
Gatekeeper was designed to help secure online services from attacks by making those services invisible to everyone but the authorized users or IPs. It does this by dynamically maintaining a list of authorized users and IPs and only allowing access to those known users. A new static IP is assigned for each device you need to protect – typically your router or firewall – and all incoming traffic is filtered prior to it ever reaching your routers/firewalls.

For installation instructions, please refer to the Gatekeeper Quick Start Guide.

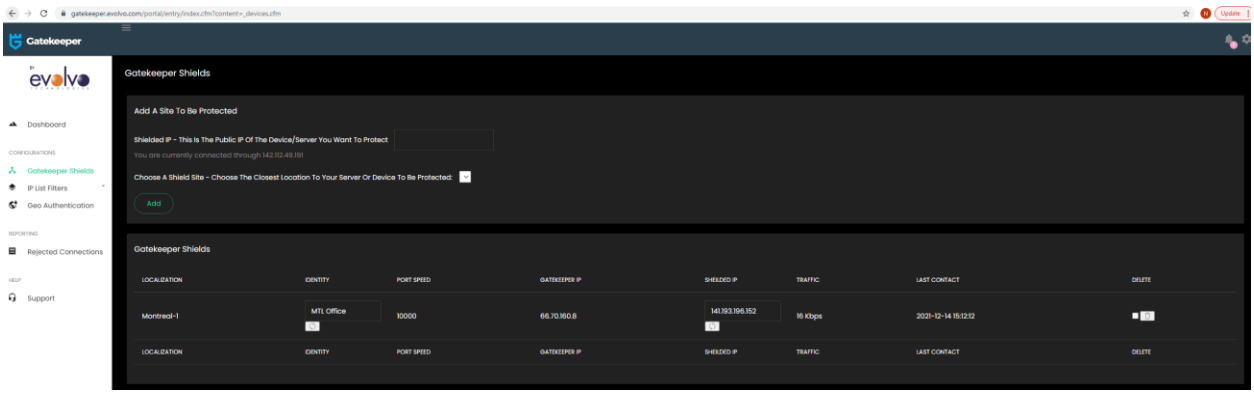
The information included in this guide is designed to help you navigate the Gatekeeper Portal and its various sections to better understand the features and functionalities of the service.

Dashboard



- The Blocked Attempts widget shows the number of packets that tried to communicate to protected services and were rejected in the last 24 hours. Typically, you will see this counter start out high and go down rapidly as the bots give up on trying to connect to a service they previously knew existed.
- The Allowed Traffic widget represents packets that are allowed through in the last 24 hours and that are on either the Private or Geolocated whitelists. This is traffic that you specifically allowed in.
- The Global Traffic widget shows the total number of packets on their way to your router/firewall in the last 24 hours.
- The Traffic Distribution widget breaks down the type of traffic going through the Gatekeeper device in the last 30 days. More specifically, the percentages of each. Here, you can view the packets that are being blocked and the traffic allowed through.
- The Geolocation Usage section shows a quick table of the last connection information from your first 6 users. The complete list can be viewed through the IP List Filters / Geolocated Whitelist pane. Entries highlighted in red or yellow denote users that exceeded the predefined range – see Geo Authentication section below for more information.
- The Rejected Traffic map gives a quick overview of your first 100 blocked attempts in the last 24 hours. Detailed data can be examined by accessing the Rejected Connections pane.

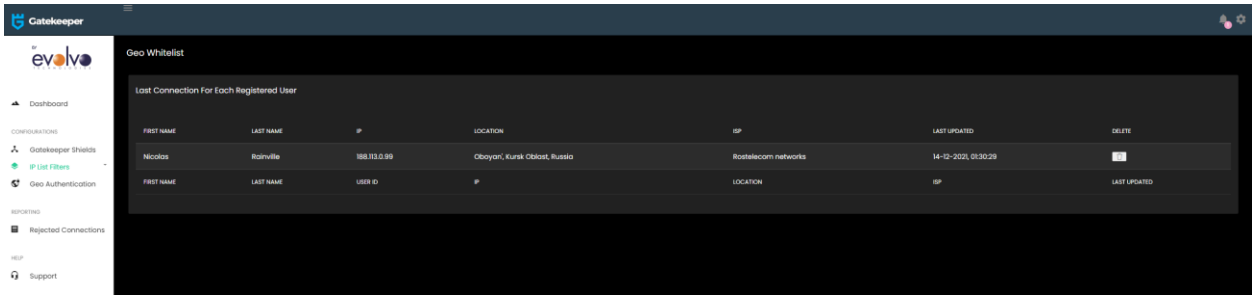
Gatekeeper Shields



- The Gatekeeper Shields page lists the Gatekeeper shields that are currently attached to the account. Each Shield protects one IP address. You may have as many shields as needed, which is particularly useful in cases of a business with multiple offices.
- You may add a shield by simply typing in the IP to be protected, selecting the Shield Type (speed) from the drop-down menu and clicking ADD. If there are entries showing up in the drop-down or you are not seeing the type you need –please contact support for assistance.
- All Gatekeeper shields will be automatically updated with the White List and Geolocated White List information.
- The page lists vital information about the shield, and will populate automatically once it starts reporting back from to the Gatekeeper Servers. If it does not get populated, there is a problem with the Gatekeeper device. Please note that it could take up to 5 minutes for this page to populate once the Gatekeeper Shield is activated for the first time.
- Once the information gets automatically populated, the Identity of an existing shield should be changed to identify it with a friendly name, such as “Main Office” or “Warehouse”. This has no impact on the service itself but is useful in identifying the device. After changing the name, please be sure to click on the associated “Refresh” icon to have the change propagate to the device.
- The IP that a shield is protecting can also be changed from this page. You may not use an IP that was already protected by another shield. After changing the IP, please be sure to click on the associated “Refresh” icon to have the change propagate to the device.
- To delete a shield that is no longer in use, put a checkmark in the Deleted section and click on the related “Garbage” icon.

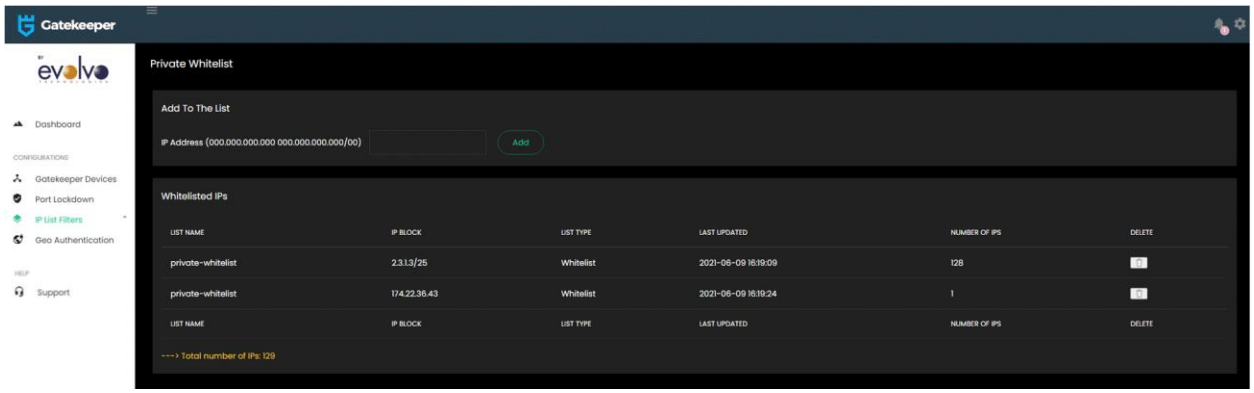
IP List Filters

- Geolocated White List



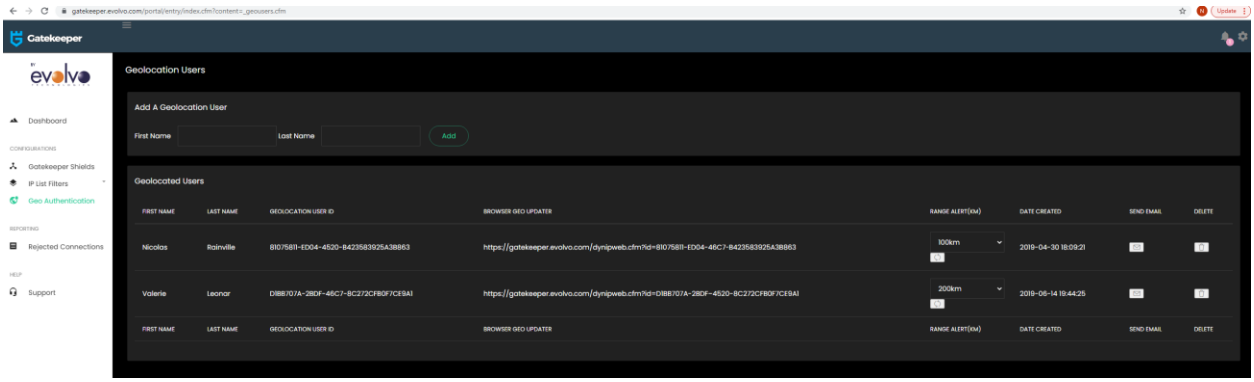
  - The Geolocated White List is a list of IPs that have been authorized either through the Apple/Android apps, the Windows/Apple/Linux service or daemon, or a Web shortcut. This list allows the last IPs authenticated for each user.
  - This list is dynamically maintained, and you may delete an entry if needed by clicking on the related “Garbage” icon.

- White List



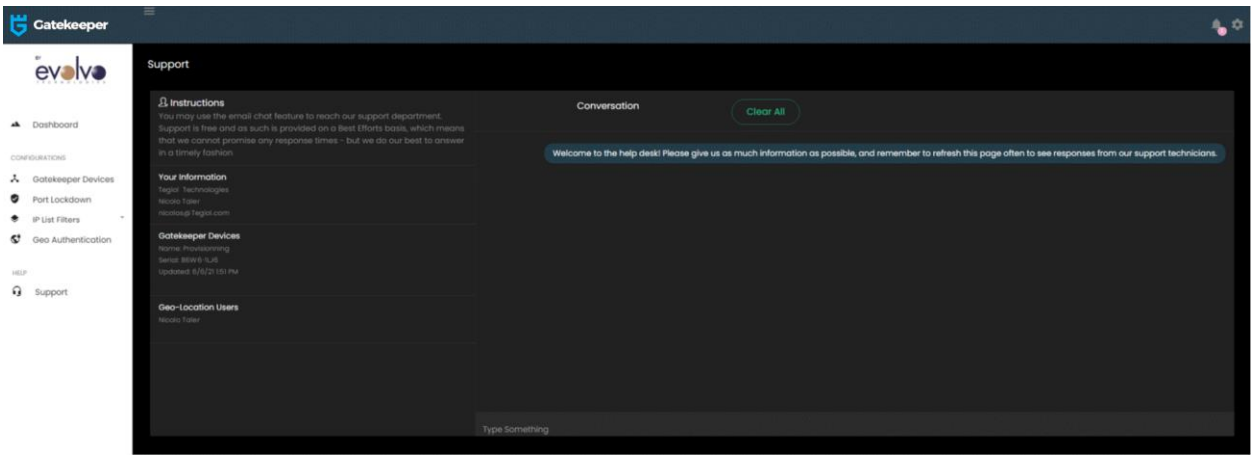
  - The White List performs the same task as the Geolocated White List, but allows IPs to be manually specified. This may come in handy for locations that are known to be safe and for which IPs are static, such as remote offices.
  - It is possible to add a single IP (000.000.000.000) or a subnet (000.000.000.000/00).
  - To delete an entry, click on the related “Garbage” icon.

Geo Authentication



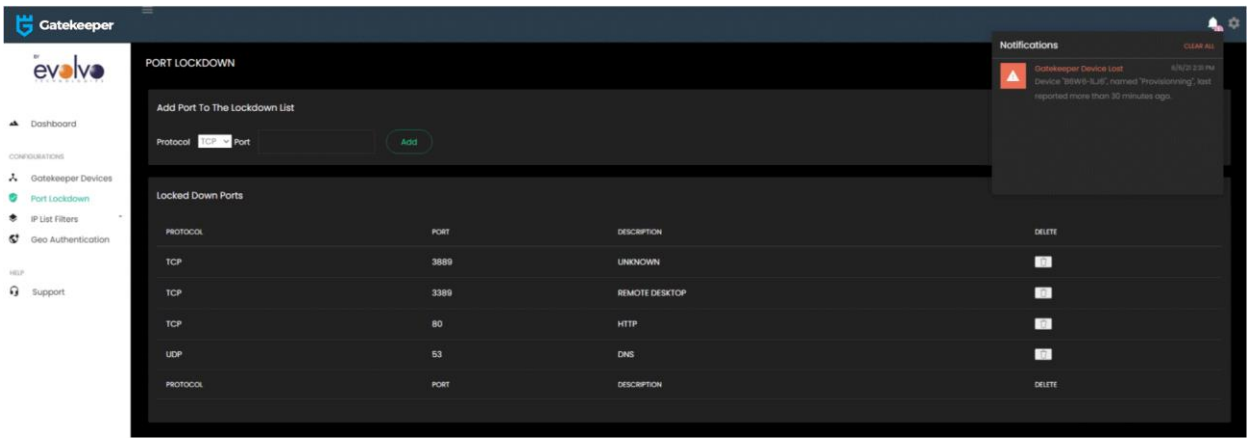
- The Geo Authentication menu item will bring up the list of users that are currently registered and allows you to add additional ones.
- From this page, you will be able to get the User Id needed for the phone/tablet apps, as well as view the web browser links for each registered user.
- It is vitally important that each user has his own ID to prevent one user from overwriting another's IP list.
- Clicking on the Send Email icon associated to a user will send an email to the administrator that can then be forwarded to the end user. It contains information and links for all of the Geo Authentication methods available.
- Clicking on the Delete icon will delete the entry.
- Selecting a range will highlight, in the dashboard, in red or yellow the authenticated user if he connects from a distance exceeding the range defined. Please note that, in the case of an organization having multiple shields, the distance is measured from the first shield. Selecting None will turn the feature off.

Support



- The Support page enables you to open a support ticket. While it is also possible to just email support@evolvo.com, going through the portal provides the support technician with much more information automatically, so you are more likely to get a faster resolution to your issue or question.
- To use the support feature of the portal, simply type in comments or questions in the bottom right box entitled “Type Something”.
- The request will be redirected to a technician, who will answer you as quickly as possible.

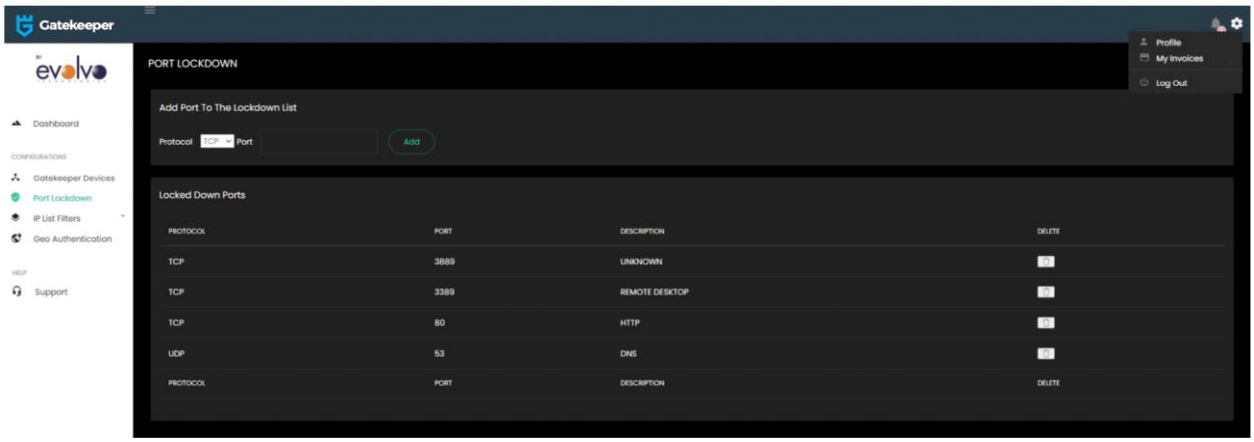
Notifications



The notifications menu can be accessed by clicking on the bell icon at the top right of your screen.

- The small number near the bell icon specifies how many messages are waiting for you.
- Clicking on the bell icon will list all messages.
- Clicking on Clear All will delete all messages.

Settings



The settings menu can be accessed by clicking on the gear icon in the top right of your screen.

- Profile
    - The Profile screen will allow you to edit your profile and the organization and billing information, as well as change your password.
    - Terms and Conditions are also available through that page.

- My Invoices
    - From the My Invoices page, you will be able to view invoices by clicking on the invoice numbers on the left.
    - The status of the payments for each invoice is also provided.
    - You may pay invoices by clicking on the “Click Here To Pay Now” link on the right of each invoice. This will bring you to a secure Paypal page where you will be able to pay by credit cards or Paypal.
- Log Out
    - The Log Out button will log your session out and return you to the login page.

Using the Service

Configuring your phone or tablet to automatically add it's public IP to the Geolocated White List

- Install the phone or tablet app from either the Google or Apple App stores, by searching for Evolvo Gatekeeper.
- In the App, in the Settings section, type the User ID corresponding to the user you created earlier. If you have an Android based Phone, it should automatically update each time the IP address changes on your phone. If you have an iPhone, Apple does not allow apps to continuously run in the background, so you will need to start the app and click on the Update button for that IP to become whitelisted. Android phones may also require that same manual procedure if you power management settings prevent apps from running in the background.
- Once the IP has been updated from your phone or tablet, any device or computer connected to the same wifi network will automatically be whitelisted in Gatekeeper.

Configuring a computer to automatically add it's public IP to the Geolocated White List

- If you are using a computer follow the links for the various operating systems (Windows/MacOS, Linux) available in the email sent to the administrator to install the service/daemon on the computer. It will then automatically refresh the IP every 30 seconds.

Other devices

- For any device or computer that can open a web browser, you can use the Browser Geo Updater link found on the Geo Authentication page of the portal at http://gatekeeper.evolvo.com/portal/entry/index.cfm?content=geousers.cfm .

WARNING – Be advised that having two separate devices using the same user id is not recommended, as one device can overwrite the entry from another if they are on different networks (such as on a cellular and wifi). We recommend creating one Geo Authentication user per device, using different names (such as Frederic Mody- Cellular).

Manually Whitelisting an IP

- You may have a situation where you want to whitelist an IP permanently (such as for a remote office). You may do so from the IP List Filters menu by selecting White List and then entering an IP address (000.000.000.000) or subnet (000.000.000.000/00). By efault, all IPs are blocked until specifically whitelisted in either the White List or the Geolocated White List.