Getting Started with the DDoS Mitigation and Reporting Portal

February 2021

Contents

Signing in to the portal

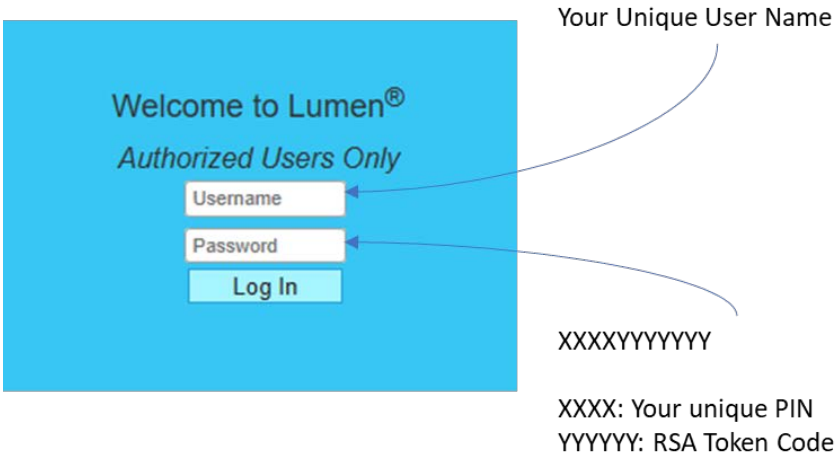
Your DDoS Mitigation service from Lumen, comes with a portal containing an extensive volume of dashboards and reports. Use this guide to acquaint yourself with the information available and how to navigate through the various pages.

When your service was activated, you received an email with instructions on how to activate your portal account. To summarize, you should have access to the following things:

- The link to the service: https://globalview.lumen.com
- Login credentials – established during service activation
- Username
- PIN
- The RSA SecurID app – available from your app store
- A Token for the RSA Secure

Each user will have a unique username and will use an auto-generated token for the password, combined with a PIN that you specify. You will need access to the RSA Token generation app that can be found at your app store.

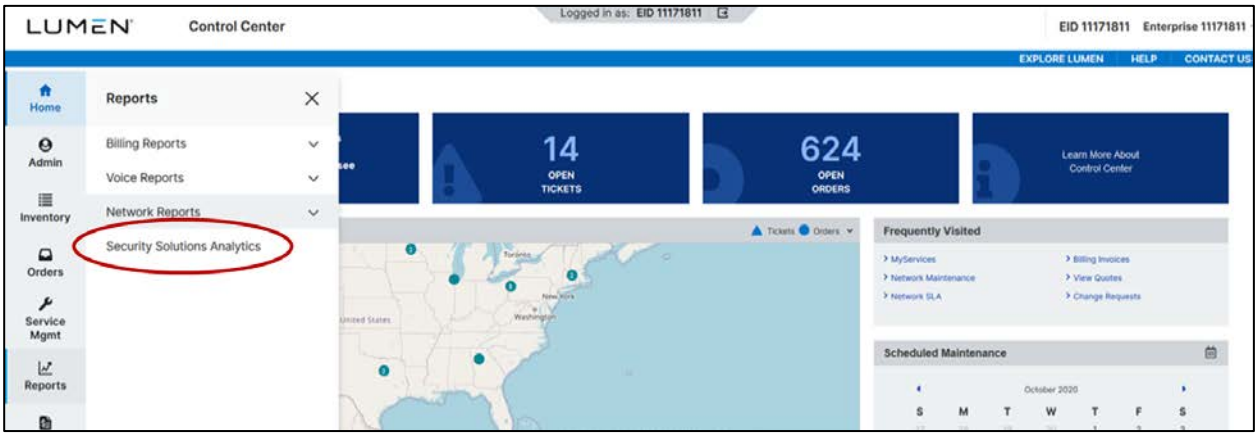
Once you have your Username, PIN and RSA Token app, you are ready to sign in. When you click the portal link you will be provided with the following dialog.



Enter your unique Username in the top box. Your password will be the 4-digit PIN number you have established concatenated with the number generated by the RSA Token app.

Once signed in, you have access to all the DDoS Mitigation portal information that is applicable to your business.

If you are already signed in to Control Center, you can navigate to the DDoS Mitigation portal: click **Reports**, then click **Security Solutions Analytics**.

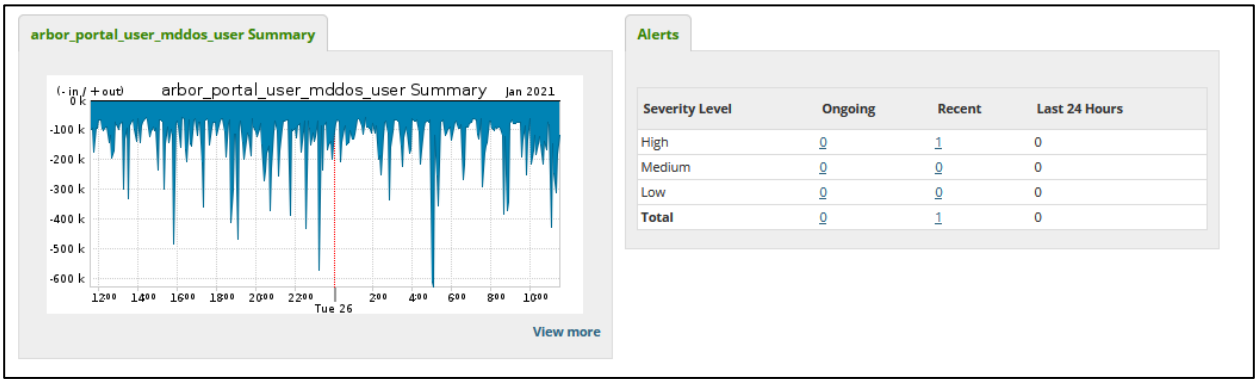


From the Security Solutions Analytics page select “DDoS Mitigation and Reporting” as shown here.

You will need to sign in to the DDoS Mitigation and Reporting portal separately as described above, using your unique username, RSA PIN, and RSA token-generated code.

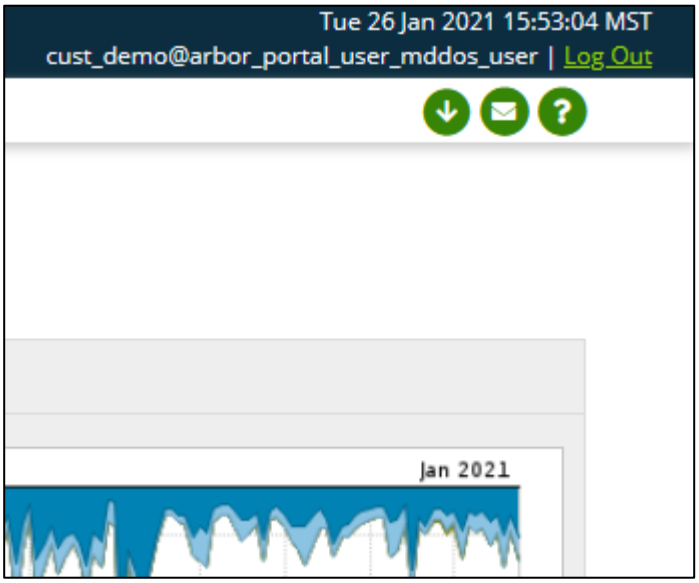
The DDoS Mitigation and Reporting dashboard

The first page presented to the Portal User is the DDoS Mitigation and Reporting dashboard. A snapshot is below.

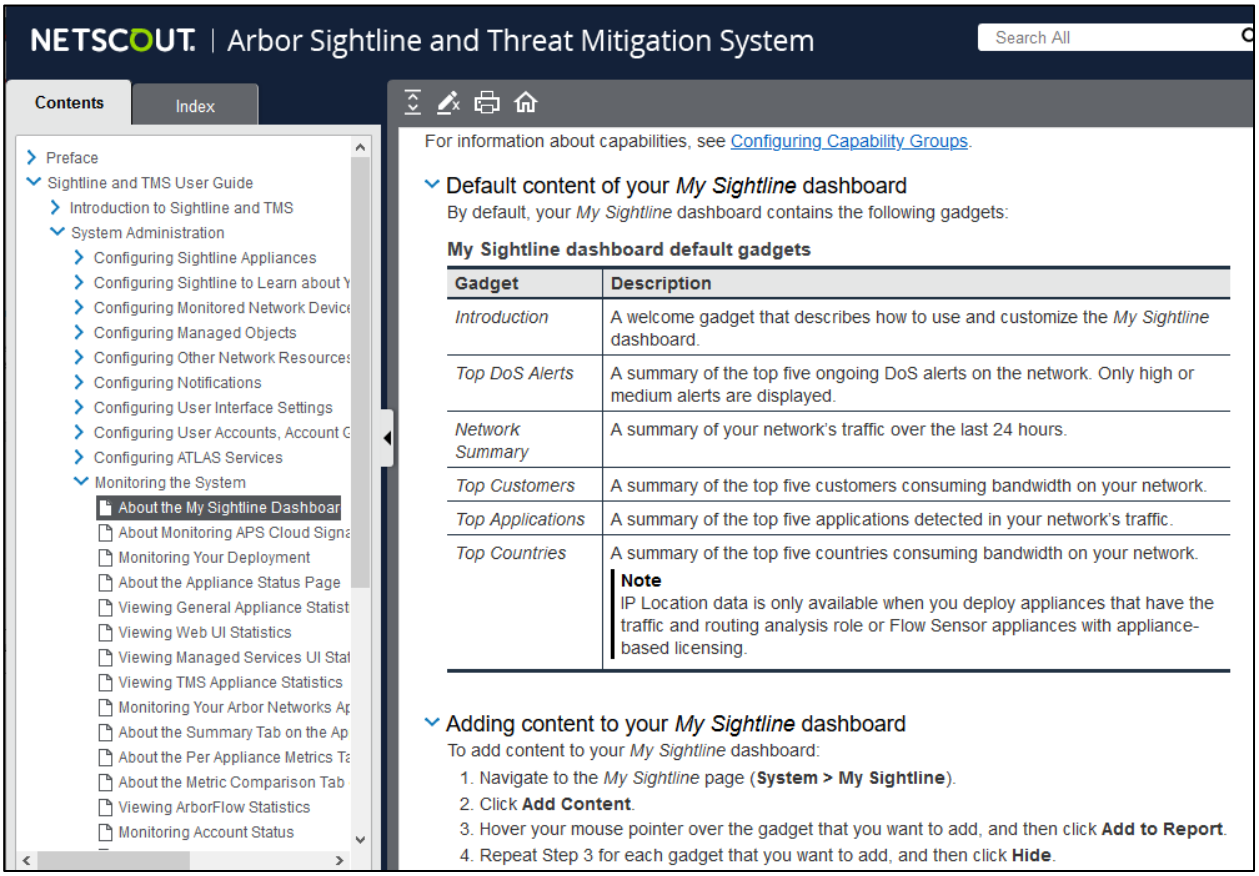


Navigating by means of the top menu bar, portal customers can examine characteristics of their network traffic at any time, independent of DDoS events and alerts. Alerts can be examined through the menu bar, or from the Alerts panel in the Status page.

Traffic into (top) and out of (bottom) of the customer network appears on the left of the Status screen. On the right, a summary of current and recent DDoS alerts is presented in the upper right, note three control icons, illustrated below.



The down-arrow icon is used to download this page to a PDF document. The mail icon us used to mail an image of the page. The question mark icon brings up an extensive on-line manual for the entire portal. This on-line manual is very detailed. Please note that not all features described in the manual are available to you as a user. A snapshot is below.

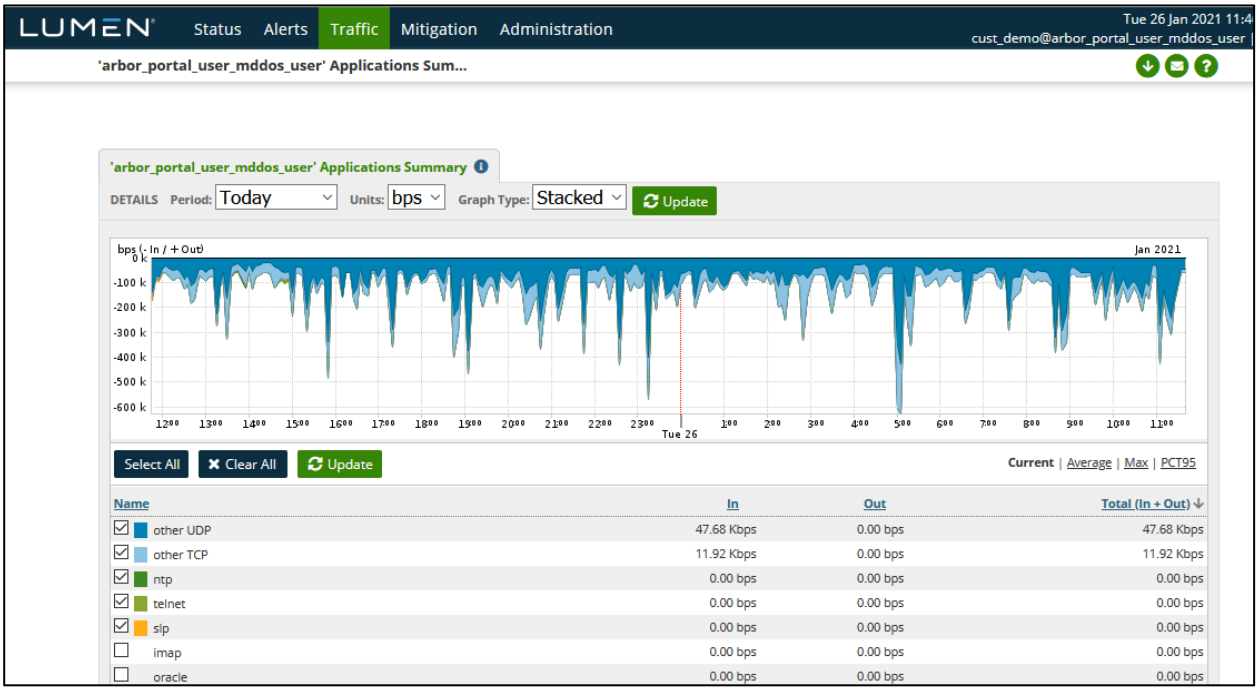


Navigating through the DDoS Mitigation portal

There are a couple of ways to navigate through this portal. Clicking through on clickable gadgets will typically bring the user to specific information on the gadget selected. Using the navigation bar is a quick way to get to specific spot in the portal.

Traffic > Summary > Application

Globalview displays a summary of the traffic, for all monitored networks of the customer, broken down by application.



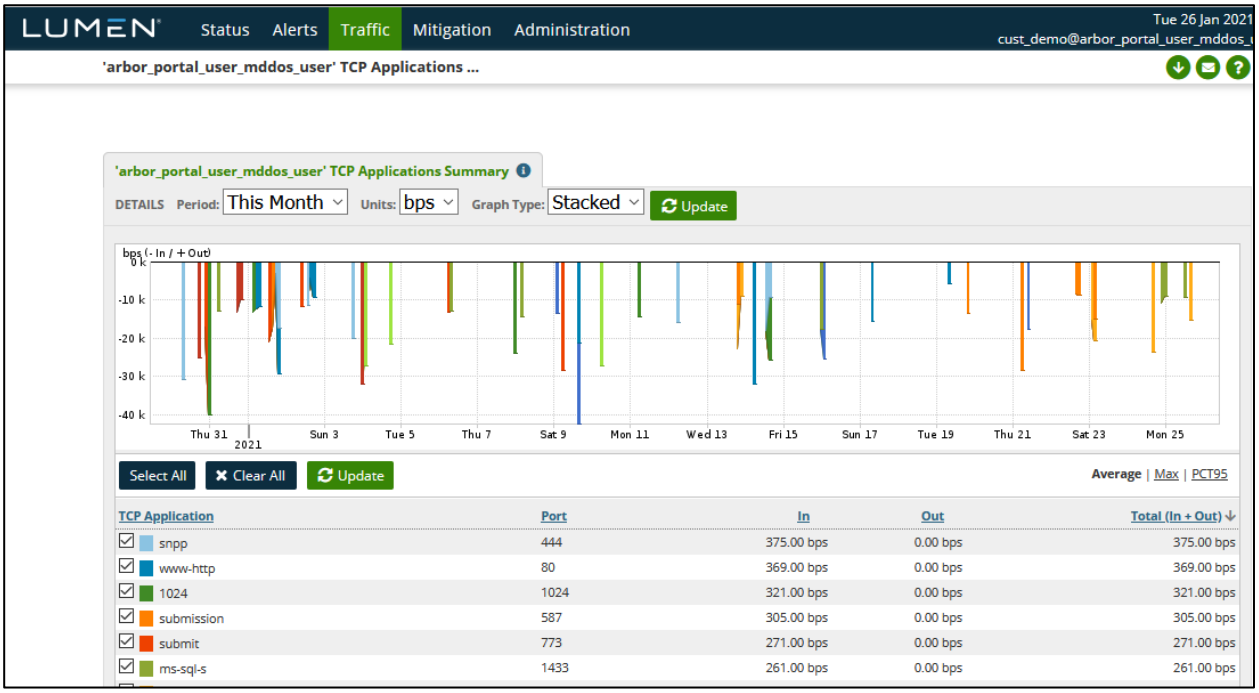
The default period is the previous 24 hours. The period can be changed to various predefined selections or to “other” for a user-defined timeframe. The default display is bits per second (bps) but can be changed to packets per second (pps). Available graph types are Stacked, (default), Pie, and Bar.

The negative values show traffic out of the customer network (“in” to Lumen), and the positive is the traffic into the customer network (“out” of Lumen)

Any selected applications are shown in the graph with a unique color. Any unchecked applications are not represented in the graph. The table can be sorted by clicking on a column header. Click the column header again to reverse the order.

Traffic > Summary > TCP

Very similar to the Applications report, this screen constrains the report to TCP traffic broken down by TCP Port.



The default period is the previous 24 hours. The period can be changed to various predefined selections or to “other” for a user-defined timeframe. The default display is bits per second (bps) but can be changed to packets per second (pps). Available graph types are Stacked (default), Pie, and Bar.

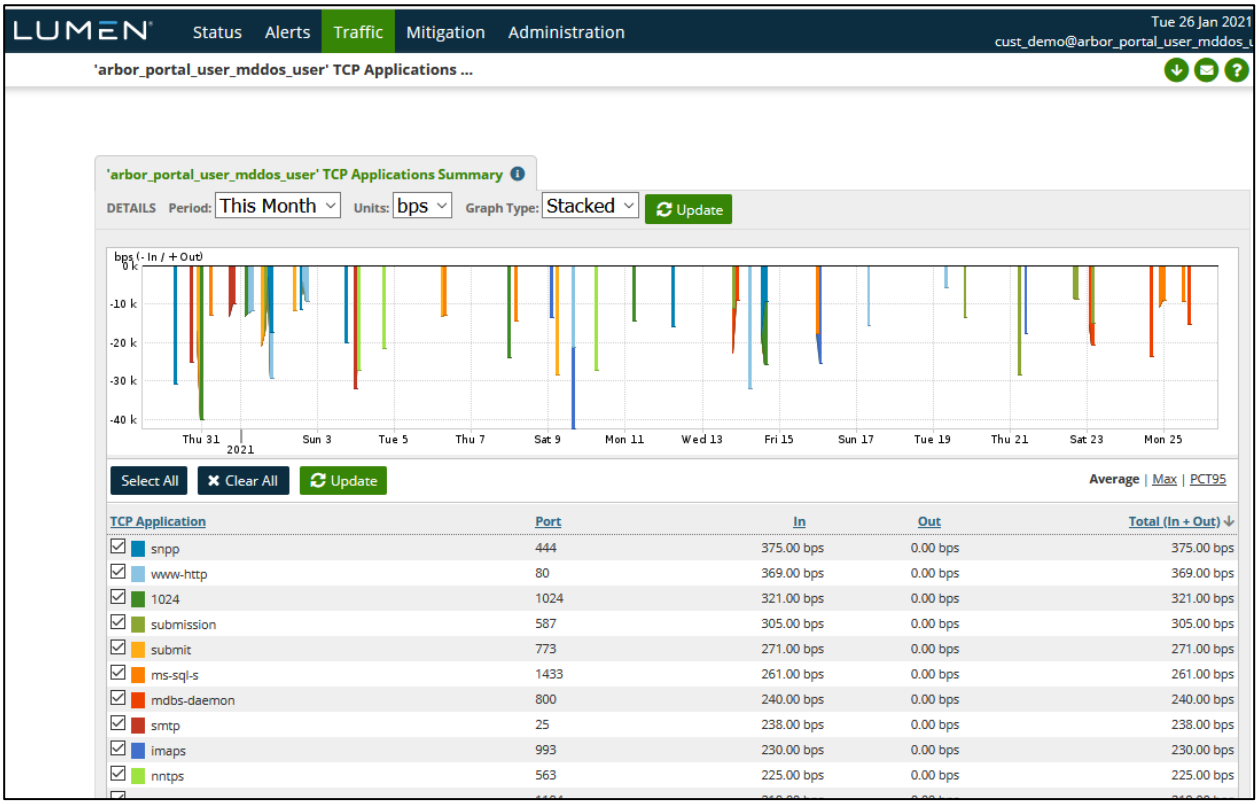
The negative values show traffic out of the customer network (“in” to Lumen), and the positive is the traffic into the customer network (“out” of Lumen).

Any selected ports are shown in the graph with a unique color. Any unchecked ports are not represented in the graph. The table can be sorted by clicking on a column header. Click the column header again to reverse the order.

There is a similar report for UDP ports that looks, and behaves identically, constraining the report to UDP traffic aggregated by UDP port.

Traffic > Summary > TCP

This screen breaks down the customer's traffic by IP-level protocol.



TCP Application	Port	In	Out	Total (In + Out)
snpp	444	375.00 bps	0.00 bps	375.00 bps
www-http	80	369.00 bps	0.00 bps	369.00 bps
1024	1024	321.00 bps	0.00 bps	321.00 bps
submission	587	305.00 bps	0.00 bps	305.00 bps
submit	773	271.00 bps	0.00 bps	271.00 bps
ms-sql-s	1433	261.00 bps	0.00 bps	261.00 bps
mdbs-daemon	800	240.00 bps	0.00 bps	240.00 bps
smtp	25	238.00 bps	0.00 bps	238.00 bps
imaps	993	230.00 bps	0.00 bps	230.00 bps
nntps	563	225.00 bps	0.00 bps	225.00 bps

Those shown here, TCP, ESP (for VPN traffic), UDP, and ICMP are the most likely to be seen. This screen is very similar in appearance, and function to those discussed previously.

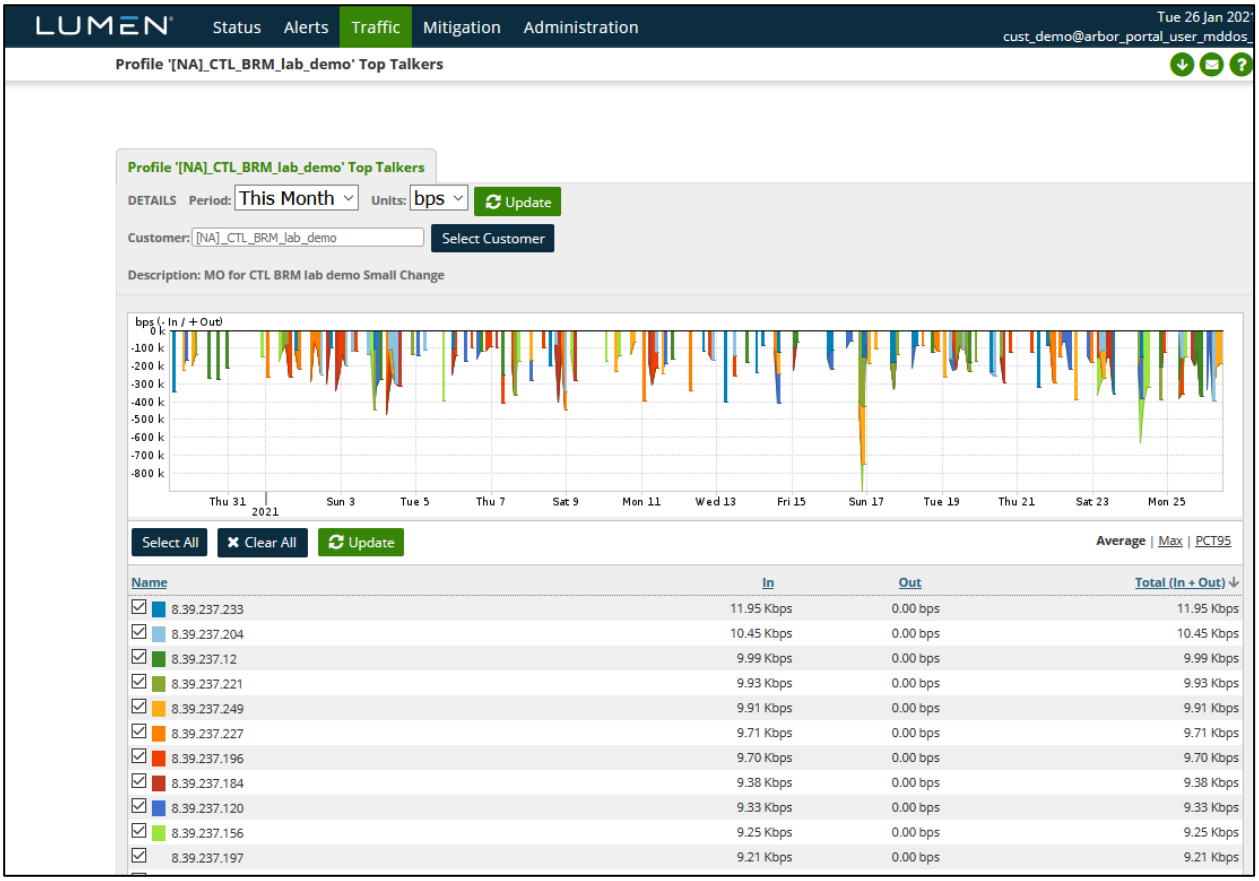
The default period is the previous 24 hours. The period can be changed to various predefined selections, or to “other” for a user-defined timeframe. The default display is bits per second (bps) but can be changed to packets per second (pps). Available graph types are Stacked, (default), Pie, and Bar.

The negative values show traffic out of the customer network (“into” Lumen), and the positive is the traffic into the customer network (“out” of Lumen).

Any selected protocols are shown in the graph with a unique color. Any unchecked protocols are not represented in the graph. The table can be sorted by clicking on a column header. Click the column header again to reverse the order.

Traffic > Profiles > Top Talkers

This screen identifies the systems generating the most traffic on the network that traverses the Lumen network:



The period is selectable from a pre-defined list. The graph type can be Bar (default), or Pie. Units can be bits per second (default) or packets per second.

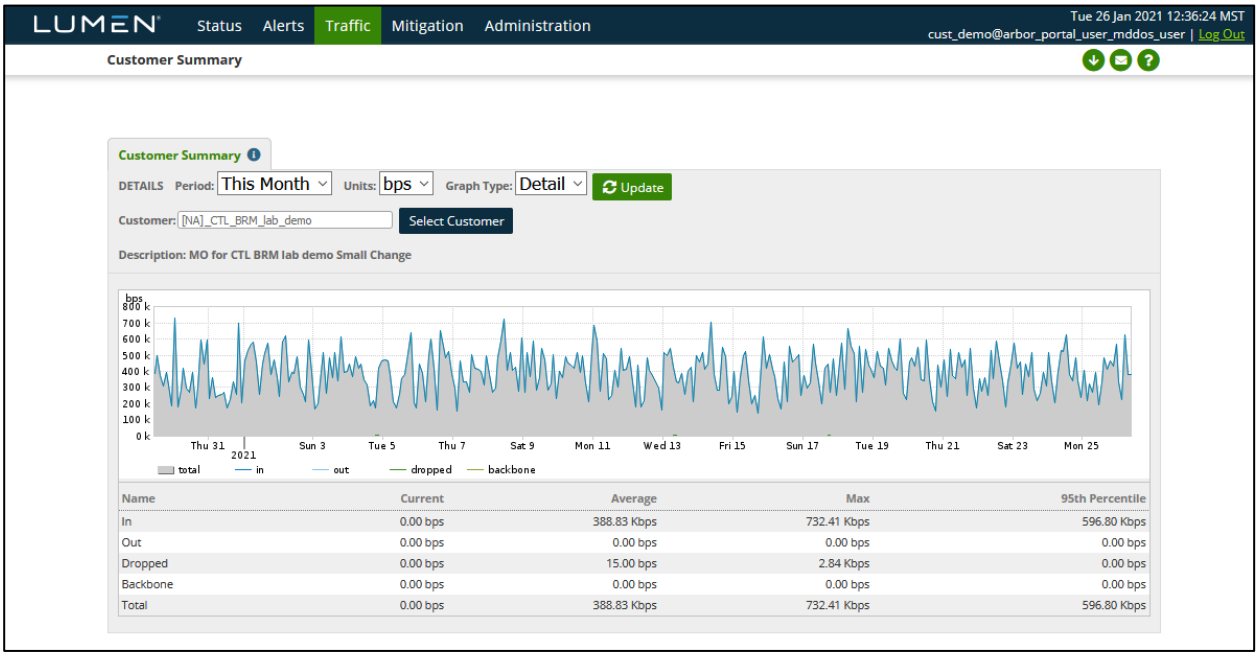
For each of the top-ranked hosts, the time, and rate of their individual peak rate is shown. Those hosts that are checked are shown on the graph with a unique color. Those hosts left unchecked are not shown in the graph.

If the DNS name of host can be resolved, it is shown to the left of the IP address. None of the addresses in the example above can be resolved. If resolved, the name would appear in the blank space to the left of the address.

The table can be sorted by clicking on a column heading. The order of the sort can be reversed by clicking on the column heading a second time.

Traffic > Profiles > Profile Detail

The summary reports above are for all the networks being monitored that are associated with the Arbor portal account. If you have multiple profiles (a.k.a. “managed objects”, or “zones”), you can view traffic reports restricted to one specific profile, with the options under Traffic →Profiles. This is a traffic summary report for one profile.



A different profile can be chosen from the selection box. The time period is selectable and customizable. Graph type can be Stacked (default), Pie, or Bar. Units can be bits per second (default), or packets per second. When any of these options is changed the “Update” button must be clicked.

Traffic is displayed as “IN” represents, into the Lumen network, hence out of the customer's networks. Likewise, “OUT” represents, out of the Lumen network and into the customer's networks.

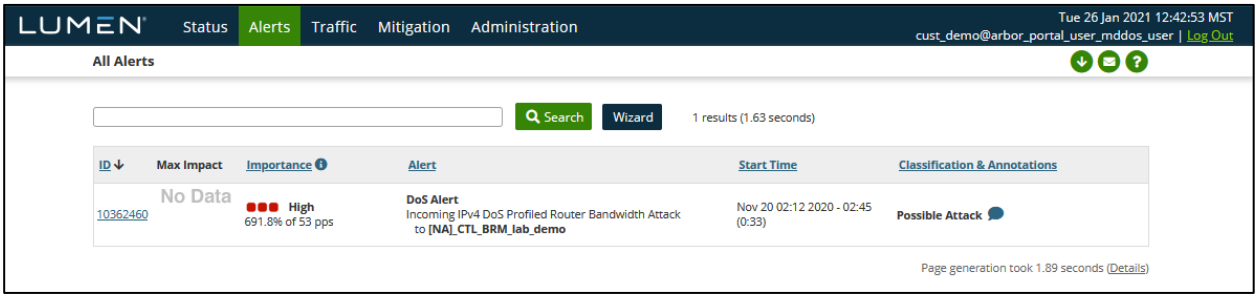
Traffic shown as “dropped” is traffic reported as dropped by backbone routers, not by the Arbor TMS DDoS mitigation devices. This data is unrelated to DDoS mitigations.

Only those directions/categories of traffic checked in the table are shown in the graph.

Application, Ports, Protocols, and Top Talker reports, identical to those previously discussed but restrained to a specific profile, are available under the Traffic →Profiles menu.

DDoS Alerts

DDoS Alerts can be viewed under Alerts →All Alerts, or by clicking on the number of ongoing or recent alerts on the status page. Here is a page resulting from clicking on the number of recent high alerts.



Alerts matching the selection criteria are listed up to 10 per page. They can be sorted in various ways by clicking on the column headers. The small graph shows the traffic rates for the affected destination IPs for the duration of the alert.

The Importance is assigned automatically by the Peakflow system based on various criteria.

The Alert details shows the type of Alert (bandwidth, misuse, profiled, e.g.) and the name of the managed object (often called “zone”) that is affected.

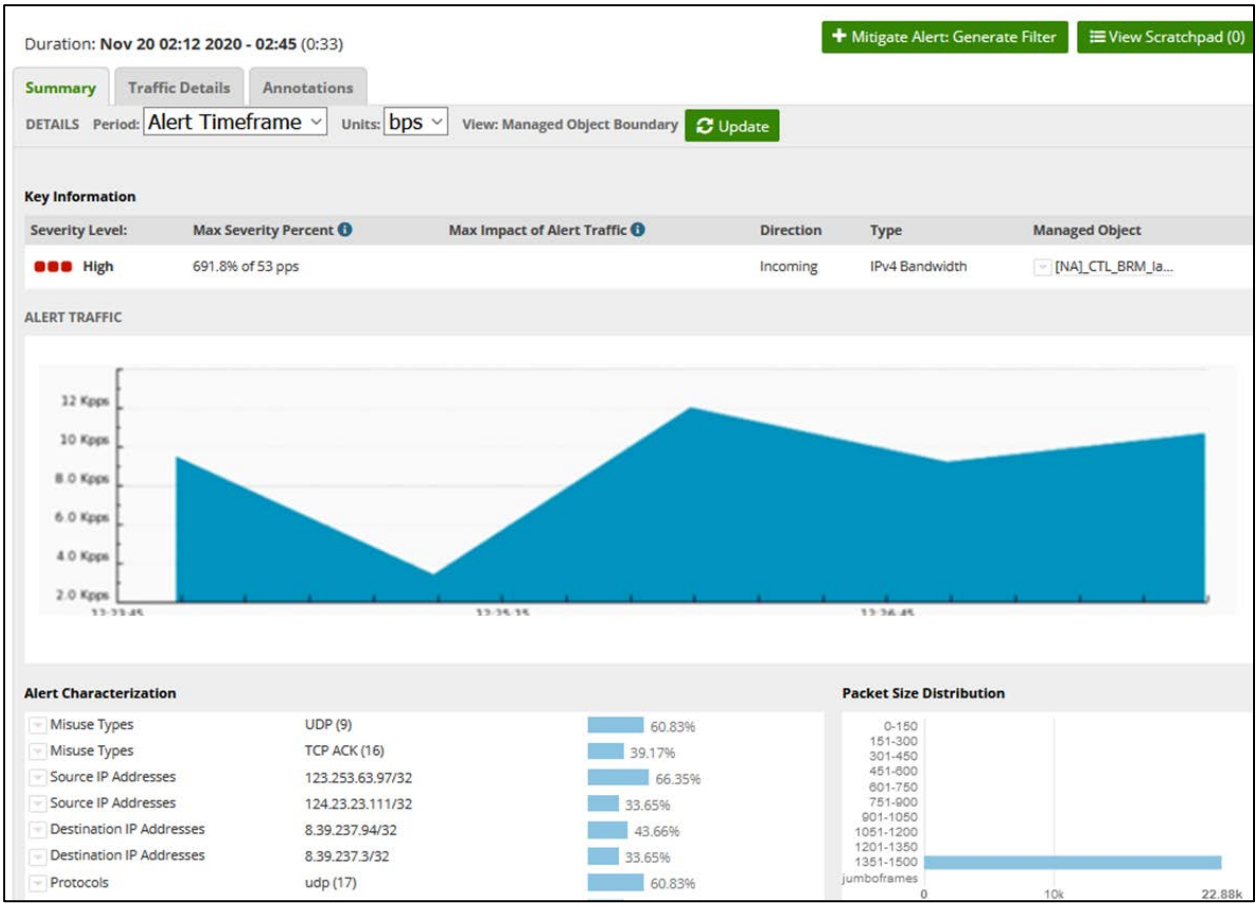
The start time and, if applicable, the end time of each alert is shown in the time zone configured for the portal account (defaults to UTC).

The Classification is initially assigned automatically by the Peakflow system as “Possible Attack”. This can be manually changed by operators to one of None, Flash Crowd, Network Failure, Trivial, or Verified Attack. This is for notational purposes only and has no effect on the operation of the system, and Lumen operators may omit setting this after investigating an alert.

Annotations, shown with the Classification, display the last automatic, or manual comment added to the alert. The third line above shows an example of an automatic comment added when a mitigation of that attack was initiated from the alert. (It is possible to initiate mitigations in other ways that don't associate the mitigation with the alert, in which case, no annotation such as this would be created.)

DDOS Alert Summary

An alert can be inspected by clicking on the alert ID number:



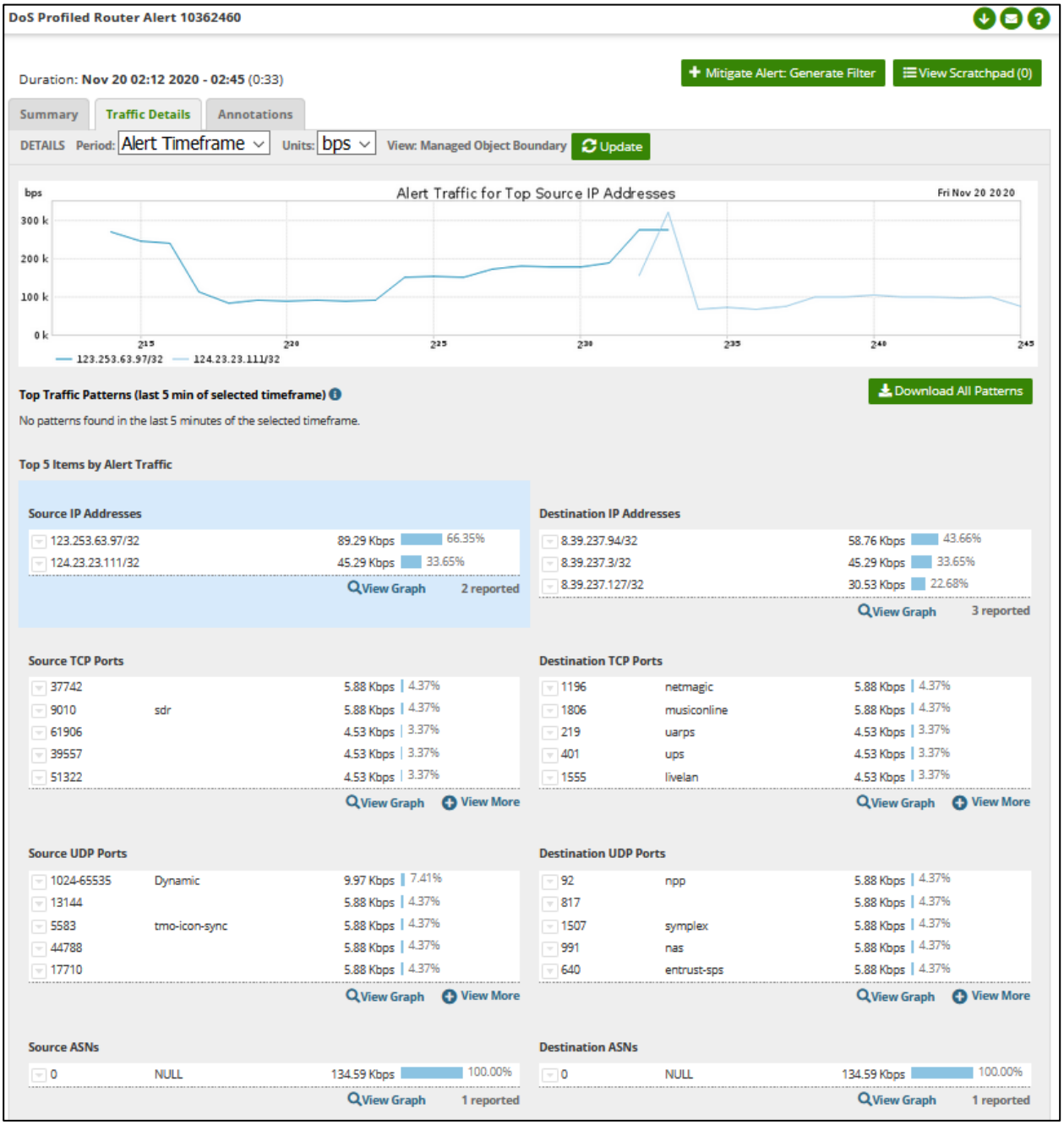
The graph shows the total traffic associated with the affected IPs during the alert, along with some information about the alert, such as the data rates, the type of alert, and the affected profile. (Most customers have one profile, a.k.a. zone, some may have multiple.)

The Alert Characteristics panel shows the most relevant source, and destination IPs, ports, and protocols. Protocol-appropriate information will also be shown, such as TCP Flags, ICMP codes, etc. The characteristics may be more or less specific, depending on the variation seen in the traffic. In this example, the source IPs are widespread on the Internet, some of the traffic has been narrowed down as coming from the same /10 network, but other traffic cannot be so categorized and is shown as coming from the Internet as a whole (0.0.0.0/0).

TCP Flags, list those flags commonly being seen in the traffic flow. These are all normal flags. A SYN Flood, e.g. would likely list only flag “S” as it would predominate.

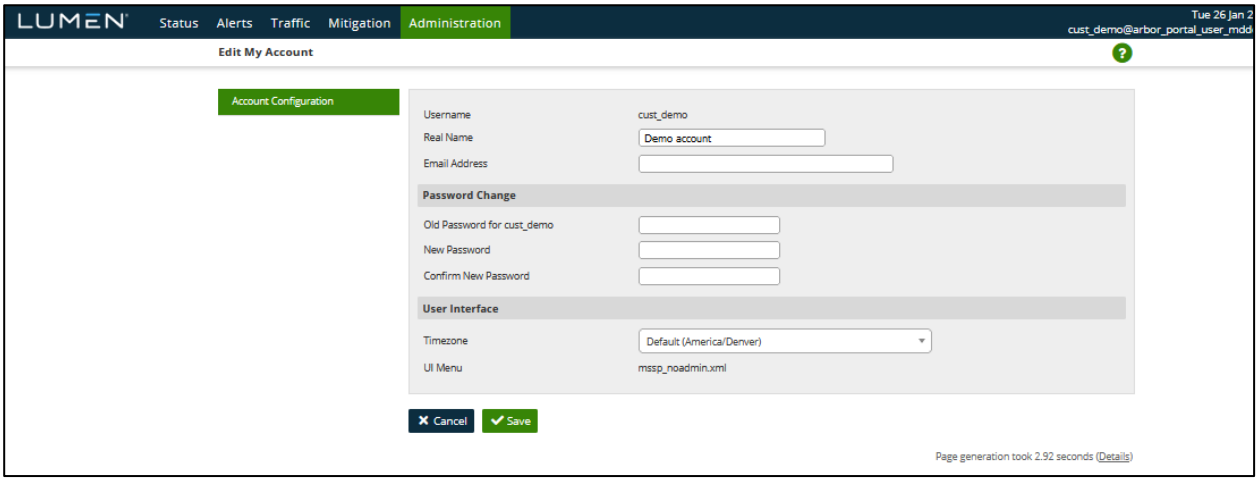
DDoS Alert Traffic Details

More detail about the traffic generating a DDoS alert is available in the data from individual routers in the Lumen backbone. The list of affected interfaces on individual routers is shown on the Alert Summary page, and the detail coming from a specific interface is accessed with the “Detail” button for a specific interface.



Administration → My Account

This page will display details of your account:



For more information

The DDoS Mitigation and Reporting portal offers excellent visibility into your DDoS Mitigation service. Make sure to use the Help selection often by selecting the "?" icon in the upper-right of every page for detailed descriptions of each page.

Additional information on DDoS Mitigation and other products can be found at the following locations:

- Lumen Security Solutions: https://www.lumen.com/en-us/solutions/connected-security.html
- DDoS Mitigation and Application Security: https://www.lumen.com/en-us/security/ddos-and-web-application.html
- Black Lotus LabsL: the Lumen Threat Research Lab: https://www.lumen.com/en-us/security/black-lotus-labs.html
- View a list of Lumen products: https://www.lumen.com/en-us/resources/product-finder.html
- Sign in to Control Center: https://www.lumen.com/login
- Learn more about Lumen: www.lumen.com