LP DDoS Shield
End-User Guide

October 2025

TABLE OF CONTENTS

CHAPTER 1 – OVERVIEW

This section provides an overview of the Customer Portal, including:

- Customer Portal Overview
- Key Functionality
- How Does the Customer Portal Work?
- DDoS Mitigation Life Cycle

LP DDoS Shield Portal Overview

LP DDoS Shield offers end-customers complete visibility of the managed security services statistics, including real-time dashboards that provide information about security attacks, traffic utilization, alerts, and more, as well as ad hoc reporting capabilities including exporting, scheduling, and saving report templates.

Key Functionality

The Customer Portal delivers the following key functionality:

- Real-time security dashboard, displaying only account-specific level security metrics
  - Select the security data associated with the asset to be displayed
- Flexibility and extensibility
  - Multiple dashboards per user
  - Persistent dashboard; retain the outline and customization after logout
- Full reporting capabilities
  - Predefined and custom reports
  - Save and load templates for future reuse
  - Scheduling report generation
  - Exporting reports (e-mailing is future capability)
- Ease of Use
  - High user experience for both peacetime and attack time
- Control a user's dashboards:
  - Enable/disable capabilities for a specific user

How Does the Customer Portal Work?

Upon deploying the LP DDoS Shield solution, Lightpath sets up accounts and assets that are to be protected. An asset is typically a network or a subnet. Each asset is mapped to a protection policy or protected object (PO). The Customer Portal routinely retrieves security data relevant to the policy or PO associated with the selected account, site or asset. In turn, the different widgets on the Customer Portal display to the end-user the relevant security measurements. Data is available on the real-time dashboard or as an ad hoc report.

DDoS Mitigation Life Cycle

The typical key stages of DDoS Mitigation are:

1. Preparation & Prevention
   Activities
   Deploy DDoS infrastructure
   Define normal traffic baselines

   Goal:
   Reduce attack surface and prepare for quick response.
   Detection & Identification - Spot anomalies that may signal an attack.

2. Monitor traffic for:
   Sudden volume spikes (volumetric)
   Protocol anomalies (e.g., SYN floods)
   Application-layer disruptions
   Use behavior analytics, heuristics, or AI-based detection.

   Goal:
   Quickly distinguish between legitimate traffic surges and malicious attacks.

3. Classification & Analysis - Understand the nature of the attack to determine the best mitigation approach.
   Key Factors:
   Attack type: volumetric, protocol, application layer
   Attack vectors: UDP floods, DNS amplification, HTTP floods, etc.
   Source IPs, geolocation, attack tools
   Targeted assets (IP, URL, service)

   Goal:
   Determine how the attack works to activate the most effective response method.

4. Mitigation & Response - Actively block or absorb the attack to maintain availability.
   Mitigation Techniques: (examples)
   Rate limiting or blackholing (for volumetric attacks)
   Geo-blocking/IP reputation filtering
   Scrubbing centers (cloud-based filtering)
   Reverse proxies or CDN rerouting
   Upstream filtering with ISPs
   Dynamic re-routing using BGP

   Goal:
   Minimize service degradation while allowing legitimate traffic through.

5. Post-Attack Recovery - Stabilize and restore normal operations after mitigation.
   Activities:
   Remove temporary filters or reroutes.
   Resume standard traffic flows.

   Goal:
   Restore full-service functionality while ensuring no lingering impacts.

CHAPTER 2 - USING THE CUSTOMER PORTAL

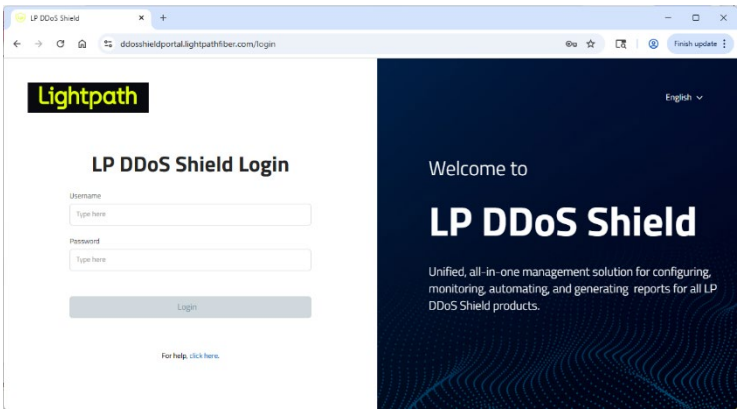
This chapter describes how to access and use the Customer management portal. The chapter includes the following sections:

- Log In
- Log Out
- Edit details about the Current User
- Customer Portal Overview
- Reports

Log In to MSSP Portal

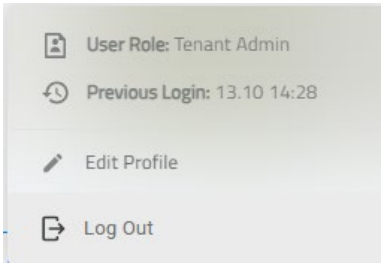
To log in to the Customer Portal

1. From a Web browser, enter the URL for the Customer Portal: https://ddosshieldportal.lightpathfiber.com/login
2. At the login prompt, enter your username and password.
    - You receive your username and password from your Lightpath Support Contact or Service Delivery Project Manager.
3. Click Login.



Log out of the MSSP Portal

1. **In the MSSP Portal toolbar, click the User ribbon at the at the far right. A drop-down dialog box opens.**



2. **Click Log Out**

Edit details about the Current User

This section describes how to edit current user details.

1. **In the User menu, click Edit Profile**
2. **In the Edit Profile dialog box, edit the following parameters, as required:**

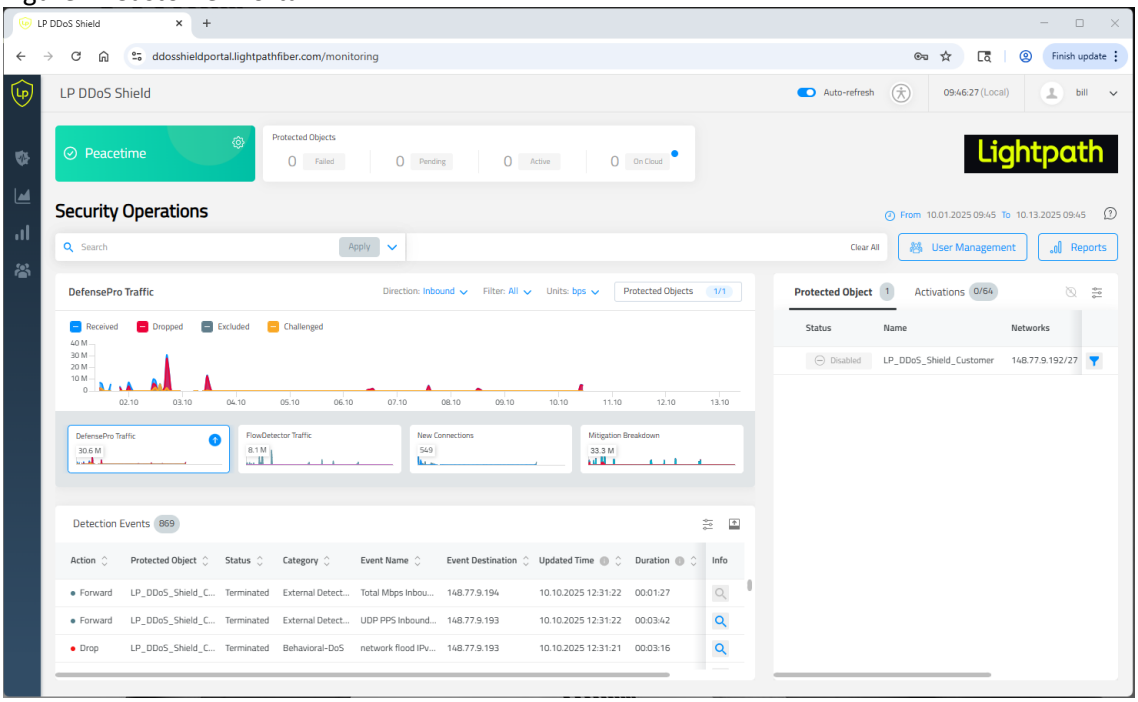
Parameter	Description
Username	The username used for login. (read-only)
User Full Name	The user's full name.
User Role	The role to which the user is associated. Each role defines a set of actions the user can perform (read-only).
Current Password	Currently defined password.
New Password	The new password, if you want to change the password.
Confirm New Password	Confirmation of the new password.
E-mail	The user's email address.
Display Time Zone	The time zone that displays in all MSSP screens. Values: Local Time Zone — Time zone where the user is located. UTC Time — Universal Time Coordinated. Default: Local Time Zone

3. **Click Submit**

CHAPTER 3 – CUSTOMER PORTAL OVERVIEW

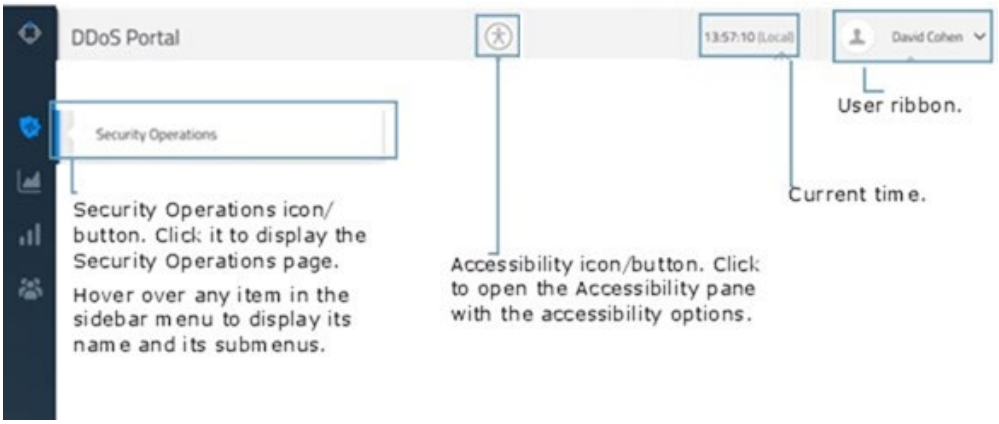
After you log in, the Customer Portal displays. The context of the display is the account associated with the username with which you logged in.

Figure 1: Customer Portal



Portal Toolbar and Sidebar Menu

The following figure shows the MSSP Portal (horizontal) toolbar and (vertical) sidebar menu



The MSSP Portal toolbar contains the following items:

- Accessibility button — The accessibility options let you globally change the look and feel of screen elements in the MSSP Portal screens.

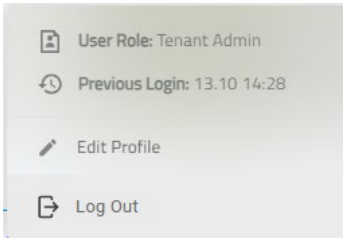
Click to open the Accessibility menu and configure the options that you require:

  - Use Patterns for Colors — When selected, the data in graphs throughout MSSP Portal display as colors with patterns (by default they display just as colors).
  - Stop Auto-refresh — When selected, pages throughout MSSP Portal do not auto-refresh (by default they auto-refresh.
  - Font Sizes — Displays a page that explains how to change the font size in various popular browsers.

- Refresh button and last refresh time — Clicking the button refreshes the dashboard with the latest data.
- User ribbon — Clicking in the ribbon opens a drop-down dialog box.

Use the dialog box to do the following:

- View the user name, RBAC role, and previous login time.
- Edit the current user profile parameters, if required. Click Edit Profile to display the Edit Profile dialog box:
  - Username (read-only) — The username used for login.
  - User Full Name — Full name of the user.
  - User Role (read-only) — The user's role.
  - *Current Password — User's current password.
  - New Password — New password, if you want to change the user's password.
  - Confirm New Password — Confirmation of the new password, if you want to change the user's password.
  - E-mail — E-mail address of the user.
  - Display Time Zone — Time zone to display. Values: Local Time Zone (Default), UTC Time
  - Log out of the session User Dialog Box



The MSSP Portal sidebar menu contains the following items:

- Security Operations — For the Real-Time Monitoring dashboard. This is also the landing page of the MSSP Portal. For more information, see MSSP Security Operations.
- Analytics — Opens a drop-down list with the following options for MSSP Portal Analytics for Radware Attack Mitigation Solution (AMS) products:
  - DefensePro Analytics — Opens the DefensePro Analytics dashboard.
  - Network Analytics — Opens the Network Analytics dashboards.
- Reporting — Opens a drop-down list with options for MSSP Portal Analytics for Radware products. Opens a drop-down list with the following options for MSSP Portal Analytics for Radware application-delivery-control products:
  - Reports — Opens the Reports module.
  - Forensics — Opens the Forensics module.
  - Alerts — Opens the Alerts module.
- User Management — Opens the User Management page for the Tenant Admin.

MSSP Security Operations

You access the MSSP Portal features from  Security Operations on the MSSP Portal sidebar menu.

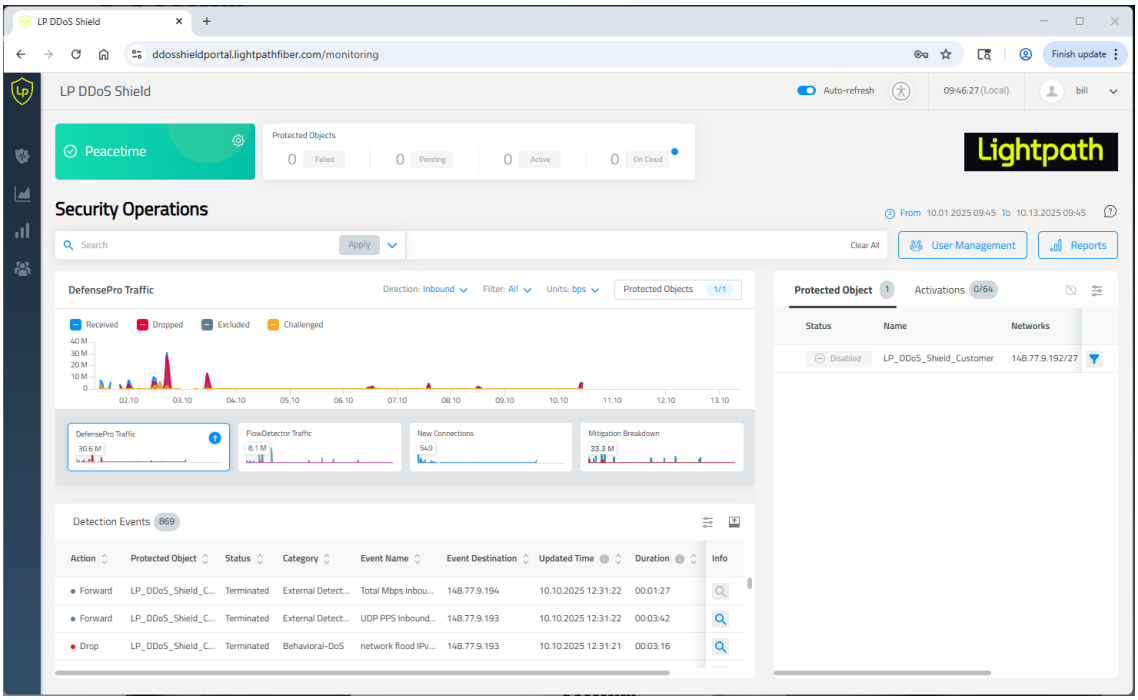
The Security Operations dashboard displays information and statistics and the operations on protected objects and activations, for both real time and historical information.

Note: For optimal viewing of the Security Operations dashboard, Radware recommends setting your screen resolution as follows:

- On a desktop: 1920x1024
- On a laptop: 1600x900

Note: You can adjust the width of the Traffic Utilization, Detection Events, and Protected Objects and Activations widget, as follows:

1. Hover between the Traffic Utilization or Detection Events widgets and the Protected Objects and Activation widget. A vertical scroll bar displays.
2. Click on the scroll bar and move it to the left or right as required to adjust the size of the widgets.
3. To revert the widgets to their default widths, double-click the vertical scroll bar.



MSSP Portal Analytics

MSSP Portal Analytics — Overview

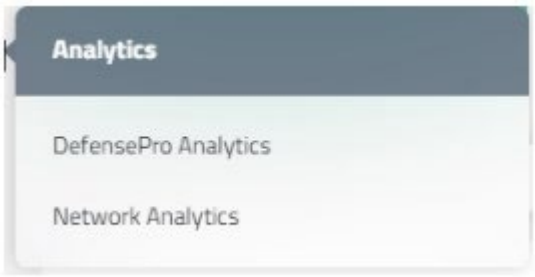
Dashboards display near real-time and historical monitoring and reporting metrics. Use the dashboards to track the security throughout the network(s) that are being protected. Dashboards summarize the existing network infrastructure in panels of graphs, charts, and tables. You can perform a deep analysis wherever necessary by drilling down into the event details.

Opening MSSP Portal Analytics

MSSP Portal Analytics opens through the MSSP Portal Web interface, which is referred to as *Web-based management* (*WBM*).

To open Analytics

1. Open the MSSP Portal WBM.
2. In the MSSP Portal sidebar menu, click Analytics. The list of Analytics items opens.
3. Select the item that you require. The selected item text changes to blue when highlighted.



Using Analytics Dashboards

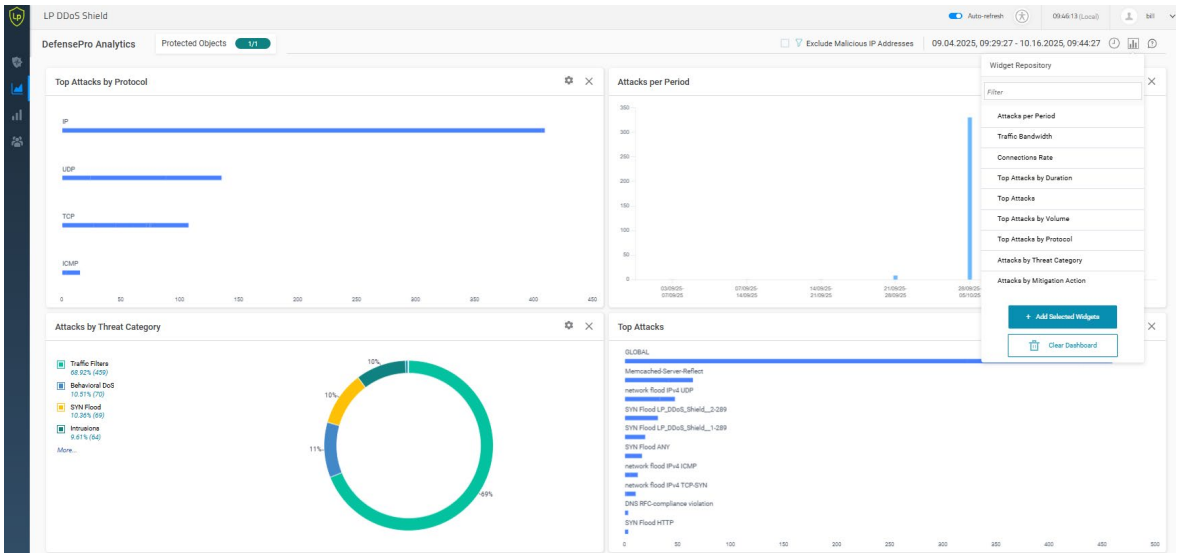
The MSSP Portal Analytics dashboards display monitoring and reporting metrics. These metrics enable you to view and track real-time and historical information on selected devices as well as security information on the traffic that the devices protect.
This section describes the following MSSP Portal Analytics dashboards:

- DefensePro Analytics dashboard
- Network Analytics dashboard

Defense Pro Analytics Dashboard

This section describes using the DefensePro Analytics dashboard.

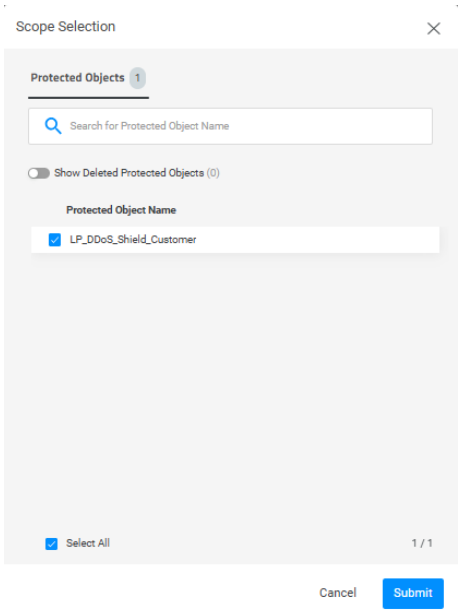
- Controlling the Information Source of the DefensePro Analytics Dashboard
- Configuring the Time Range of the DefensePro Analytics Dashboard
- Managing the Set of Widgets in the Analytics Dashboards



Controlling the Information Source of the DefensePro Analytics Dashboard

The DefensePro Analytics dashboard relates to specified protected objects on a specified virtual appliance.
To specify the protected object that the DefensePro Analytics dashboard relates to

1. Click the Protected Objects 1/1 box on the dashboard toolbar to open the Protected Objects dialog box.
2. In the Search for Protected Object Name text box, type a relevant value to narrow your search.



3. Select the option button next to the item that you require.
   - If you select only one protected object, the protected object name displays to the right of the Protected Objects 1/1 box.
   - If you select multiple protected objects, the selected protected objects display at the top of the list in alphabetical order. The remaining unselected protected objects display below the selected protected objects, also in alphabetical order.
4. You can select or deselect all of the protected objects with the Select All ( ) box.
   - If the list is unfiltered, this selects or deselects all of the protected objects. In this case, all of the protected objects available to the user are represented in the dashboards.
   - If the list is filtered, this only selects or deselects the filtered set of protected objects. In this case, only the filtered set of protected objects available to the user is represented in

the dashboards, and the Select All box displays as (partial).

- By default, the Protected Objects list includes only the currently configured protection objects. You can select the Show Deleted Protected Objects option.

When the Show Deleted Protected Objects option is enabled ( ), the Protected Objects list includes the currently configured protected objects — and also the protected objects deleted manually but still stored in the MSSP Portal database for historical statistical analysis. The names of the protected objects that were deleted manually are displayed in dark red.

5. Click Submit to save the configuration.

The display of the dashboard updates.

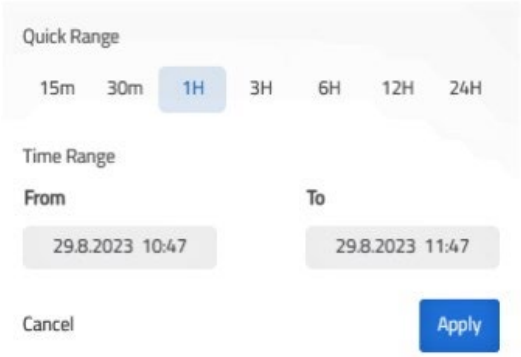
To export information in this display to a PDF file
Click Export. The file is downloaded to your local computer.

Configuring the Time Range of the DefensePro Analytics Dashboard

You can configure the time range for the information that dashboard widgets display information. The default time range is 1 hour — that is, from 1 hour ago until now.
DefensePro Analytics displays the configured time range to the left of the clock button ( ).

1. Click the clock button ( ) on the dashboard toolbar to open the Quick Range dialog box.
2. Do one of the following:
   - Select one of the following preset ranges (Quick Range):
     - 15m — The last 15 minutes
     - 30m — The last 30 minutes
     - 1H — The last hour
     - 3H — The last three hours
     - 6H — The last six hours
     - 12H — The last 12 hours
     - 24H — The last 24 hours

   Default: 1H



   - Specify a time range up to one year in the past, using the From and To boxes. You can click in a box to open a month calendar and a 24-hour digital clock. Use the left and right arrows to choose the required month. You can click the 24-hour digital clock to choose the time of day.
3. Click Apply to apply the configuration.

Managing the Set of Widgets in the Analytics Dashboards

You can add or remove widgets that some Analytics dashboards display currently.

Tip: Add a duplicate widget and modify its display to optimize the information that a dashboard provides or improves the legibility and/or clarity of a dashboard.

To add one or more widgets that the Analytics dashboard does not display currently

1. Click the  button on the dashboard toolbar.
2. Click the widget names and display the checkmark next to each name.
3. Click ADD SELECTED WIDGETS.

To remove a widget that the Analytics dashboard displays currently

Hover over the upper-right corner of the widget and click the  button.

To clear all the widgets that the Analytics dashboard displays currently

1. Click the  button on the dashboard toolbar.
2. Click CLEAR DASHBOARD.

The information that the widgets in the DefensePro Analytics dashboard display is according to the specified devices and scopes and the configured time range. For more information, see Controlling the Information Source of the DefensePro Analytics Dashboard and Configuring the Time Range of the DefensePro Analytics Dashboard, respectively.

Every widget in the DefensePro Analytics dashboard displays a legend, which identifies elements in the widget chart.

You can show and hide elements that a widget displays. To filter out a selected element from the display of a widget, click on the full colored square box in the legend (for example, ). To return a selected element to the display of a widget, click on the empty colored square in the legend (for example, ).

To identify an element in a chart and view more information about the element, hover over the relevant element.

Information about an element may be the name of the associated Protection policy, the absolute value of an element displayed as a percentage, the attack-protection, and so on.

If an element is the *attack-protection*, this refers to the DefensePro Attack-Protection identifier issued by the device.

Selecting the Exclude Malicious IP Addresses option (at the top-right of the dashboard) filters out all the attacks that the *ERT Active Attackers Feed module* handled. Selecting this option facilitates improved clarity when the data contains a high percentage of attacks in the Malicious IP Addresses category. This option applies only to widgets that relate to attack data, not to widgets that show statistics.

The DefensePro Analytics dashboard supports the following widgets:

- Attacks per Period — Displays a bar graph, where the bar shows the number of attacks per the specified time range for that bar.
    - To change the Scope setting of the widget, hover over the upper-right corner of a widget and click the gear button ( ).
    - To increase the size of the chart, hover over the lower-right corner of the widget and pull the arrow to the size you want.
- Traffic Bandwidth — Displays a graph showing the bandwidth of received, dropped, excluded, and challenged traffic over time — according to your preferences: bps or pps — and Inbound or Outbound.
    - The widget displays the relevant maximum value and minimum value — and also the date and time that the values were recorded. Hover over Max or Min to open a popup that shows the specific, relevant DefensePro device and Protection policy. Click on Max or Min to open a dialog box showing the Protection policies (in the specified scope) with the top five values.
        - To change the Scope setting of the widget, hover over the upper-right corner of a widget and click the gear button ( ).
        - To increase the size of the chart, hover over the lower-right corner of the widget and pull the arrow to the size you want.
    - You can hide the received, dropped, excluded, or challenged data in the graph by clicking Received, Dropped, Excluded, and Challenged as required.

Notes

- When traffic matches multiple Protection policies with Out-of-State protection, the value that the MSSP Portal Analytics displays for the total dropped traffic represents the sum of all dropped traffic for all relevant Protection policies. This is because when traffic matches multiple Protection policies with Out-of-State protection, all those Protection policies count the same dropped traffic.
- Excluded data refers to traffic that DefensePro passed through, because the traffic matched no Protection policy configured on the device.
- Challenged data refers to traffic that DefensePro challenged according to the configuration of the SYN Flood Protection profile and/or HTTPS Flood Protection profile in the Protection policy of the selected devices running DefensePro version 8.29 or later.

- Connections Rate — Displays the average connections per second (y-axis) (aggregated from all the selected devices) over time (x-axis).
    - The widget displays the relevant maximum value and minimum value — and also the date and time that the values were recorded. Hover over Max or Min to open a popup that shows the specific, relevant DefensePro device and Protection policy. Click on Max or Min to open a dialog box showing the Protection policies (in the specified scope) with the top five values.
        - To change the Scope setting of the widget, hover over the upper-right corner of a widget and click the gear button ( ).
        - To increase the size of the chart, hover over the lower-right corner of the widget and pull the arrow to the size you want.
- Top Attacks by Duration — Displays the duration-ranges of the attack-protections with the most attacks (arranged top to bottom in descending order from most prevalent, with attack quantity displayed on the x-axis). The duration-ranges are predefined: Less than 1 min, 1-5 min, 5-10 min,

10-30 min, 30-60 min, More than 1 hour. The hover popup shows the attack-protection and the number of attacks during the time range.

- To change the Scope setting of the widget, hover over the upper-right corner of a widget and click the gear button (⚙).
- To increase the size of the chart, hover over the lower-right corner of the widget and pull the arrow to the size you want.

- Top Attacks — Displays the 10 attack-protections with the most attacks (arranged top to bottom in descending order from most prevalent, with attack quantity displayed on the x-axis). To view the attack-protections details at Protection policy level, use Reports with the Summary Table enabled (for more information
  - To change the Scope setting of the widget, hover over the upper-right corner of a widget and click the gear button (⚙).
  - To increase the size of the chart, hover over the lower-right corner of the widget and pull the arrow to the size you want.
- Top Attacks by Volume — Displays the 10 attack-protections with the highest volume (arranged top to bottom in descending order from most prevalent, with attack volumes displayed on the x-axis). To view the attack-protections details at Protection policy level, use Reports with the Summary Table enabled
  - To change the Scope setting of the widget, hover over the upper-right corner of a widget and click the gear button (⚙).
  - To increase the size of the chart, hover over the lower-right corner of the widget and pull the arrow to the size you want.
- Top Attacks by Protocol — Displays the protocols with the highest number of attacks (arranged top to bottom in descending order from most prevalent, with attack quantity displayed on the x-axis). To view the attack-protections details at Protection policy level, use Reports with the Summary Table enabled.
  - To change the Scope setting of the widget, hover over the upper-right corner of a widget and click the gear button (⚙).
  - To increase the size of the chart, hover over the lower-right corner of the widget and pull the arrow to the size you want.
- Attacks by Threat Category — Displays a doughnut chart showing the distribution of the attacks according to threat category — that is, the name of the protection module or protection mechanism.
  - To change the Scope setting of the widget, hover over the upper-right corner of a widget and click the gear button (⚙).
  - To increase the size of the chart, hover over the lower-right corner of the widget and pull the arrow to the size you want.
- Attacks by Mitigation Action — Displays the mitigation action(s) (Forward, Challenge, or Drop) with the highest number of attacks (arranged top to bottom in descending order from most prevalent, with attack quantity displayed on the x-axis). To view the attack-protections details at Protection policy level, use Reports with the Summary Table enabled.
  - Note: The name of the protection module may also be referred to as the threat type or threat category the attack.
  - To change the Scope setting of the widget, hover over the upper-right corner of a widget and click the gear button (⚙).
  - To increase the size of the chart, hover over the lower-right corner of the widget and

pull the arrow to the size you want.

Network Analytics Dashboard

Network Analytics includes the DefensePro and FlowDetector Analytics dashboards, enabling users to view and monitor statistics collected by DefensePro and the FlowDetector Collector, respectively.
This section includes:

- DefensePro Analytics
- FlowDetector Analytics
- Application Analytics
- DNS Analytics

These dashboards

- Aid you understanding traffic patterns, services, and long-term trends in peacetime
- Aid you in detecting anomalies and suspicious patterns during attacks
- Help you to tune your DefensePro or FlowDetector configuration, respectively
- Let you generate and share reports

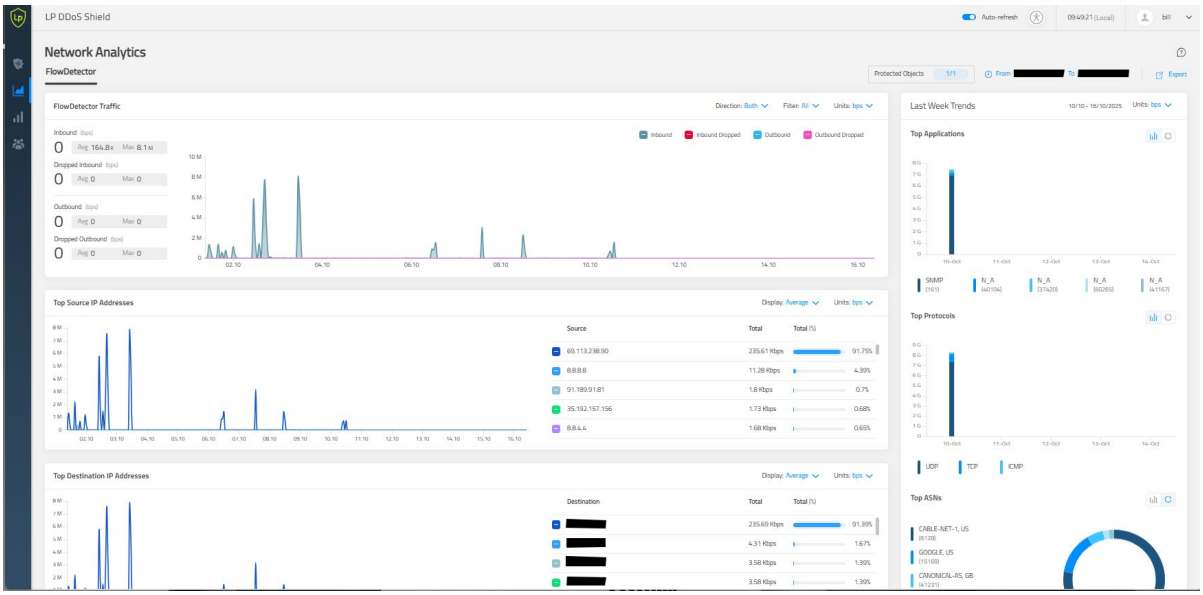
NOTE: Analytics for different components are available to LP DDoS Shield Customers according to the table below:

LP DDoS Shield Customer	DefensePro	FlowDetector	Application	DNS
Plus		✓		
Premier	✓	✓	✓	✓

FlowDetector Analytics

Definition: The Flow Detector monitors network traffic, establishing a baseline of normal traffic patterns using flow counters, and automatically redirects suspicious traffic to mitigation appliances when a deviation occurs. The input to the Flow Detector is samples of network traffic (netflow sampling).

After you open the dashboard, you can specify the scope and the time frame that the dashboard-display relates to. You can also filter the display to show statistics on selected protected objects.



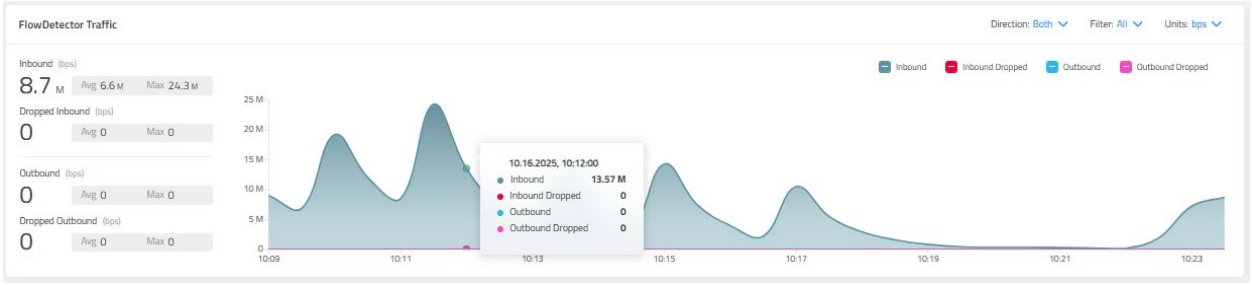
Every widget in the FlowDetector Analytics dashboard displays a legend, which identifies elements in the widget chart. To identify an element in a chart and view more information about the element, hover over the relevant element.

Information about an element may be the name of the associated protected object, the absolute value of an element that is displayed as a percentage, and so on.

The FlowDetector Analytics dashboard supports the following widgets:

FlowDetector Traffic

This widget includes the average and maximum traffic for the flow statistics that the MSSP Portal receives from FlowDetector per the selected scope and time range. To identify an element in the chart and view more information about the element, hover over the relevant element.



FlowDetector Statistics

Parameter	Description
Inbound	Inbound FlowDetector traffic.
Dropped Inbound	Dropped inbound FlowDetector traffic.
Outbound	Outbound FlowDetector traffic.
Dropped Outbound	Dropped outbound FlowDetector traffic.

To select with protocol to display: From the filter drop-down list, select the protocol to display: All, TCP, UDP, Other, ICMP, Fragmented. The display changes per your selection.

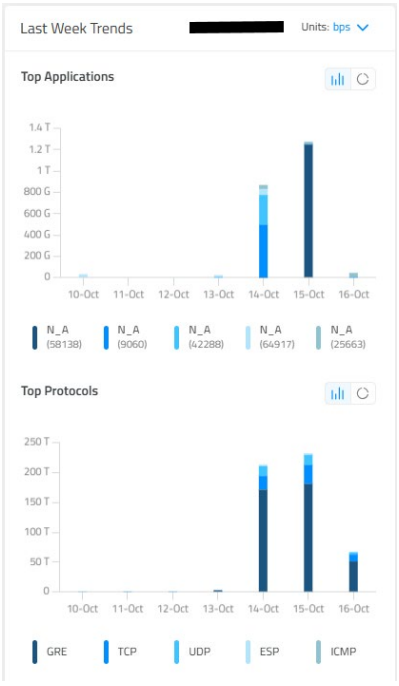
To select which traffic units to display: From the units drop-down list, select the traffic units to display: bps (bits per second) or pps (packets per second), The display changes per your selection

To remove/include individual statistics in the statistics display: By default, all FlowDetector traffic statistics display in the graph. You can remove/include individual statistics to display:

1. To remove a statistic from the graph, click the label of that statistic. The label is grayed out and the statistic is removed from the graph.
2. To include a statistic in the graph, click the grayed-out label of that statistic. The statistic displays in the graphic.

Last Week Trends

This widget displays last week's trends for the top five applications, protocols, and ASNs either as bar or pie charts. The graphs are not affected by the selected scope and time range for the FlowDetector Analytics dashboard. To identify an element in the chart and view more information about the element, hover over the relevant element.



The graphs have corresponding individual widgets (see Top Applications, Top Protocols, and Top ASNs), which display the data per the general time range of the FlowDetector Analytics dashboard.

To select which type of graph to display for each graph (separately)

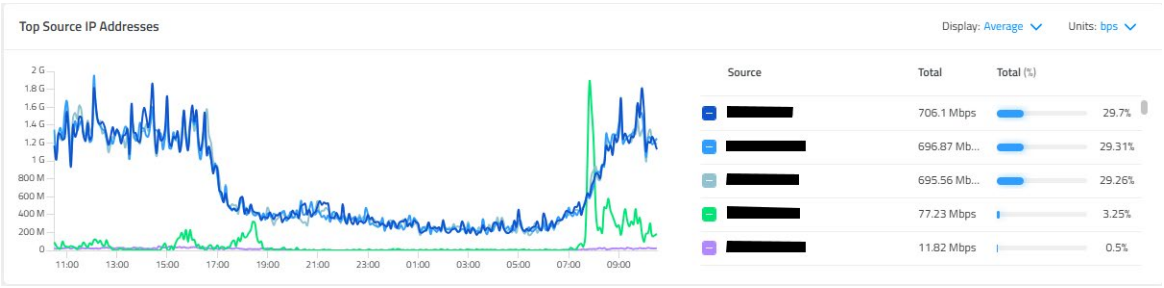
- To change the graph type between a horizontal bar graph and a pie chart, toggle between the horizontal bar graph icon ()and the pie chart icon ().
- The display changes per your selection.
- The bar graph displays the total capacity of the top five (5) items per day for the last seven (7) days.
  Some days may display as empty because none of the top (5) items had collected traffic on that day.

To select which traffic units to display:

- From the units drop-down list, select the traffic units to display: bps (bits per second) or pps (packets per second), The display changes per your selection.

Top Source IP Addresses

This widget displays the top 100 source IP addresses per the selected scope and time range for the FlowDetector Analytics dashboard in both graphical and tabular form. This includes the source IP address, the total traffic from that IP address, and the percentage of the total traffic of the top 100 source IP addresses. To identify an element in the chart and view more information about the element, hover over the relevant element.



To select by which parameter to display the FlowDetector traffic data: From the Display drop-down list, select the method by which to display the FlowDetector traffic data: Total, Avg, Last, Max
The display changes per your selection.
Sort options:

- Total — Displays the total top 100 source IP addresses per the bps or pps values, as selected.
- Avg — Displays the average top 100 source IP addresses per the bps or pps values, as selected.
- Last — Displays the top 100 source IP addresses per the last sample in the configured time frame per the bps or pps values, as selected.
- Max — Displays the maximum top 100 source IP addresses per the bps or pps values, as selected.

Note: If the selected time frame is greater than one (1) hour, the Max option does not display and is not available.

Default: Avg
By default, the top five (5) items are selected, and you can scroll the table to see the remaining items. You change the selected items and choose up to 10 items.

To select which traffic units to display: from the units drop-down list, select the traffic units to display: bps (bits per second) or pps (packets per second), The display changes per your selection.

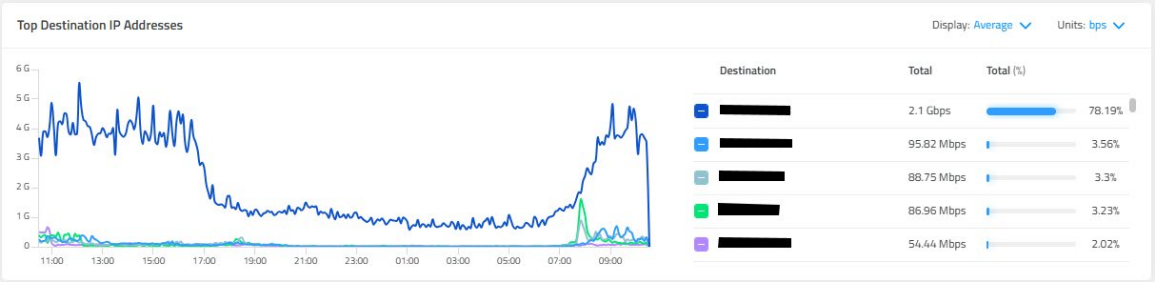
To remove/include individual statistics in the statistics display: By default, all statistics display. You can remove/include individual statistics to display:

1. To remove a statistic, click the label of that statistic. The label is grayed out and the statistic is removed.

2. To include a statistic, click the grayed-out label of that statistic. The statistic displays.

Top Destination IP Addresses

This widget displays the top 100 destination IP addresses per the selected scope and time range for the FlowDetector Analytics dashboard in both graphical and tabular form. This includes the destination IP address, the total traffic to that IP address, and the percentage of the total traffic of the top 100 destination IP addresses. To identify an element in the chart and view more information about the element, hover over the relevant element.



To select by which parameter to display the FlowDetector traffic data: From the Display drop-down list, select the method by which to display the FlowDetector traffic data: Total, Avg, Last, Max
The display changes per your selection.

Sort options:

- Total — Displays the total top 100 destination IP addresses per the bps or pps values, as selected.
- Avg — Displays the average top 100 destination IP addresses per the bps or pps values, as selected.
- Last — Displays the top 100 destination IP addresses per the last sample in the configured time frame per the bps or pps values, as selected.
- Max — Displays the maximum top 100 destination IP addresses per the bps or pps values, as selected.

Note: If the selected time frame is greater than one (1) hour, the Max option does not display and is not available.

Default: Avg
By default, the top five (5) items are selected, and you can scroll the table to see the remaining items. You change the selected items and choose up to 10 items.

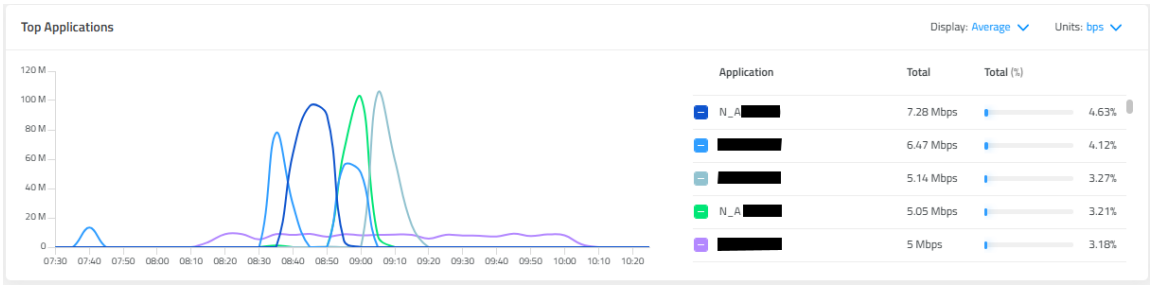
To select which traffic units to display: From the units drop-down list, select the traffic units to display: bps (bits per second) or pps (packets per second), The display changes per your selection.

To remove/include individual statistics in the statistics display: By default, all statistics display. You can remove/include individual statistics to display:

1. To remove a statistic, click the label of that statistic. The label is grayed out and the statistic is removed.
2. To include a statistic, click the grayed-out label of that statistic. The statistic displays.

Top Applications

This widget displays the top 100 applications per the selected scope and time range for the FlowDetector Analytics dashboard in both graphical and tabular form. This includes the application, the total traffic for that application, and the percentage of the total traffic of the top 100 applications. To identify an element in the chart and view more information about the element, hover over the relevant element.



To select by which parameter to display the FlowDetector traffic data: From the Display drop-down list, select the method by which to display the FlowDetector traffic data: Total, Avg, Last, Max
The display changes per your selection.
Sort options:

- Total — Displays the total top 100 applications per the bps or pps values, as selected.
- Avg — Displays the average top 100 applications per the bps or pps values, as selected.
- Last — Displays the top 100 applications per the last sample in the configured time frame per the bps or pps values, as selected.
- Max — Displays the maximum top 100 applications per the bps or pps values, as selected.

Note: If the selected time frame is greater than one (1) hour, the Max option does not display and is not available.

Default: Avg
By default, the top five (5) items are selected, and you can scroll the table to see the remaining items. You change the selected items and choose up to 10 items.

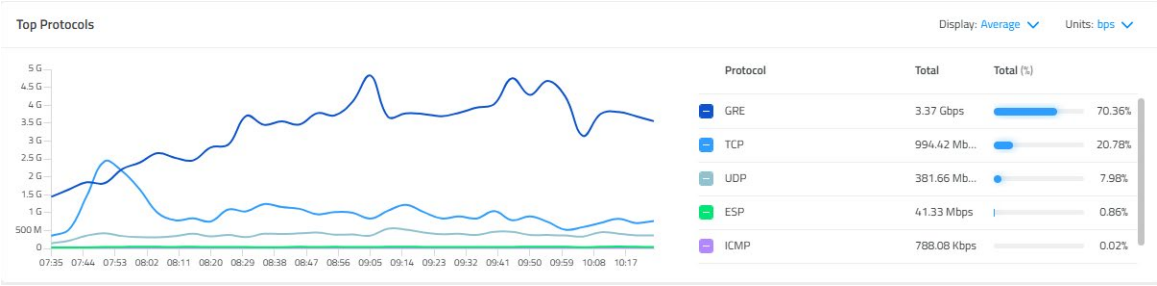
To select which traffic units to display: From the units drop-down list, select the traffic units to display: bps (bits per second) or pps (packets per second), The display changes per your selection.

To remove/include individual statistics in the statistics display
By default, all statistics display. You can remove/include individual statistics to display:

1. To remove a statistic, click the label of that statistic. The label is grayed out and the statistic is removed.
2. To include a statistic, click the grayed-out label of that statistic. The statistic displays.

Top Protocols

This widget displays the top 100 protocols per the selected scope and time range for the FlowDetector Analytics dashboard in both graphical and tabular form. This includes the protocol, the total traffic for that protocol, and the percentage of the total traffic of the top 100 protocols. To identify an element in the chart and view more information about the element, hover over the relevant element.



To select by which parameter to display the FlowDetector traffic data: From the Display drop-down list, select the method by which to display the FlowDetector traffic data: Total, Avg, Last, Max
The display changes per your selection.
Sort options:

- Total — Displays the total top 100 applications per the bps or pps values, as selected.
- Avg — Displays the average top 100 applications per the bps or pps values, as selected.
- Last — Displays the top 100 applications per the last sample in the configured time frame per the bps or pps values, as selected.
- Max — Displays the maximum top 100 applications per the bps or pps values, as selected.

Note: If the selected time frame is greater than one (1) hour, the Max option does not display and is not available.

Default: Avg
By default, the top five (5) items are selected, and you can scroll the table to see the remaining items. You change the selected items and choose up to 10 items.

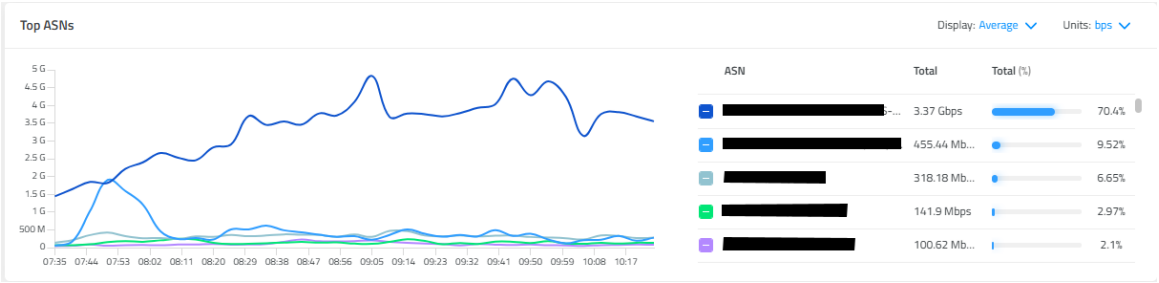
To select which traffic units to display: From the units drop-down list, select the traffic units to display: bps (bits per second) or pps (packets per second), The display changes per your selection.

To remove/include individual statistics in the statistics display
By default, all statistics display. You can remove/include individual statistics to display:

1. To remove a statistic, click the label of that statistic. The label is grayed out and the statistic is removed.
2. To include a statistic, click the grayed-out label of that statistic. The statistic displays.

Top ASNs

This widget displays the top 100 ASNs per the selected scope and time range for the FlowDetector Analytics dashboard in both graphical and tabular form. This includes the total traffic for that ASN, and the percentage of the total traffic of the top 100 ASNs. To identify an element in the chart and view more information about the element, hover over the relevant element.



To select by which parameter to display the FlowDetector traffic data : From the Display drop-down list, select the method by which to display the FlowDetector traffic data: Total, Avg, Last, Max The display changes per your selection.
Sort options:

- Total — Displays the total top 100 applications per the bps or pps values, as selected.
- Avg — Displays the average top 100 applications per the bps or pps values, as selected.
- Last — Displays the top 100 applications per the last sample in the configured time frame per the bps or pps values, as selected.
- Max — Displays the maximum top 100 applications per the bps or pps values, as selected.

Note: If the selected time frame is greater than one (1) hour, the Max option does not display and is not available.

Default: Avg
By default, the top five (5) items are selected, and you can scroll the table to see the remaining items. You change the selected items and choose up to 10 items.

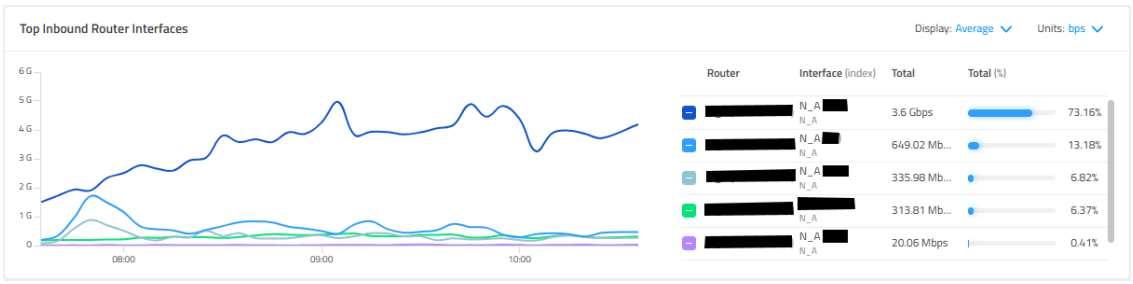
To select which traffic units to display: From the units drop-down list, select the traffic units to display: bps (bits per second) or pps (packets per second), The display changes per your selection.

To remove/include individual statistics in the statistics display
By default, all statistics display. You can remove/include individual statistics to display:

1. To remove a statistic, click the label of that statistic. The label is grayed out and the statistic is removed.
2. To include a statistic, click the grayed-out label of that statistic. The statistic displays.

Top Inbound Router Interfaces

This widget displays the top 100 inbound router interfaces per the selected scope and time range for the FlowDetector Analytics dashboard in both graphical and tabular form. This includes the router name, router interface, the total traffic for that router interface, and the percentage of the total traffic of the top 100 inbound router interfaces. To identify an element in the chart and view more information about the element, hover over the relevant element.
Currently the MSSP Portal can display only the router IP address and the interface index number. In future releases there are plans to add SNMP integration with the routers to complete the full interface name and description.



To select by which parameter to display the FlowDetector traffic data: From the Display drop-down list, select the method by which to display the FlowDetector traffic data: Total, Avg, Last, Max
The display changes per your selection.
Sort options:

- Total — Displays the total top 100 applications per the bps or pps values, as selected.
- Avg — Displays the average top 100 applications per the bps or pps values, as selected.
- Last — Displays the top 100 applications per the last sample in the configured time frame per the bps or pps values, as selected.
- Max — Displays the maximum top 100 applications per the bps or pps values, as selected.

Note: If the selected time frame is greater than one (1) hour, the Max option does not display and is not available.

Default: Avg
By default, the top five (5) items are selected, and you can scroll the table to see the remaining items. You change the selected items and choose up to 10 items.

To select which traffic units to display: From the units drop-down list, select the traffic units to display: bps (bits per second) or pps (packets per second), The display changes per your selection.

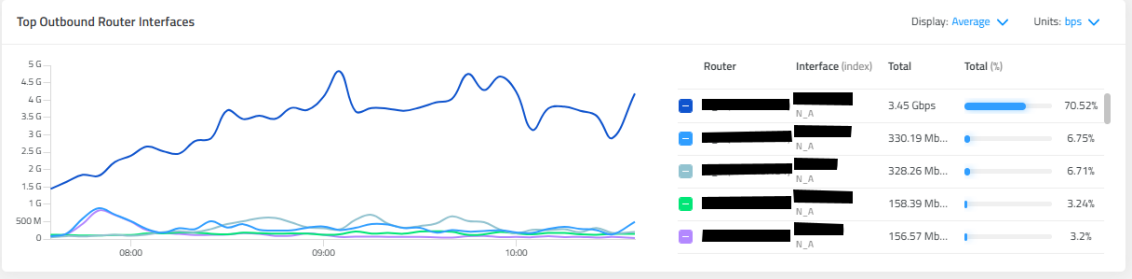
To remove/include individual statistics in the statistics display
By default, all statistics display. You can remove/include individual statistics to display:

1. To remove a statistic, click the label of that statistic. The label is grayed out and the statistic is removed.
2. to include a statistic, click the grayed-out label of that statistic. The statistic displays.

Top Outbound Router Interfaces

This widget displays the top 100 outbound router interfaces per the selected scope and time range for the FlowDetector Analytics dashboard in both graphical and tabular form. This includes the router name, router interface, the total traffic for that router interface, and the percentage of the total traffic of the top 100 outbound router interfaces. To identify an element in the chart and view more information about the element, hover over the relevant element.

Currently the MSSP Portal can display only the router IP address and the interface index number. In future releases there are plans to add SNMP integration with the routers to complete the full interface name and description.



To select by which parameter to display the FlowDetector traffic data: From the Display drop-down list, select the method by which to display the FlowDetector traffic data: Total, Avg, Last, Max
The display changes per your selection.
Sort options:

- Total — Displays the total top 100 outbound router interfaces per the bps or pps values, as selected.
- Avg — Displays the average top 100 outbound router interfaces per the bps or pps values, as selected.
- Last — Displays the top 100 outbound router interfaces per the last sample in the configured time frame per the bps or pps values, as selected.
- Max — Displays the maximum top 100 outbound router interfaces per the bps or pps values, as selected.

Note: If the selected time frame is greater than one (1) hour, the Max option does not display and is not available.

Default: Avg
By default, the top five (5) items are selected, and you can scroll the table to see the remaining items. You change the selected items and choose up to 10 items.

To select which traffic units to display: From the units drop-down list, select the traffic units to display: bps (bits per second) or pps (packets per second), The display changes per your selection.

To remove/include individual statistics in the statistics display: By default, all statistics display. You can remove/include individual statistics to display:

1. To remove a statistic, click the label of that statistic. The label is grayed out and the statistic is removed.
2. To include a statistic, click the grayed-out label of that statistic. The statistic displays.

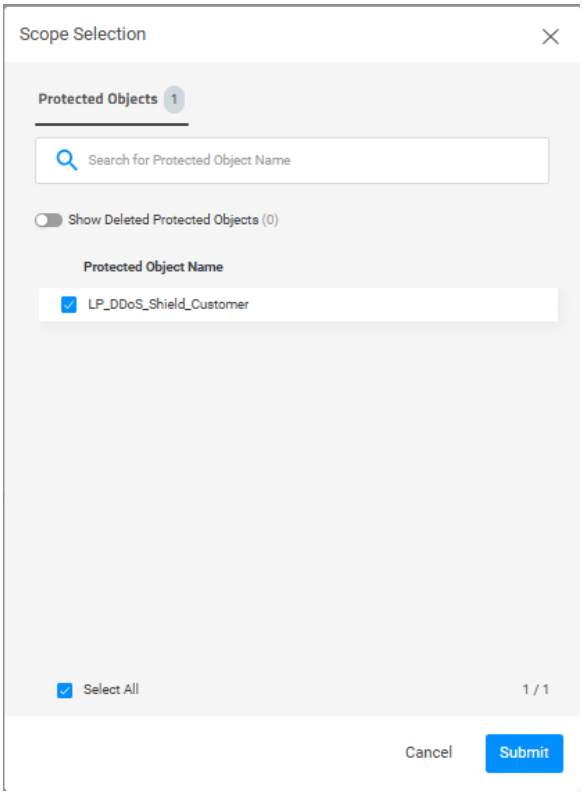
DefensePro Analytics

DefensePro Traffic
Last Week Trends
Top Inbound Source IP Addresses
Top Inbound Destination IP Addresses
Top Inbound Source Applications
Top Inbound Destination Applications
Top Inbound Protocols
Top Inbound Countries

FlowDetector Analytics

Application Analytics

Top TLS Fingerprints Dashboard



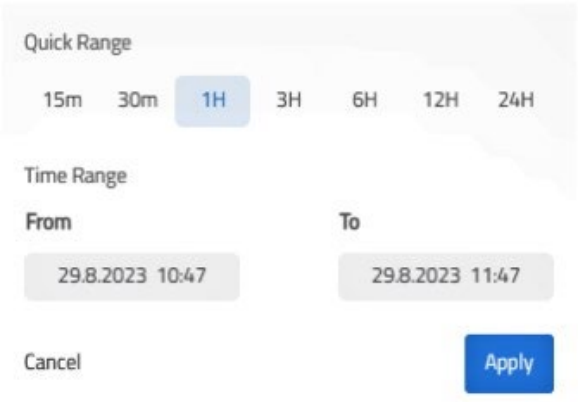
1. Click the Protected Objects 1/1 box on the dashboard toolbar to open the Protected Objects dialog box.
2. In the Search for Protected Object Name text box, type a relevant value to narrow your search.
3. Select the option button next to the item that you require.
   - If you select only one protected object, the protected object name displays to the right of the Protected Objects 1/1 box.
   - If you select multiple protected objects, the selected protected objects display at the top of the list in alphabetical order. The remaining unselected protected objects display below the selected protected objects, also in alphabetical order.
4. You can select or deselect all of the protected objects with the Select All ( ) box.
   - If the list is unfiltered, this selects or deselects all of the protected objects. In this case, all of the protected objects available to the user are represented in the dashboards.
   - If the list is filtered, this only selects or deselects the filtered set of protected objects. In this case, only the filtered set of protected objects available to the user is represented in the dashboards, and the Select All box displays as (partial).
   - By default, the Protected Objects list includes only the currently configured protection objects. You can select the Show Deleted Protected Objects option.
   - When the Show Deleted Protected Objects option is enabled ( ), the Protected Objects list includes the currently configured protected objects — and also the protected objects deleted manually but still stored in the MSSP Portal database for historical statistical analysis. The names of the protected objects that were deleted manually are displayed in dark red.
5. Click Submit to save the configuration.

The display of the dashboard updates.

To configure the time range for the Top TLS Fingerprints dashboard information

You can configure the time range for the information that dashboard widgets display information. The default time range is 1 hour — that is, from 1 hour ago until now.
The Top TLS Fingerprints dashboard displays the configured time range to the left of the clock button ( ).

1. Click the clock button ( ) on the dashboard toolbar to open the Quick Range dialog box.
2. Do one of the following:
   - Select one of the following preset ranges (Quick Range):
     - 15m — The last 15 minutes
     - 30m — The last 30 minutes
     - 1H — The last hour
     - 3H — The last three hours
     - 6H — The last six hours
     - 12H — The last 12 hours
     - 24H — The last 24 hours



Default: 15m

   - Specify a time range up to one year in the past, using the From and To boxes. You can click in a box to open a month calendar and a 24-hour digital clock. Use the left and right arrows to choose the required month. You can click the 24-hour digital clock to choose the time of day.
3. Click Apply to apply the configuration.

To export information in this display to a PDF file
- ➢ Click Export. The file is downloaded to your local computer.

To select by which parameter to display the TLS data
- ➢ From the Display drop-down list, select the method by which to display the TLS data: Average, Last, Max, Total

The display changes per your selection.
Options:
- Average — Displays the data in the table by the average values of TLS fingerprints hits for the selected time filter
- Last — Displays the data in the table by the current first ten TLS fingerprints, per the last sample in the configured time frame.
- Max — Displays the data in the table by the maximum 10 values per parameter for the selected time filter.
- Total — Displays the data in the table by the total number of TLS fingerprints hits for the selected time filter.

Note: If the selected time frame is greater than one (1) hour, the Max option does not display and is not available.

Default: Average
By default, the top five (5) items are selected, and you can scroll the table to see the remaining

items. You change the selected items and choose up to 10 items.

To select which traffic units to display

- From the Units drop-down list, select the traffic units to display: bps (bits per second) or tps (transactions per second), The display changes per your selection.

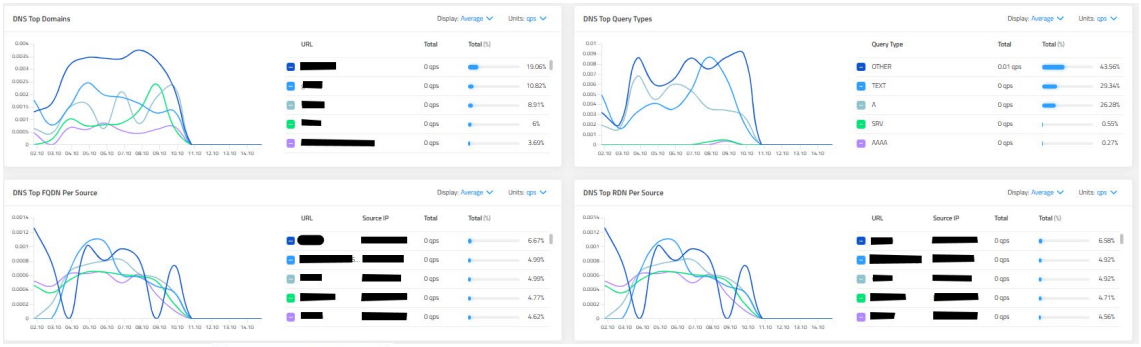
To remove/include individual statistics in the statistics display

By default, all statistics display. You can remove/include individual statistics to display:

1. To remove a statistic, click the label of that statistic. The label is grayed out and the statistic is removed.
2. To include a statistic, click the grayed-out label of that statistic. The statistic displays.

DNS Analytics

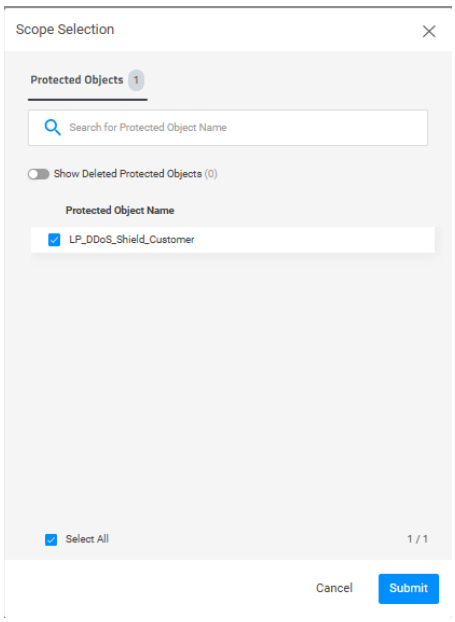
The DNS Analytics dashboard displays the list of the top ten (10) DNS requests according to the chosen display option (Average, Last, Max, Total), and always at least the last attack point.



1. Click the 

box on the dashboard toolbar to open the Protected Objects dialog box.
2. In the Search for Protected Object Name text box, type a relevant value to narrow your search.
3. Select the option button next to the item that you require.
   - If you select only one protected object, the protected object name displays to the right of the 

box.
   - If you select multiple protected objects, the selected protected objects display at the top of the list in alphabetical order. The remaining unselected protected objects display below the selected protected objects, also in alphabetical order.
4. You can select or deselect all of the protected objects with the Select All () box.
   - If the list is unfiltered, this selects or deselects all of the protected objects. In this case, all of the



protected objects available to the user are represented in the dashboards.
- If the list is filtered, this only selects or deselects the filtered set of protected objects. In this case, only the filtered set of protected objects available to the user is represented in the dashboards, and the Select All box displays as (partial).
- By default, the Protected Objects list includes only the currently configured protection objects. You can select the Show Deleted Protected Objects option.

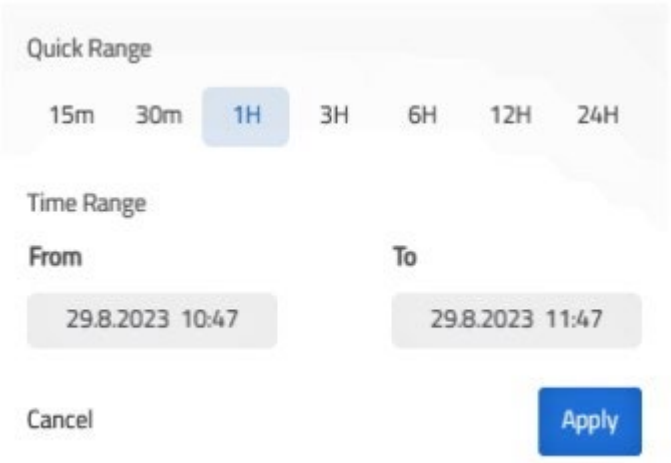
When the Show Deleted Protected Objects option is enabled ( ), the Protected Objects list includes the currently configured protected objects — and also the protected objects deleted manually but still stored in the MSSP Portal database for historical statistical analysis. The names of the protected objects that were deleted manually are displayed in dark red.

5. Click Submit to save the configuration.

The display of the dashboard updates.

To configure the time range for the Top TLS Fingerprints dashboard information
You can configure the time range for the information that dashboard widgets display information. The default time range is 1 hour — that is, from 1 hour ago until now.
The Top TLS Fingerprints dashboard displays the configured time range to the left of the clock button ( ).

1. Click the clock button ( ) on the dashboard toolbar to open the Quick Range dialog box.
2. Do one of the following:
   - Select one of the following preset ranges (Quick Range):
     - 15m — The last 15 minutes
     - 30m — The last 30 minutes
     - 1H — The last hour
     - 3H — The last three hours
     - 6H — The last six hours
     - 12H — The last 12 hours
     - 24H — The last 24 hours

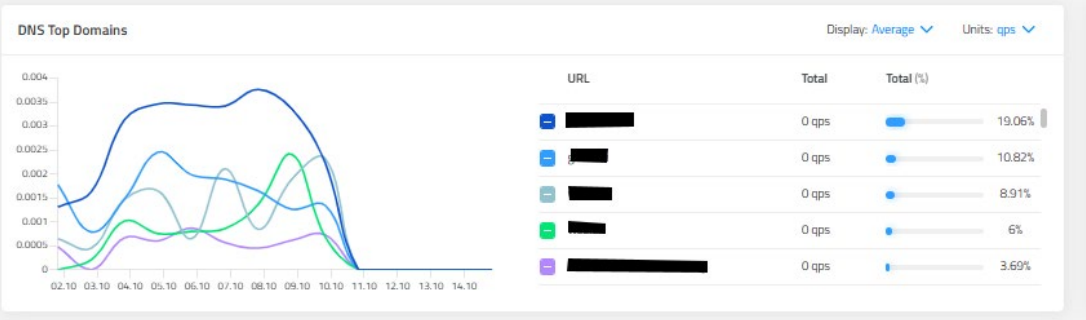


Default: 15m
   - Specify a time range up to one year in the past, using the From and To boxes. You can click in a box to open a month calendar and a 24-hour digital clock. Use the left and right arrows to choose the required month. You can click the 24-hour digital clock to choose the time of day.
3. Click Apply to apply the configuration.

DNS Top Domains

This widget displays the top ten DNS domains per the selected scope and time range for the *DNS*

Analytics dashboard in both graphical and tabular form. To identify an element in the chart and view more information about the element, hover over the relevant element.



DNS Top Domains Statistics

Parameter	Description
URL	The domain URL.
Total	The total DNS traffic by domain.
Total (%)	The percentage of DNS traffic by domain out of the top ten visible requests from all the domains.

To select by which parameter to display the DNS traffic data

- From the Display drop-down list, select the method by which to display the DNS traffic data: Average, Last, Max, Total

The display changes per your selection.

Sort options:

- Average — Displays the average top 100 DNS domains per the qps or bps values, as selected.
- Last — Displays the top 100 DNS domains per the last sample in the configured time frame per the qps or bps values, as selected. Available only when selecting values that are less than 1 hour (raw data index).
- Max — Displays the maximum top 100 DNS domains per the qps or bps values, as selected. Available only when selecting values that are less than 1 hour (raw data index)
- Total — Displays the total top 100 DNS domains per the qps or bps values, as selected.

Note: If the selected time frame is greater than one (1) hour, the Max option does not display and is not available.

Default: Average

By default, the top five (5) items are selected, and you can scroll the table to see the remaining items. You change the selected items and choose up to 10 items.

To select which traffic units to display

- From the units drop-down list, select the traffic units to display: qps (queries per second) or bps (bits per second)

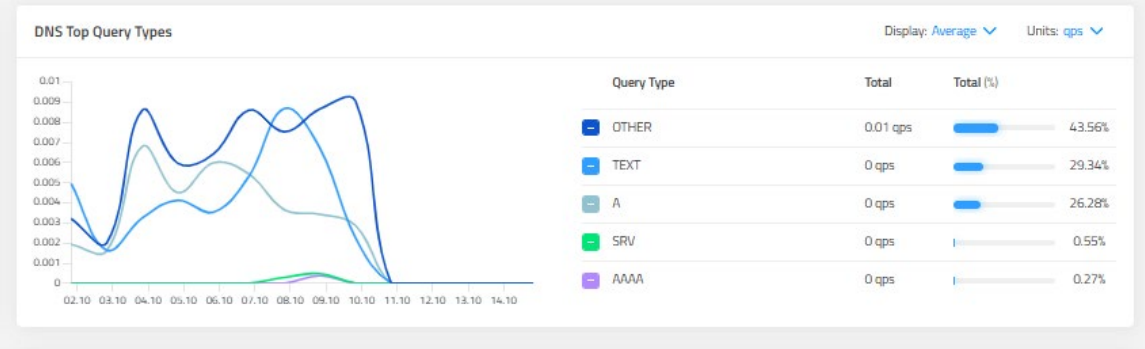
The display changes per your selection.

To remove/include individual statistics in the statistics display
By default, all statistics display. You can remove/include individual statistics to display:

1. To remove a statistic, click the label of that statistic. The label is grayed out and the statistic is removed.
2. To include a statistic, click the grayed-out label of that statistic. The statistic displays.

DNS Query Types

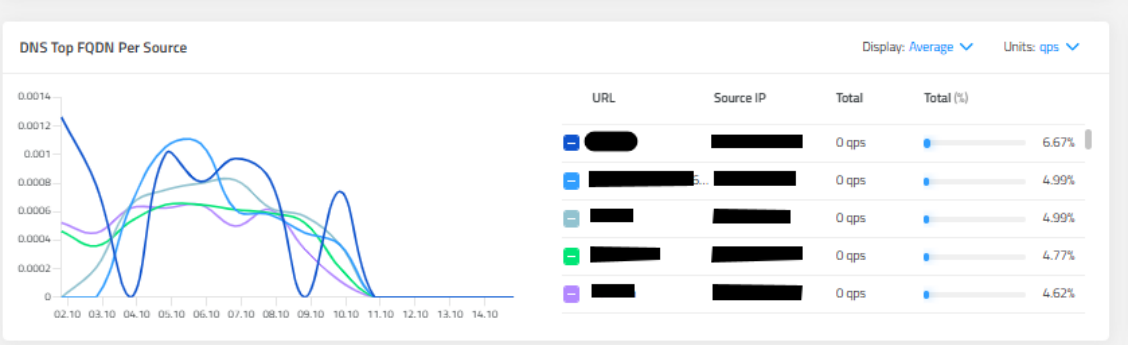
This widget displays the top 100 DNS query types per the selected scope and time range for the DNS Analytics dashboard in both graphical and tabular form. To identify an element in the chart and view more information about the element, hover over the relevant element.



Parameter	Description
Query Type	The DNS query type.
Total	The total DNS traffic by query type.
Total (%)	The percentage of DNS traffic by query out of the top ten visible requests from all the domains.

DNS Top FQDN Per Source

This widget displays the top 100 DNS FQDNs per the selected scope and time range for the DNS Top FQDN Per Source dashboard in both graphical and tabular form. To identify an element in the chart and view more information about the element, hover over the relevant element.

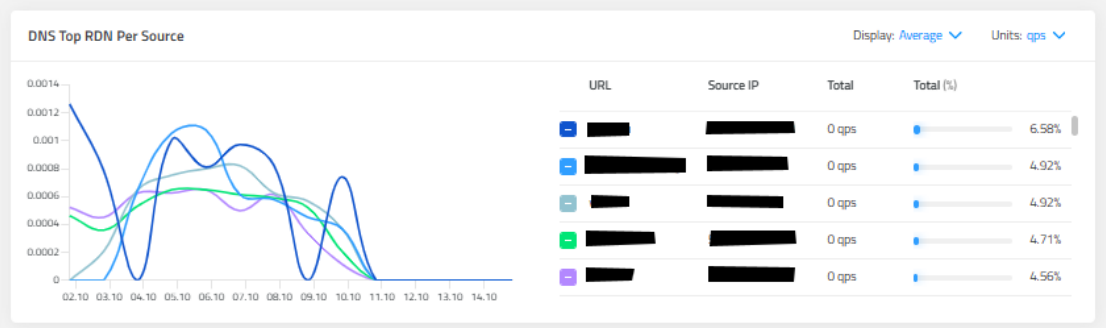


DNS Top FQDN Per Source Statistics

Parameter	Description
URL	The FQDN URL.
Source IP	The source IP address of the FQDN DNS traffic.
Total	The total DNS traffic per FQDN source IP address.
Total (%)	The percentage of DNS traffic per FQDN source out of the total traffic from all the FQDN sources.

DNS Top RDN Per Source

This widget displays the top 100 RDNs per source per the selected scope and time range for the DNS Top RDN Per Source dashboard in both graphical and tabular form. To identify an element in the chart and view more information about the element, hover over the relevant element.



DNS Top RDN's Per Source Statistics

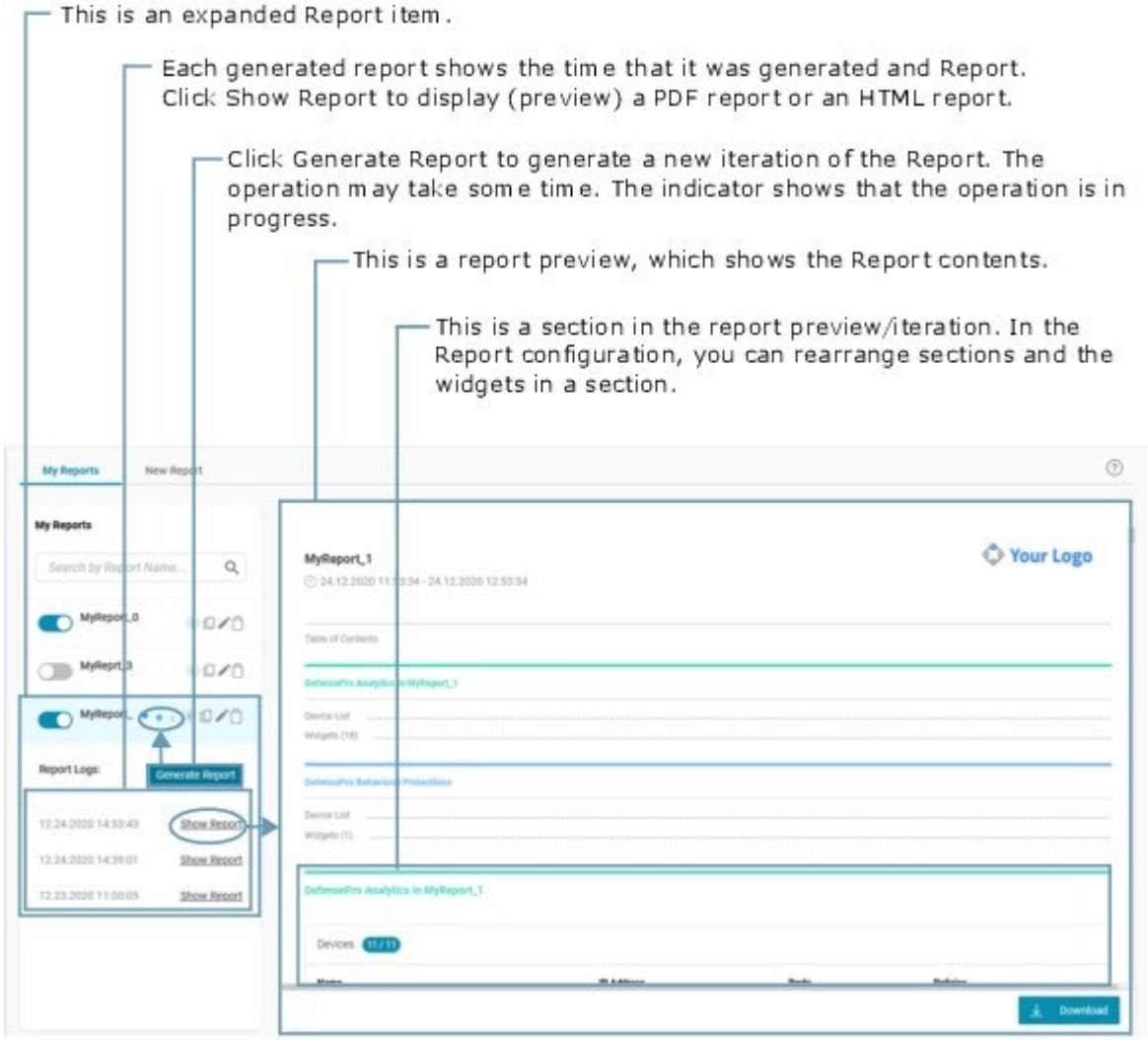
Parameter	Description
URL	The RDN URL.
Source IP	The source IP address of the RDN DNS traffic.
Total	The total DNS traffic per RDN source IP address.
Total (%)	The percentage of DNS traffic by RDN source out of the total traffic from all the RDNs.

MSSP Portal Reporting

Use the Reports module to do the following:

- Create and generate a report and view it on the fly — For example, the content of a single widget of a single Analytics dashboard relating to a specific time range and scope. This is helpful when you want to quickly view data for a single query.
- create and generate complex customized reports — You can create reports with multiple instances of the same widget. For example, you can have one instance of a widget showing packets per second and the other showing bit/s.

Analytics Reports Screen — with Report Item Expanded and Report Preview



My Reports Tab — Managing Existing Analytics Reports

The My Reports tab displays, alphabetically, the Report items.
You can filter the list as required. The text that you enter in the box to filter the list of report items is case-sensitive.

Each row in the My Reports list displays icons for the following basic actions:

- Enable or disable running the Report according to the configured schedule (or respectively).
- View the configuration summary of the Report ( ).
- *Duplicate the Report () to use as a template for a new Report.
- *Edit the configuration of the Report ( ).
- *Delete the Report item ( ).

Click anywhere in a Report row (except for right on an icon) to expand the item and do the following:

- Display (preview) a report that was already generated — Each already generated report shows the time that it was generated and Report. Click Report below the report that you want to preview. Click Download File in the report preview to download an HTML file with the report.
- Generate a new iteration of the Report — Click Generate Now to generate a new iteration of the Report. The operation may take some time. The  indicator shows that the operation is in progress.

New Report Tab — Configuring Analytics Reports

A Report configuration comprises the following:

- Configuring the following general Report Parameters:
  - Report Name — The report name must be unique within an MSSP account. However, an MSSP account can use a report name that is used by another MSSP account.

Notes:
If this is a duplicated Report, the Name of the Report is displayed as Report_Name_copy. You can change the name as required.

  - Executive Summary (optional) — A custom introduction for the report.
  - Logo (optional) — A custom logo for the report.
  - Attack Story (optional) — An Attack Story is a way to view the chronological order of attack events in an illustrative way. When configuring an Attack Story type of report, the Time and Schedule parameters are disabled. An Attack Story is only relevant for the Security Operations template.
    - To enable it, select the Attack Story toggle. When configured and enabled, the Attack Story will run immediately when the attack event on protected objects is finished.
  - Time — The time range for the information that the report contains.

Note: If this is an Attack Story, Time is disabled.

  - Schedule — For example, Daily, where the report runs daily at the specified time.

Note: If this is an Attack Story, Schedule is disabled.

  - Share (Future) — The e-mail recipient(s), subject, and text for the generated reports. If there are no recipients configured, you can generate the report manually and download the HTML output of the report.
  - Format — PDF, HTML, or CSV.
- Configuring the Report contents — The contents of a Report item comprise one or more sections.

The following Templates/dashboards are available, along with their widgets:

- Security Operations — This template is relevant only to Attack Stories, and only displays when you select the Attack Story report. For more details.

Note: Attack Stories are only relevant with a Cyber Controller Plus license.

The Security Operations Template includes the Summary and Attack Story sections. The Summary section includes the following Charts Settings:

- DefensePro Traffic:
  Units: bps, pps
- Mitigation Breakdown:
  Chart Type: Line, Stack
  Units: bps, pps

- DefensePro Analytics — For information about the contents of this dashboard.

Note: When you select DefensePro Analytics Template items to include in Report, there is an additional widget: Attack Statistics Totals. The Attack Statistics Totals widget comprises Total Number of Events, Total Number of Dropped Packets, and Total Dropped Bandwidth. The DefensePro Analytics dashboard does not include a widget called Attack Statistics Totals.

- DefenseFlow Analytics — For information about the contents of this dashboard, see FlowDetector Analytics.

Note: The recommended reports creation mode is to use predefined scheduled reports. During heavy user hours, manual reports generation may take a few more minutes for each user.

To open the configuration of a Report

1. In the MSSP Portal sidebar menu, select Reporting () > Reports.
2. Do one of the following:
   - To create a new Report, select the New Report tab.
   - To edit the configuration of an existing Report, in the My Reports tab, select the item and click the  (Edit) icon.
   - To duplicate a Report to use as a template for a new Report, select the Report and click the  (Duplicate) icon.

To configure the general Report Parameters

1. In the MSSP Portal sidebar menu, select Reporting () > Reports.
2. Select the New Report tab.
3. Click Name, and in the Report Name text box, enter a name for the Report.

Note: If this is a duplicated Report, the Name of the Report is displayed as Report_Name_copy. You can change the name as required.

4. If you require a custom introduction for the report — typically, to be used as an executive summary, do the following:
   a. Click Create a Summary. The Executive Summary dialog box opens.
   b. Type the body text.
   c. Format the text using the provided buttons (). To format text as a hyperlink, select the relevant text and click the  icon to open the Insert Link dialog box and specify the URL.
   d. Click Save. The Executive Summary option is enabled ().

5. For Attack Stories, do the following:
   a. Ensure that the Run immediately when activation is finished toggle is enabled.
   b. Set the following parameters:
   - Min Activation Duration — The minimum total activation time that is required for generating the Attack Story.
   - Values:
     - Units: Sec, Min, Hour, Day
     - Default: 1 minute
     - Min Attack Bandwidth — The minimum single attack bandwidth in activation that is required for Attack Story report generation. Default: 100 Mbps
   - Values:
     - Units: Kbps, Mbps, Gbps
     - Default: 100 Mbps

6. If you require a custom logo for the Report, do the following:
   a. Click Logo.
   b. Click Add Logo (PNG, 100×100).
   c. Browse to and select the 100-pixel × 100-pixel .png file of the logo that you require. The filename is displayed under Logo.

7. Click Time, and do one of the following to configure the time range for the information that the report contains:

Note: Not relevant for Attack Stories.

- From Quick Range tab, select one of the following preset ranges:
  - 15m — The last 15 minutes
  - 30m — The last 30 minutes
  - 1H — The last hour
  - 1D — The last day
  - 1W — The last seven days
  - 1M — The last month
  - 3M — The last three months
  - Today — From 00:00 today
  - Yesterday
  - This Week — From 00:00 Sunday
  - This Month
  - Previous Month
  - Quarter — From the beginning of the current quarter year

Default: 1H

- From the Absolute tab, specify the time range up to one year in the past. You can click in a box to open a month calendar and a 24-hour digital clock. Use the left and right arrows to choose the required month. You can click the 24-hour digital clock to choose the time of day.

Note: When specifying an absolute time range, ongoing attacks are not included in the report.

- From the Relative tab, specify the time range up to one year in the past. Use the Relative tab and specify a time range when the Quick Range options do not suffice. Enter a number in the text box, and select the required time unit.

8. Click Schedule, and turn the Run Report switch ON or OFF, as follows:

Note: Not relevant for Attack Stories.

- OFF — The report runs only when triggered manually.
- ON — The report runs according to the schedule. To configure the schedule, select the frequency, and then, configure the related time and day/date parameters.

Values:

- Daily — The report runs daily at the specified Time of Day.
- Weekly — The report runs at the specified Time of Day, on the specified Days of Week.
- Monthly — The report runs at the specified Time of Day, on the specified Day of Month in the specified Months.
- Once — The report runs one time only at the specified Time of Day, on the specified Day.

Note: Scheduled reports run according to the time as configured on the Cyber Controller server.

9. Click Share, and do the following:
   - Click in the To box, and enter email addresses as required.
   - Click in the Subject box, and enter the text for the Subject line of the email message.
   - Click in the bottom box, and type the message body of the email message.

Note: If there is no recipient configured in the To box, there is no delivery method for the report (but you can generate the report manually and download the HTML output of the report).

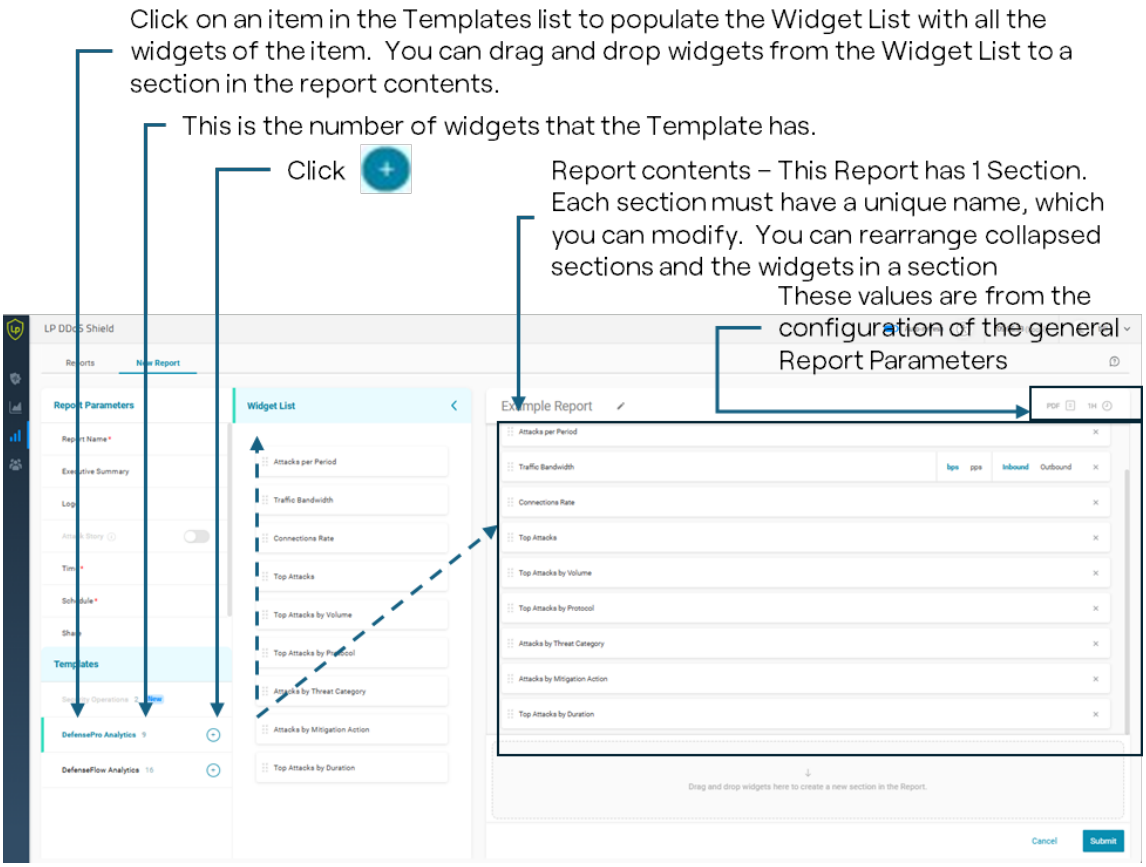
10. Click Format, and select the PDF, HTML, or CSV, as required.

Note: CSV reports contain more-detailed information than PDF or HTML reports. Furthermore, CSV reports can be used by other systems for further analysis.

11. Click Save.

After you have configured the general Report Parameters, configure the Report contents.

Configuring the Contents of a Report



1. Do one of the following:
   - To add the contents of a Template as a new section in the Report contents — In the Templates list, click the icon next to the Template name.
   - To add separate widgets to the Report contents:
     a. In the Templates list, click the template with widgets you want in the report output. The Widget List displays the associated widgets.
     b. From the Widget List, drag and drop widgets to a new section or an existing section of the same Template set.
     c. For widgets that support multiple measurement types (for example Min, Max, Inbound/Outbound or bps/pps), specify the measurements that you require.
     d. For widgets from the DefensePro Analytics template, if required, select the Exclude Malicious IP Addresses option. Enabling this option filters out all the attacks that the ERT Active Attackers Feed module handled, which can improve clarity when the data contains a high percentage of attacks in the Malicious IP Addresses category. This option applies only to widgets that relate to attack data, not to widgets that show statistics.

Notes

- When you select DefensePro Analytics Template items to include in the Report, there is an additional widget: Attack Statistics Totals. The Attack Statistics Totals widget comprises Total Number of Events, Total Number of Dropped Packets, and Total Dropped Bandwidth. The DefensePro Analytics dashboard does not include a widget called Attack Statistics Totals.

- The Security Operations Template includes the Summary and Attack Story sections. The Summary section includes the following Charts Settings:
    - DefensePro Traffic — Units: bps, pps
    - Mitigation Breakdown — Chart Type: Line, Stack
    - Units: bps, pps

2. Repeat step 1 until the Report contains all the contents that you require.
3. To modify the name of a section, click on the name and modify it as you require.
4. To move a widget in a section, drag the widget to the required position.
5. For widgets that support multiple measurement types (for example Min, Max, Inbound/Outbound, bps/pps, or Events/Packets/Volume), specify the measurements that you require.
6. To move a section in the Report contents:
    a. Collapse the section if required (by clicking the down arrow, at the right of the section header).
    b. Drag the section to the required position.

7. For each section, click Protected Objects, and then select the protected objects that the information in the report output relates to.

By default, the Display Scope Selection in Report Output option is enabled (). Turn off this option if you require.

Select the protected objects that the dashboards relate to per one of the following options:

- Select all protected objects to represent in the dashboards:
    - Select the Select All box () to select all of the protected objects.
    - Clear the Select All box () to deselect all of the protected objects.
- Select individual protected objects to represent in the dashboards:
    - Select the box () next to each protected object to represent in the dashboards.
    - Clear the () box next to each protected object not to represent in the dashboards.

After your selection, the Select All box displays as  (partial), and the number of selected protected objects displayed at the bottom right of the dialog box changes accordingly (for example, 6/12).

- Select protected objects from a filtered set of protected objects to represent in the dashboards:
    - In the Search for Protected Object Name text box, type a search value based on a common name or string in the protected object list.
    - From the filtered list, do one of the following:
        - Select the box () next to each protected object to represent in the dashboards.
        - Clear the () box next to each protected object not to represent in the dashboards.
        - Select the Select All box () to select all of the protected objects in the

filtered list.

- Click Submit to save the configuration.

8. Click Submit.

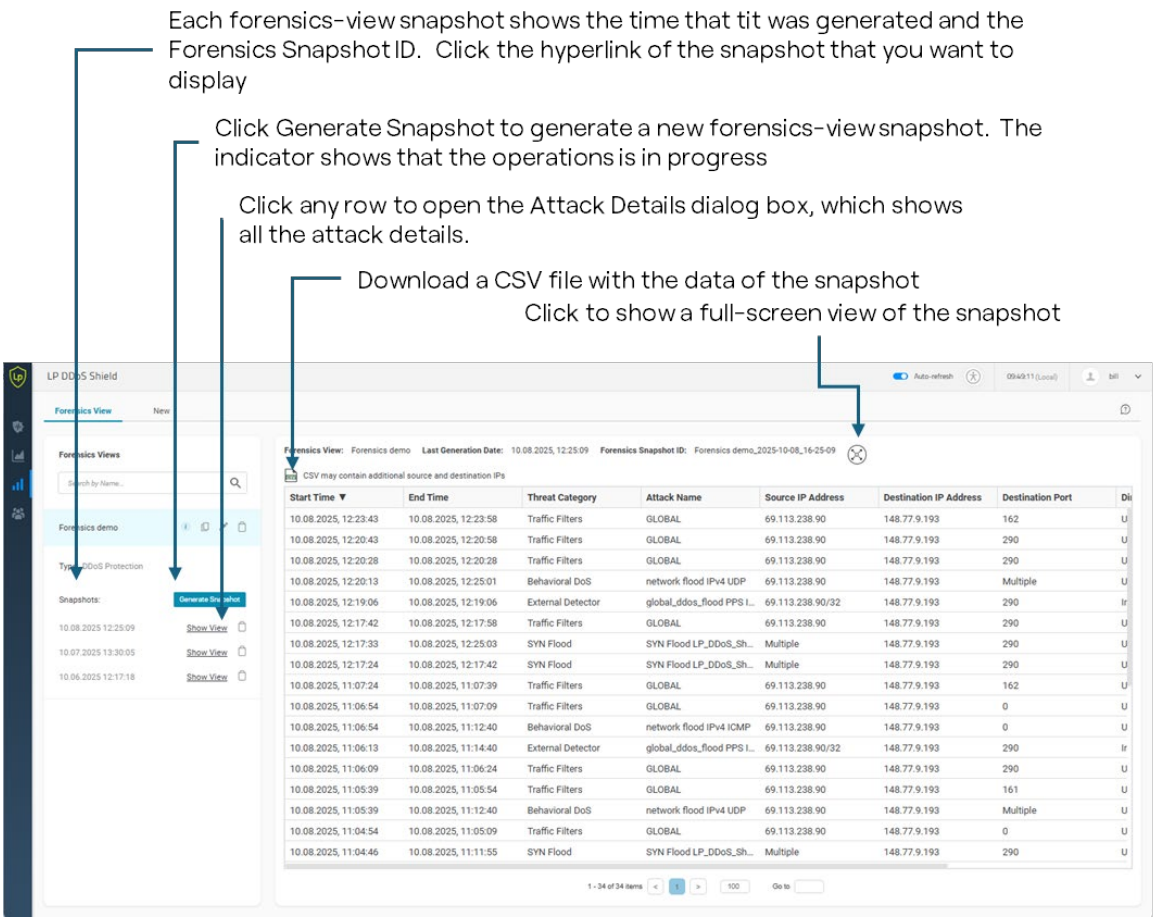
Using Analytics Forensics

Use the Forensics module to analyze and discover the source of security attacks, attack methods and trends, or other problem incidents.

When the Forensics module generates an iteration of a forensics-view, it is referred to as a forensics-view snapshot.

Through the GUI and in CSV files with attack details, a forensics-view snapshot is limited to 10,000 entries. However, in a CSV file, the number of entries without attack details is not limited.

Forensics Screen — Expanded Item with Forensics-View Snapshot



You can configure *forensics views* as required. For information on *using and managing* forensics views that are already configured

The configuration of a forensics view comprises the following main items:

- The name of the forensics view and an optional description

- The devices and scopes
- A time range
- Criteria, based on field values
- The output fields to include in the forensics view
- A schedule (optional)

Creating a Forensics View

1. In the MSSP Portal sidebar menu, select Reporting () > Forensics.
2. Click New. The Forensics View wizard opens.
3. In the Forensics Name box, enter a name for the forensics view.

Note: If this is a duplicated forensics view, the Forensics Name is displayed as Forensics_Name_copy. You can change the name as required.

4. Optionally, in the Description box, you can enter a description of the forensics view.
5. Click Protected Objects, select the protected objects that the dashboards relate to per one of the following options:
   - Select all protected objects to represent in the dashboards:
     - Select the Select All box () to select all of the protected objects.
     - Clear the Select All box () to deselect all of the protected objects.
   - Select individual protected objects to represent in the dashboards:
     - Select the box () next to each protected object to represent in the dashboards.
     - Clear the () box next to each protected object not to represent in the dashboards.

   After your selection, the Select All box displays as  (partial), and the number of selected protected objects displayed at the bottom right of the dialog box changes accordingly (for example, 6/12).
6. Click Time, and do one of the following to configure the time range for the information that the forensics view contains:
   - From Quick Range tab, select one of the following preset ranges:
     - Today — From 00:00 today
     - Yesterday
     - This Month
     - 1D — The last 24 hours
     - 1W — The last seven days
     - 1M — The last month
     - 3M — The last three months
     - 1Y — The last 365 days

   Default: 1D
   - From Absolute tab, specify the time range up to one year in the past. You can click in a box to open a month calendar and a 24-hour digital clock. Use the left and right arrows to

choose the required month. You can click the 24-hour digital clock to choose the time of day.

Note: When specifying an absolute time range, ongoing attacks are not included in the report.

- From the Relative tab, specify the time range up to one year in the past. Use the Relative tab and specify a time range when the Quick Range options do not suffice. Enter a number in the text box, and select the required time unit.

7. Click **Criteria** and do the following:
   a. From Attribute drop-down list, select the attack parameter/attribute, click the right-arrow and select the operator (Equals or Not Equals), and select or specify the Attribute Value.

The attribute value depends on the attack parameter that you select. In addition, there may be an additional parameter to select. For example, if you select the attack parameter Source Port, you also select Port or Port Range. Then, if you select Port Range, you must specify the From and To values.

The following attack parameters are available:

- Action
- Attack Name
- Attack Rate in bps
- Attack Rate in pps
- Destination IP
- Destination Port
- Direction
- Duration
- Max pps
- Packet Type
- Protocol
- Risk
- Source IP
- Source Port
- Threat Category

Note: When you select Destination IP and/or Source IP and there are multiple results for a specific attack, the Forensics module will also analyze the Sampled Data of each multiple-source/destination attack. This process enriches the snapshot with all the requested IP addresses that were part of the sample information of the attack.

   b. Click Add New Condition. The condition is displayed in the Conditions list, with a number displayed on the row.
   c. Repeat step a and step b to configure more conditions, as necessary.
   d. Select one of the following Apply To option buttons:
      - All Conditions — The forensics view uses a Boolean AND for the rows in the Conditions list.
      - Any Condition — The forensics view uses a Boolean OR for the rows in the Conditions list.

Caution: If you select either Destination IP and/or the Source IP as conditions, you should only set

Apply To Any Condition if you are comparing more than one IP address.
In all other cases, if you have selected at least one destination IP address or source IP address and another condition that is not an IP address, do not set Apply To Any Condition. Per the behavior of the IP address conditions, any other conditions you might have selected are ignored, which will not produce the results you may be expecting.

- Custom — The forensics view uses the user-defined Boolean expression for the rows in the Conditions list. You can use the number displayed on the row to represent a condition. Example: (1 AND 2) OR (3 OR 5) AND 6)

8. Click Output and select which fields to include in the forensics view.
   The following output fields are available:
   - Action
   - Device Type
   - Device Name
   - Workflow Rule Process
   - Activation ID
   - Attack ID
   - Attack Name
   - Destination IP Address
   - Destination Port
   - Device IP Address
   - Direction
   - Duration
   - End Time
   - Footprint
   - Max Attack Rate
   - Max pps
   - Packet Type
   - Physical Port
   - Policy Name
   - Protected Object
   - Protocol
   - Radware ID
   - Risk
   - Start Time
   - Source IP Address
   - Source Port
   - Threat Category
   - Total Mb
   - Total Packets
   - VLAN Tag

9. Click Schedule, and turn the Run Report switch (that is, running forensics view) ON or OFF, as follows:
   - OFF — The forensics view runs only when triggered manually.
   - ON — The forensics view runs according to the schedule. To configure the schedule, from the Run drop-down list, select the frequency, and then, configure the related time and

day/date parameters.

Values:

- Daily — The forensics view runs daily at the specified Time of Day.
- Weekly — The forensics view runs at the specified Time of Day, on the specified Days of Week.
- Monthly — The forensics view runs at the specified Time of Day, on the specified Day of Month in the specified Months.
- Once — The forensics view runs one time only at the specified Time of Day, on the specified Day.

Note: Scheduled forensics views run according to the time as configured on the Cyber Controller client.

10. Click Format and select the format of the file with the forensics-view snapshots: HTML, CSV, or CSV with Attack Details.

If you select CSV with Attack Details, the Include All Signatures and Fingerprints check box displays. Select this check box to include the following additional CSV files in addition to the main attack details file:

- A CSV file with the signature information
- A CSV file with the list of fingerprints per attack, including the following anomalous details:
  - Attack ID
  - Fingerprint
  - Fingerprint Alias
  - Category
  - Action
  - Client Profile
  - Max hits (hps)
  - Fingerprint Baseline (hps)
  - Peacetime Portion %
  - Start Time
  - End Time

Notes

- If the Format is CSV with Attack Details, the information in the main attack details file is limited to 10,000 attacks, including up to the 10 first sampled packets for each attack.
- If the Format is HTML, you can only download the Forensics report via e-mail or SFTP.

11. Click Share, and do the following:
    a. Select the tab with the required format of the content: Email or FTP.
    b. Do one of the following:

- When you select Email, do the following:
  - Click in the To box, and enter email addresses as required.
  - Click in the Subject box, and enter the text for the Subject line of the email message.
  - Click in the bottom box, and type the message body of the email message.
- When you select FTP, do the following:
  - Click in the Hostname/IP box, and enter the hostname or IP address of the FTP server.

- Click in the Path box, and enter the path on the FTP server to place the forensics-view snapshots.
- Click in the User name box, and enter the username for connecting to the FTP server.
- Click in the Password box, and enter the password for the FTP server.

12. Click Submit.

Using and Managing Existing Forensics Views

The Forensics screen displays, alphabetically, a list of the forensics-view items that you configured

Caution: The text that you enter in the box to filter the list of forensics-view items is case-sensitive.
Each row in the Forensics Views list displays icons for the following basic actions:

View the configuration summary of the item ( ).

- Duplicate the item ( ) to use as a template for a new forensics-view.
- Edit the configuration of the item ( ).
- Delete the item ( ).

Click anywhere in a forensics-view row (except for right on an icon) to expand the item and do the following:

- Display an existing (already generated) forensics-view snapshot — Each snapshot shows the time that it was generated and the Forensics Snapshot ID. Click the identifier of the snapshot that you want to display.
- Download a CSV file with the data of the forensics-view snapshot — Click (Download CSV) in the snapshot display to download the file.
- Note: Timestamps in Forensics CSV files are in the UTC time zone.
- Generate a new snapshot of the forensics-view — Click Generate Now to generate a new forensics-view snapshot. The operation may take some time. The indicator shows that the operation is in progress.
- Each forensics-view snapshot can contain a maximum of 10,000 entries.
- If the number of entries in a forensics-view snapshot exceeds the maximum, the Forensics module displays the Generate Full Snapshot button.
- To get the full snapshot, click Generate Full Snapshot. When the process completes, click (Download). The full snapshot is contained in a .zip file, which you can extract using 7-Zip or WinRAR.

Caution: Clicking Generate Full Snapshot when the number of entries greatly exceeds 10,000 may overload system resources and cause unexpected behavior. To avoid such a situation, Radware recommends refining the configuration of the forensics-view as much as possible — for example, with a narrower scope, smaller time range, or additional criteria.

Each row in a forensics-view snapshot shows details of the security event (that is, the attack) with the parameters that you specified in the Output step of the Forensics View wizard.
Click in a row of a forensics-view snapshot to do the following:

- Open the Attack Details dialog box, which shows all the attack details.

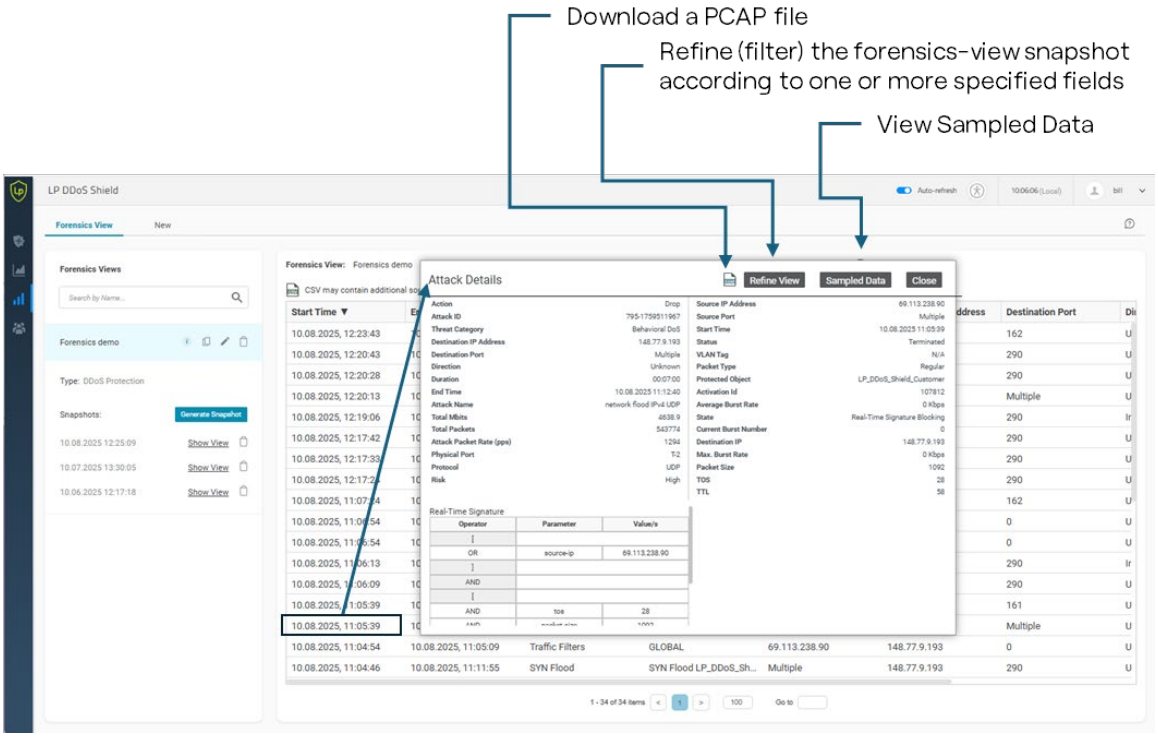
- Download a PCAP file with sampled captured packets — Click (Download PCAP) to download the file.

Notes

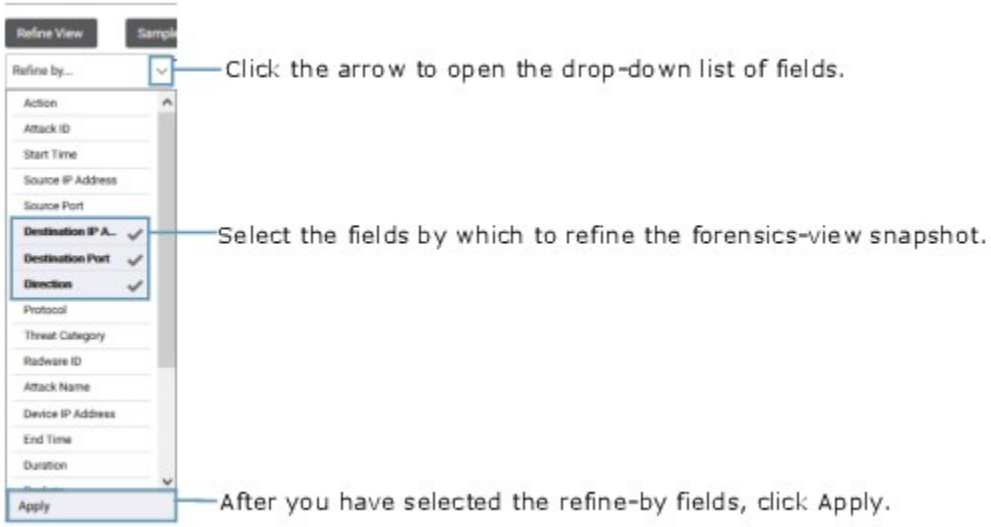
- You can send the PCAP file to a packet analyzer.
- Up to 255 bytes of packet information is saved in the CAP file. That is, DefensePro and/or DefenseFlow export full packets but MSSP Portal trims them to 255 bytes.
- Creation of a PCAP file is possible only if packet reporting is enabled in the configuration of the protection profile that detected the attack.
- DefensePro exports only the last packet in a sequence that matches the filter. Furthermore, if traffic matches a signature that consists of more than one packet, the reported packet will not include the whole expression in the filter.
- For DoS attacks of very short duration, there might be no sampling or ongoing traps. Consequently, for such attacks, there might be no sampled data or capture files.

- Refine (filter) the forensics-view snapshot according to one or more specified fields — This action refines the criteria that is specified in the Criteria step of the Forensics View wizard. Do this to drill down and discover the source of security attacks, attack methods and trends, or other problem incidents. To configure and apply the filter, click Refine Data, click the arrow to open the drop-down list of fields, select the required fields, and click Apply. Click (Clear Filter) to clear the filter and go back to the unfiltered attack details.
- View sampled data and download a PCAP file of the data — Click Sampled Data to open the Sampled Data dialog box. Click (Download PCAP) to download a PCAP file with the sampled data. Click Attack Details to go back to the Sampled Data dialog box. Click Close to go back to the forensics-view snapshot.

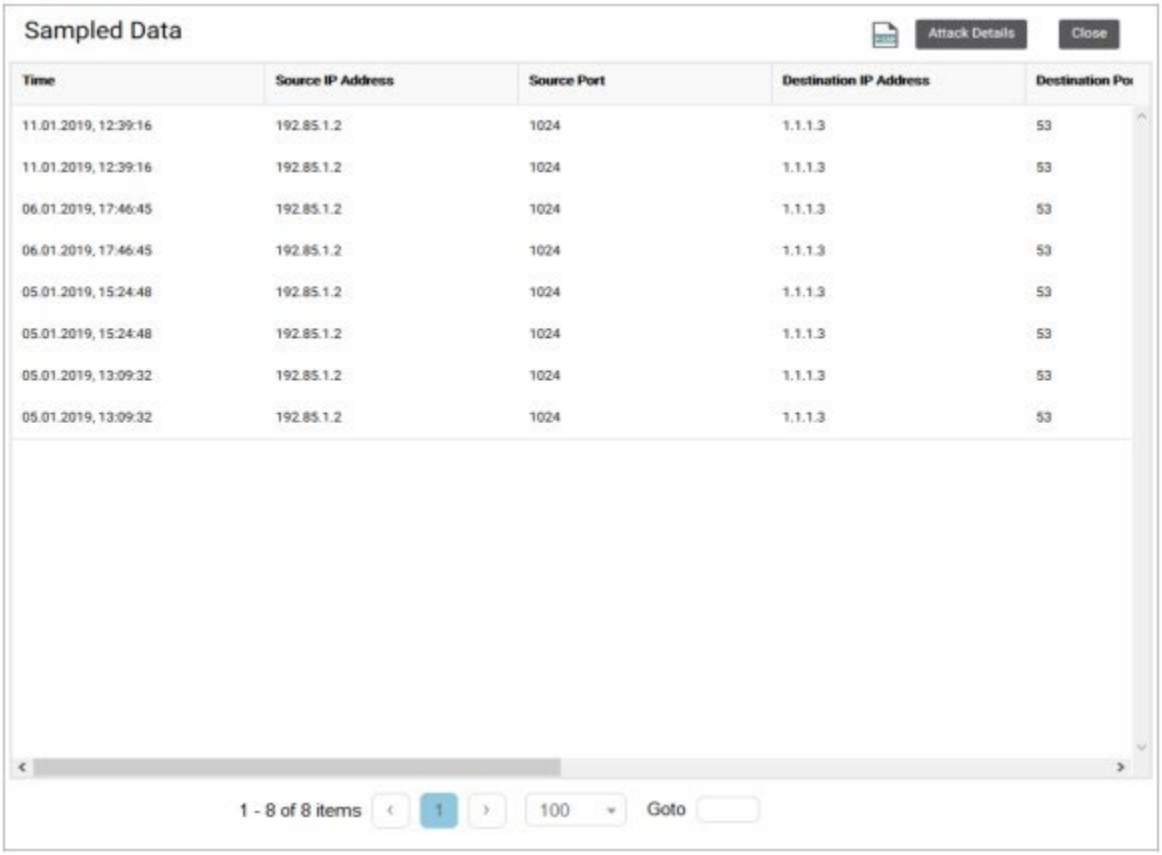
Attack Details Dialog Box from a Forensics-View Snapshot



Refining the Forensics-View Snapshot



Sampled Data Dialog Box



User Management

A user with the Tenant Admin role can create more users (from all MSSP roles) that will be part of his account group. This section explains how to display user information in the User Management pane, create a new user, or edit an existing user.

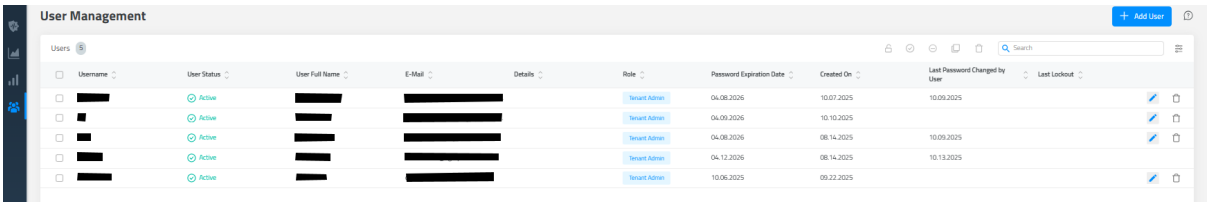
Note: If the MSSP operator has set authentication mode to a third party (not local), the Tenant admin will not be able to create users and will not be able to access the MSSP User Management page.

This section includes:

- Displaying the User Management Pane
- Adding New Users
- Actions to Perform in the User Management Table

Displaying the User Management Pane

Select the User Management item ( ) from the MSSP Portal sidebar menu. The User Management pane opens. The User Management table displays information for each MSSP user.



User Management Table – Parameters

Parameter	Description
Username	The username used for login.
User Status	User status: *Active — The user is allowed to log in to the system. *Inactive — The user is not allowed to log in to the system. *Locked — The user is locked out because of too many password retries.
User Full Name	Full name of the user.
E-mail	E-mail address of the user or operator
Details	Free text user details.
Role	The user's role Values: *Tenant Admin — The user has both monitoring and administrator rights. A user with administrator rights can manage the users defined for his account. *Tenant User — The user can monitor only himself, and can only modify his own settings. *Tenant Viewer — The user can only view the dashboards and create reports. He has no access to do actions
Password Expiration Date	Expiration of the user's password
Created On	Date the user was created
Last Password Change	Last time the user's password was changed
Last Lockout	Last time the user was locked out
Edit User	You can edit the user parameters from the User Management table. Note: A Tenant Admin cannot edit his own user entry. The Edit button is disabled for his user entry. To edit the user parameters, click the (Edit) button for the user. The Edit User dialog box displays

Adding New Users

1. Click 

at the top right of the pane.
2. Set the parameters as required:

Parameter	Description
Username	Mandatory. The username used for login.
User Full Name	Full name of the user.
E-mail	Mandatory. E-mail address of the user or operator. Note: Not used with TACACS+ user authentication.
User Role	Mandatory. The user's role. Values: Tenant Admin — The user has both monitoring and administrator rights. A user with administrator rights can manage the users defined for his account. Tenant User — The user can monitor only himself, and can only modify his own settings. Tenant Viewer — The user can only view the dashboards and create reports. He has no access to do actions.
Password	Mandatory. The user's password. Note: Not used with TACACS+ user authentication
Confirm Password	Mandatory. Verification of the user's password (must be the same as Password).
Details	Free text user or operator details.
Password Policy Note: The password policy is controlled by Lightpath	
Password change on next login	Forces the user to change his password on his next login.
Allow login only from this IP Address	Allow login only from a particular IP address. Enter the IP address in the text field.
Permissions and Access	
Network Analytics Page	If selected, displays the *Network Analytics* menu option in the user's menu. If deselected, hides the *Network Analytics* menu option from the user's menu. Selected by default. Note: This check box displays in the Add/Edit User dialog box only if DDoS Shield Premier
Extended Analytics Package	When the Network Analytics Page check box is selected, this check box becomes available. Selected by default. Note: This check box displays in the Add/Edit User dialog box only if DDoS Shield Premier If deselected, hides the *DefensePro*, *Application Analytics*, and *DNS*

	Analytics tabs from the *Network Analytics* pane, and hides the *Attack Analytics* tab from the Info details for Security Operations detection events.
Security Operations Page	If selected, displays the *Security Operations* page in the user's menu. Selected by default. If deselected, *Security Operations* does not display in the MSSP portal menu.
Reporting Pages	If selected, displays the Reports, Forensics, and Alerts in the *Reports* menu in the user's MSSP Portal menu. Selected by default. If deselected, *Reporting* does not display in the *Reports* menu in the MSSP portal menu.

3. Click Submit to save the new user. New users are added to the *User Management* table.

Actions to Perform in the User Management Table

Sorting Table Columns

1. Click the heading for a column you want to sort.
2. Select the down arrow to sort the column in descending order. Select the up arrow to sort in ascending order.
3. Click the heading to reset the column sorting.

Removing, Adding Columns from the Display

1. Click the  icon at the top far right of widget.
2. From the drop-down menu, select which columns to hide. The selected column is hidden from the table and the column name in the drop-down menu is grayed out.
3. To redisplay a column, from the drop-down menu, select the grayed-out column name. The column displays and the menu item reverts to blue.
4. To restore the default column display, in the drop-down menu click the Reset button.

Duplicating Existing MSSP Users

You can duplicate an existing MSSP user to use as a basis for creating a new MSSP user.

1. Do the following:
    a. If you do not immediately see the MSSP user that you want to duplicate in the table, search for the MSSP user by typing a string in the search field.

To clear the filter and perform a new search, delete and/or modify the search text.

    b. —When you find the MSSP user you want to duplicate, select the MSSP user and click the (Duplicate) button to open the MSSP user.
2. Edit the parameters for the MSSP user, and then click Submit to save your changes. A new MSSP user is created.

Deleting MSSP Users

Note: A Tenant Admin cannot delete his own user entry. The Delete icon is disabled for his user entry.

1. If you do not immediately see the MSSP user that you want to delete in the table, search for the MSSP user by typing a string in the search field.

To clear the filter and perform a new search, delete and/or modify the search text.

2. When you find the MSSP user you want to delete:
    a. Select the MSSP user you want to delete.

Note: If you want to delete multiple users in one action, you can select multiple users

    b. Do one of the following:
        i. Delete individual MSSP users from the user entry in the User Management table by clicking the (Delete) icon at the far right-end of the user entry.
        ii. With the MSSP user(s) selected, click the (Delete) icon at the top of the User Management table.
    c. At the prompt, click Yes to confirm that you want to delete the MSSP user(s), or click No if you do not confirm you want to delete the MSSP user(s).

Unlocking MSSP Users

An MSSP user is locked if they retried their password too many times.

1. If you do not immediately see the MSSP user that you want to unlock in the table, search for the MSSP user by typing a string in the search field.

To clear the filter and perform a new search, delete and/or modify the search text.

2. When you find the MSSP user you want to unlock:
    a. Select the MSSP user you want to unlock.

Note: If you want to unlock multiple users in one action, you can select multiple users

    b. Do one of the following:
        i. Unlock individual MSSP users from the user entry in the User Management

table by clicking the (Unlock) icon at the far right-end of the user entry.

ii. With the MSSP user(s) selected, click the (Unlock) at the top of the User Management table.

The MSSP users are unlocked.

Activating MSSP Users

You can activate users who were deactivated (not able to log in) by the Administrator.

1. If you do not immediately see the MSSP user that you want to activate in the table, search for the MSSP user by typing a string in the search field.

To clear the filter and perform a new search, delete and/or modify the search text.

2. When you find the MSSP user you want to activate:
   a. Select the MSSP user you want to activate.

Note: If you want to activate multiple users in one action, you can select multiple users.

   b. Do one of the following:
      i. Activate individual MSSP users from the user entry in the User Management table by clicking the (Activate) icon at the far right-end of the user entry.
      ii. With the MSSP user(s) selected, click the (Activate) at the top of the User Management table.

The MSSP users are activated.

Deactivating MSSP Users

You can deactivate users so they will not be able to log in.

1. If you do not immediately see the MSSP user that you want to deactivate in the table, search for the MSSP user by typing a string in the search field.

To clear the filter and perform a new search, delete and/or modify the search text.

2. When you find the MSSP user you want to deactivate:
   a. Select the MSSP user you want to deactivate.

Note: If you want to deactivate multiple users in one action, you can select multiple users

   b. Do one of the following:
      i. Deactivate individual MSSP users from the user entry in the User Management table by clicking the (Deactivate) icon at the far right-end of the user entry.
      ii. With the MSSP user(s) selected, click the (Deactivate) at the top of the User Management table.

The MSSP users are deactivated.

APPENDIX A – DATA RETENTION STRATEGY

Table 10: Data Retention Strategy

Period	Data Granularity
Three days	Raw
Two weeks	Five minutes
Three months	One hour
Six months	One day

APPENDIX B – GLOSSARY

This appendix includes descriptions of important terms and concepts used in this document.

Table 9: Glossary

Term	Description
Account	The customer's account associated with a specific security policy profile and protection plan.
Asset	An object that should be protected by the DDoS mitigation service.
DDoS Attack	A distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. It generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. By way of clarification, DDoS (Distributed Denial of Service) attacks are sent by many persons, or bots.
DefenseFlow	A network-wide DDoS attack detection and cyber command and control application designed to protect networks against known and emerging network attacks that threaten network resource availability.
DefensePro	A real-time, behavioral-based attack mitigation device that protects your infrastructure against network and application downtime, application vulnerability exploitation, malware spread, network anomalies, information theft, and other emerging cyber attacks.
Diversion	Attack traffic diversion from its original path to the scrubbing center. After the filtering, the clean traffic is passed back to its original destination.
Incident	Diversion of a specific asset.
Scrubbing Center	The Operation Center is a Cloud-based scrubbing center, staffed by an emergency response team. The scrubbing center is built of networking and DDoS Attack Mitigation devices used to provide the most efficient extraction of the clear traffic (filtering).
Service Provider	The entity that directly offers the Customer Portal to end-customers. The service provider can manage one or more tenants (accounts).
Site	Represents a customer's site connected to the scrubbing center.
User	A system user. The user might have one of the following privileges: Values for users: User-Dashboard, User-Basic, User-Monitor, User-Admin Values for operators: Operator-Monitor, Operator-Admin.