Introduction to the ExtraHop Web UI

Published: 2019-01-10

The ExtraHop Discover and Command appliances provide access to network activity data through a dynamic and highly customizable Web UI.

This guide provides an overview of the global navigation and controls, fields, and options available throughout the UI.

Supported browsers for the ExtraHop Web UI

The following browsers are compatible with all ExtraHop appliances.

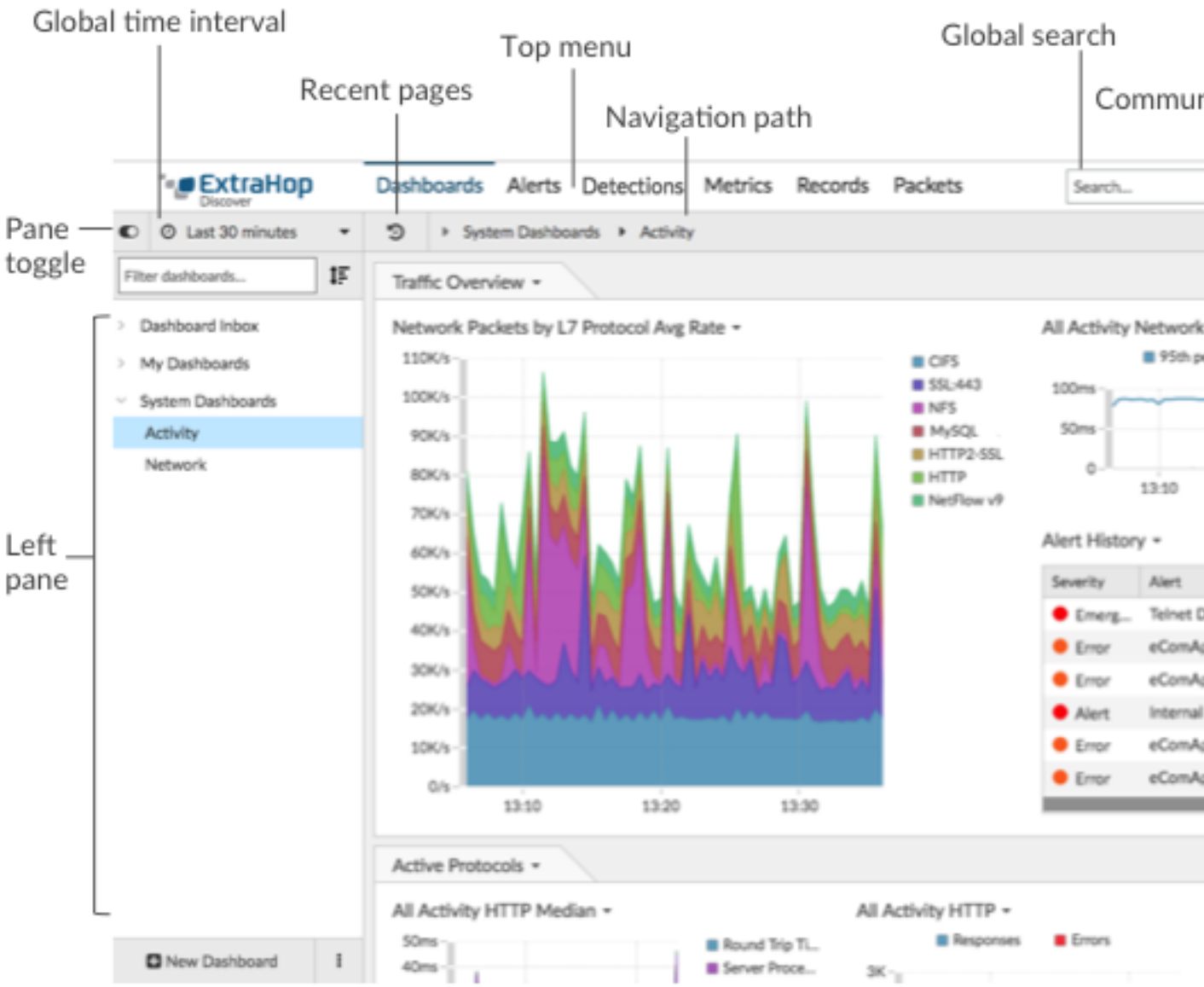
- Firefox
- Google Chrome
- Internet Explorer 11
- Safari

You must allow cookies and ensure that Adobe Flash Player is installed and enabled. Visit the Adobe website to confirm that Flash Player is installed and up-to-date.

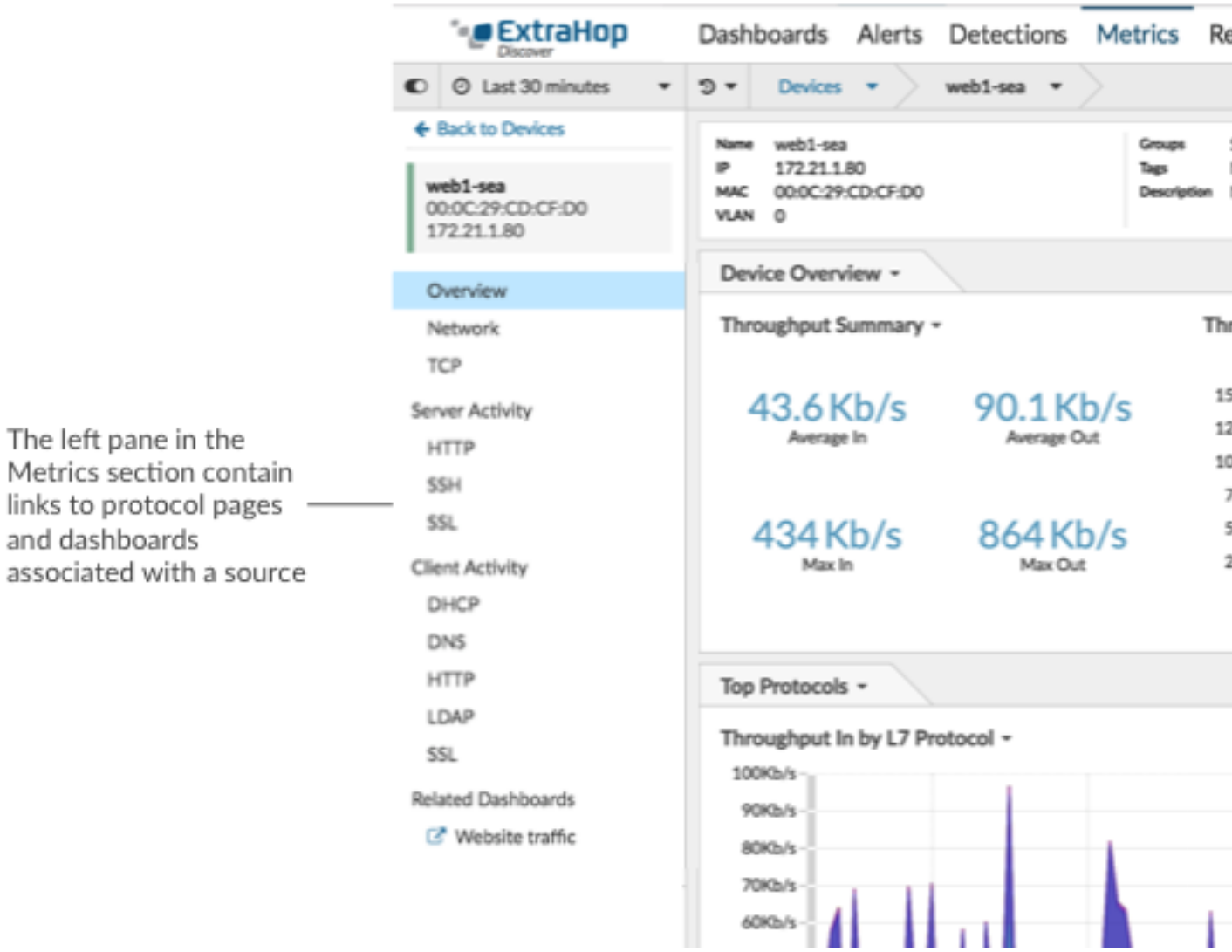
Navigate the Web UI

Global navigation elements located at the top of the page contain links to the main sections of the Web UI. Within each section, the left pane contains links to specific pages or data.

The following figure shows both global and left pane navigation elements.



The following figure shows an example of how the left pane navigation changes based on the section you are viewing.



Here are definitions of each global navigation element:

Dashboards

Click **Dashboards** to view, create, or share dashboards for monitoring any aspect of your network or applications. System dashboards give you an instant view of the activity on your network. You can also create and share custom dashboards with other users.

Alerts

Click **Alerts** to view alert history, which displays information about each alert generated during the time interval.

Detections

If your Discover appliance is connected to the ExtraHop Machine Learning Service, the top level navigation shows the **Detections** menu. Click **Detections** to view detections identified from your wire data. You can access stored detections even if your appliance is disconnected from the Machine Learning Service.

Note: Detections require a connection to the cloud-based ExtraHop Machine Learning Service.

Metrics

Click **Metrics** to find any application, network, or device discovered by the ExtraHop system and view their protocol metrics.

Records

If you have an Explore appliance, the top level navigation shows the Records menu. Click **Records** to query for all records stored on the Explore appliance for the current time interval. Records are structured information about transactions, messages, and network flows.

Packets

If you have a Trace appliance, the top level navigation shows the Packets menu. Click **Packets** to query for all packets stored on the Trace appliance for the current time interval.

Global search field

Type the name of any device hostname or IP address, application, or network to find a match on your Discover or Command appliance. If you have a connected ExtraHop Explore appliance, you can search for saved records. If you have a connected Trace appliance, you can search for packets.

Community forum icon

Visit the ExtraHop forum within a new browser tab to ask a product or bundle question.

Help icon

See help information for the page that you are currently viewing. To access the most current and comprehensive set of ExtraHop documentation, visit the ExtraHop Documentation website.

System Settings icon

Access system configuration options, such as Triggers, Alerts, Reports, and Custom Devices.

User option icon

Log in and log out of your Discover appliance or Command appliance, change your password, and access API options.

Pane toggle

Collapse or expand the left pane.

Global Time Selector

Change the time interval to view application and network activity that was observed by the ExtraHop system for a specific time period. The global time interval is applied to all metrics across the ExtraHop Web UI and does not change as you navigate to different pages.

Recent pages

See a list of the most recent pages you visited in a drop-down menu and make a selection to go back to a previous page. Repeated pages are deduplicated and condensed to save space.

Navigation path

View where you are in the system and click a page name to access a drop-down menu of pivot points, which let you access other protocols or sources.

Command menu drop-down

Click to access specific actions for the page you are viewing. For example, when you click **Dashboards** at the top of the page, the command menu ⋮ provides actions for changing dashboard properties or creating a new dashboard.

Start analyzing data

Begin your data analysis journey with the ExtraHop system by following the basic workflows listed below. As you become familiar with the ExtraHop system, you can complete more advanced tasks, such as installing bundles and building triggers.

Here are some basic ways to navigate and work with the ExtraHop Web UI to analyze network activity.

Monitor metrics and investigate interesting data

When you first log into the ExtraHop system, you see the Activity dashboard. This dashboard is a good starting point because it shows you a summary of important metrics about application performance on your network. When you see a spike in traffic, errors, or server processing time, you can interact with dashboard data to drill down and identify which clients, servers, methods, or other factors contributed to the unusual activity.

You can then continue performance monitoring or troubleshooting by creating a custom dashboard to track a set of interesting metrics and devices.

Search for a specific device and investigate related metrics and transactions

If you want to investigate a slow server, you can search for the server in the ExtraHop system by device name or IP address and then investigate the server's activity on a protocol page. Was there a spike in response errors or requests? Was server processing time too high or did network latency affect the rate of data transfer? Click on different protocols in the left pane to investigate more metric data collected by the ExtraHop system. Drill down by peer IP addresses to see which clients or applications the server talked to.

If you have an Explore appliance, you can investigate entire transactions that the server participated in by creating a record query.

Get visibility into changes to your network by searching for protocol activity

You can get a top-down view of your network by looking at activity groups. An activity group is a collection of devices automatically grouped together by the ExtraHop system based on the protocol traffic observed over the wire. For example, you can find new or decommissioned servers that are actively communicating over a protocol by creating an activity map.

If you find a collection of devices that you want to continue monitoring, you can add a device tag or custom device name to make those devices easier to find in the ExtraHop system. You can also create a custom device group or a custom dashboard to monitor device group activity.

Advanced workflows for customizing your ExtraHop system

After becoming familiar with basic Web UI workflows, you can customize your ExtraHop system by setting up alert notifications, creating custom metrics, or installing bundles.

Set up alerts

Configure threshold and trend-based alerts that notify you when there is a potential issue with a network device. For more information, see Configure threshold alert settings and Configure trend alert settings.

Install a bundle to enhance ExtraHop features and integrations

Bundles are a saved set of system configurations that can be uploaded to an ExtraHop appliance. Check out the following popular bundles:

- Ransomware Detection
- Active Directory v3.0
- AppDynamics Events
- ExtraHop for ServiceNow

Apply a bundle to your ExtraHop system, or create a bundle to share with others. For more information, see Bundles.

Build a trigger to create custom metrics and applications

Triggers are custom scripts that perform an action upon a pre-defined event. Triggers require planning to make sure a trigger doesn't negatively impact system performance. For more information, see Triggers.

Access keyboard shortcuts

Keyboard shortcuts help you quickly navigate across the ExtraHop Web UI and manage dashboards with a few keystrokes.

1. Log into the Web UI on the Discover or Command appliance.
2. Type one of the following keyboard combinations:

Keyboard combinations	Action
?	Show or hide a hot key help menu
G then S	Go to Dashboard
G then A	Go to Alerts
G then P	Go to Application Metrics
G then N	Go to Network Metrics
G then D	Go to Device Metrics
G then G	Go to Group Metrics
/	Global Search
O then H	Open Page History
O then M	Open Metric Explorer
G then E	Go to System Settings
G then T	Go to Trigger Editor
G then H	Open Help
O then Q	View system information
Ctrl+S	Save widget configuration
O then L	Toggle Edit Layout Mode
O then P	Show Dashboard Properties
C then D	Copy the current dashboard
D then D	Delete the current dashboard
O then S	Toggle Descriptions
CTRL+SHIFT+F	Toggle Presentation Mode
N then D	Create a new dashboard
N then F	Create a new folder
O then D	Toggle Edit Dock
P then P	Print or Export to PDF
S then R	Open Scheduled Reports
J	Select the next item on the History
K	Select the previous item on the History

Manage dashboards with keyboard shortcuts

The following keyboard shortcuts only apply to dashboards.

1. Log into the Web UI on the Discover or Command appliance and then click .**Dashboards** at the top of the page.
2. Type one of the following keyboard combinations:

Keyboard combinations	Action
O then L	Toggle edit layout mode
O then P	Show dashboard properties
C then D	Copy the current dashboard
D then D	Delete the current dashboard
O then S	Toggle descriptions
Ctrl+Up Arrow+F	Toggle presentation mode
N then D	Create a new dashboard
N then F	Create a new folder
O then D	Toggle dock edit mode

Related topics

Check out the following guides and resources that are designed to familiarize new users with our top features.

- Introduction to the ExtraHop system
- Monitor website performance in a dashboard
- Monitor DNS errors in a dashboard
- Monitor database health in a dashboard
- Explore metrics in the ExtraHop system to investigate DNS failures
- Query records to find missing web resources
- Build a trigger to collect custom metrics for HTTP 404 errors
- Build a trigger to monitor responses to NTP monlist requests
- Troubleshooting Principles (online training)