

How To's

Published: 2018-11-19

Activity Maps

- [Create an activity map](#)
- [Save and share an activity map](#)
- [Load and manage a saved activity map](#)

Admin

- [Configure a static IP address through the CLI](#)
- [Add a local user account](#)
- [Configure remote authentication through LDAP](#)
- [Configure remote authentication through RADIUS](#)
- [Configure remote authentication through TACACS+](#)
- [Manage imported LDAP user groups](#)
- [Register your ExtraHop appliance](#)
- [Configure the system time](#)
- [Upgrade the firmware on your ExtraHop appliance](#)
- [Connect to Atlas services](#)
- [Create a certificate signing request from your ExtraHop appliance](#)
- [Add a trusted certificate to your ExtraHop appliance](#)
- [Send audit log data to a remote syslog server](#)
- [Configure email settings for notifications](#)
- [Configure settings to send notifications to an SNMP manager](#)
- [Send system notifications to a remote syslog server](#)
- [Configure license expiration notifications for Discover and Command appliances](#)
- [Configure the Discover appliance to collect traffic from NetFlow and sFlow devices](#)
- [Set up shared SNMP credentials for your NetFlow or sFlow networks](#)
- [Save system settings to the running config file](#)
- [Download the running config as a text file](#)
- [Reset the local datastore and remove all device metrics from the Discover appliance](#)
- [Calculate the size needed for your extended datastore](#)
- [Configure an extended CIFS or NFS datastore](#)
- [Archive an extended datastore for read-only access](#)
- [Troubleshoot issues with the extended datastore](#)
- [Create an Explore cluster](#)
- [Connect the Discover and Command appliances to Explore appliances](#)
- [Connect the Discover and Command appliances to the Trace appliance](#)
- [Install the ExtraHop session key forwarder on a Windows server](#)
- [Install the ExtraHop session key forwarder on a Linux server](#)
- [Configure the iDRAC IP address with a monitor, keyboard, and mouse](#)
- [Import external data to your Discover appliance](#)
- [Configure an HTTP target for an open data stream](#)
- [Configure a Kafka target for an open data stream](#)
- [Configure a MongoDB target for an open data stream](#)
- [Configure a raw data target for an open data stream](#)
- [Configure a syslog target for an open data stream](#)
- [Back up a Discover or Command appliance](#)

- [Restore a Discover or Command appliance from a system backup](#)
- [Restore a Discover or Command appliance from a backup file](#)
- [Migrate settings to a new Command or Discover appliance](#)
- [Run a support script](#)
- [Upload a threat intelligence collection to ExtraHop Reveal\(x\)](#)
- [Enable network overlay decapsulation](#)
- [Discover new devices by IP address](#)
- [Integrate ExtraHop with Splunk](#)
- [Increase the capacity of your ExtraHop Explore cluster in VMware](#)
- [Disable record ingest on an Explore cluster](#)

Alerts

- [Configure detection alert settings](#)
- [Configure threshold alert settings](#)
- [Configure trend alert settings](#)
- [Configure an alert to track a custom metric](#)
- [Assign an alert configuration to a source](#)
- [Add a notification to an alert configuration](#)
- [Add Markdown to an alert description](#)
- [Create an exclusion interval for alerts](#)

Applications

- [Create an application through the Web UI](#)
- [Create an application through the Trigger API](#)

Bundles

- [Install a bundle](#)
- [Create a bundle](#)
- [Post a bundle to the ExtraHop website](#)

Charts

- [Create a chart](#)
- [Copy a chart](#)
- [Edit a chart with the Metric Explorer](#)
- [Drill down](#)
- [Export data](#)
- [Display a rate or count in a chart](#)
- [Display percentiles or a mean in a chart](#)
- [Edit metric labels in a chart legend](#)
- [Add a dynamic baseline to a chart](#)
- [Add a static threshold line to a chart](#)
- [Display device group members in a chart](#)
- [Create regular expression filters in a chart](#)
- [Find all devices talking to external IP addresses](#)
- [Monitor a device for external IP address connections](#)

Custom Metrics

- [Create a custom metric](#)

- [Delete a custom metric](#)

Dashboards

- [Create a dashboard](#)
- [Copy a dashboard](#)
- [Display a dashboard in a NOC or SOC](#)
- [Create a dashboard with dynamic sources](#)
- [Edit a dashboard layout](#)
- [Edit a chart with the Metric Explorer](#)
- [Edit a text box widget](#)
- [Edit a dashboard region](#)
- [Change the time interval for a dashboard region](#)
- [Edit dashboard properties](#)
- [Present a dashboard](#)
- [Share a dashboard](#)
- [Share a dashboard with a restricted user](#)
- [Export data](#)
- [Create a PDF file](#)
- [Organize custom and shared dashboards](#)

Detections

- [Connect to ExtraHop Cloud Services](#)
- [Investigate detections](#)
- [Share a detection](#)
- [Troubleshoot your connection to ExtraHop Cloud Services](#)
- [Configure ticket tracking for detections](#)

Devices

- [Find a device](#)
- [Create a device group](#)
- [Create a device group based on discovery time](#)
- [Remove devices from a static device group](#)
- [Change a device name](#)
- [Change a device role](#)
- [Create a tag](#)
- [Add a tag to a device](#)
- [Create a custom device](#)
- [Delete or disable custom devices](#)
- [Migrate pseudo devices to custom devices](#)
- [Prioritize groups for Advanced Analysis](#)
- [Prioritize groups for Standard Analysis](#)
- [Add a device to the watchlist](#)
- [Remove a device from the watchlist](#)
- [Transfer management of analysis priorities for a Discover appliance](#)
- [Specify the locality for IP addresses](#)

General

- [Create a scheduled report](#)
- [Change a scheduled report](#)

- [Disable or delete a scheduled report](#)
- [Export data](#)
- [Create a PDF file](#)
- [Compare time intervals to find the metric delta](#)
- [Zoom in on a custom time range](#)
- [Freeze the time interval to create a custom time range](#)
- [Set a global display theme](#)
- [Enable or disable detection markers](#)

Geomaps

- [Generate a geomap](#)

Packet Capture

- [Configure global packet capture](#)
- [Analyze a packet capture file on the Discover appliance](#)
- [Filter packets with Berkeley Packet Filter syntax](#)
- [Store SSL session keys on connected Trace appliances](#)
- [Download session keys with packet captures](#)

Records

- [Collect flow records](#)
- [Collect L7 records](#)
- [Collect custom records](#)
- [Query for stored records on an Explore appliance from a Discover or Command appliance](#)
- [Enable record queries for custom metrics](#)

REST API

- [Change a dashboard owner through the REST API](#)
- [Create custom devices through the REST API](#)
- [Extract metrics through the REST API](#)
- [Extract the device list through the REST API](#)
- [Tag a device through the REST API](#)
- [Upload STIX files through the REST API to Reveal\(x\)](#)
- [Create a trusted SSL certificate through the REST API](#)
- [Update system health REST API scripts](#)

Triggers

- [Build a trigger](#)
- [Monitor trigger performance](#)