Create a custom device to monitor remote office traffic

Published: 2019-01-08

After deploying the ExtraHop system at your data center, insights about your network quickly emerge. As devices that communicate on your network are automatically discovered by the ExtraHop system, you can start to identify traffic bottlenecks or troubleshoot slow services. But how do you gather insights about important traffic for remote locations outside of your data center?

By creating a custom device, you can easily learn how remote locations consume services and applications. Custom devices act as a place to store metrics for traffic that meets conditions you specify, such as an IP address subnet, a range of ports, or a virtual LAN (VLAN). With a custom device, you can monitor the following types of traffic:

- Remote location traffic, such as branch offices, stores, and clinics.
- Third-party business partner traffic, such as credit card processors and timekeepers.
- "The internet," where you can collect traffic from a range of known public IP addresses such as 8.0.0.0/7.

A custom device only counts as a single device towards your licensed device limit, which is helpful for keeping device counts low. But it's important to note that custom devices affect system performance if they are not configured properly.

This walkthrough shows you how to create a custom device and monitor remote office traffic by completing the following steps:

- Create a custom device for a subnet of branch office devices
- Create a dashboard to monitor bandwidth and latency of branch office traffic

Prerequisites

You must have access to an ExtraHop Discover appliance, and you must have a user account with personal, limited, or full write privileges to create a dashboard.

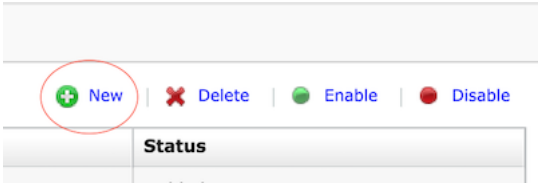
Here are some guidelines about configuring custom devices:

- Avoid creating multiple custom devices for the same IP addresses or ports. Overlapping custom devices might affect system performance.
- Custom devices are unique to a single Discover appliance. You cannot configure a custom device from a Command appliance.

Create a custom device

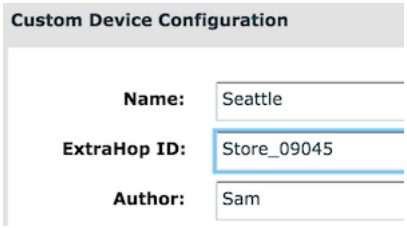
Let's start building a custom device for our Seattle branch office.

1. Log into the Web UI of the Discover appliance and then click the System Settings icon in the top right corner of the page.
2. Click **Custom Devices**.
3. In the upper right corner, click **New**.



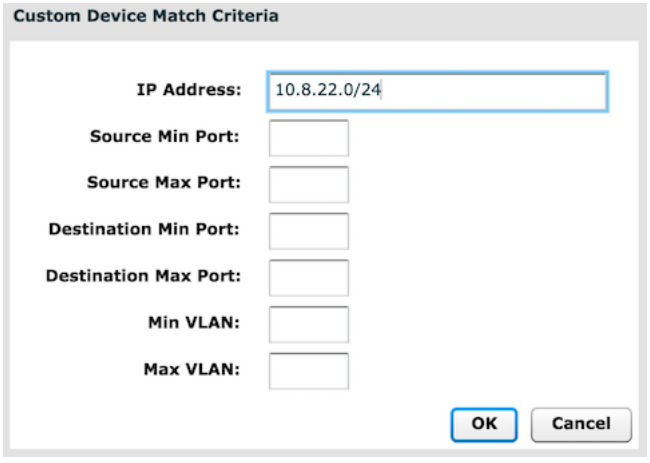
4. In the Name field, type a name for your device. For example, name your device with the branch office region. In this example, we'll name the device, `Seattle`.
5. In the ExtraHop ID field, type information that will help you search for a device. If left blank, the ExtraHop ID is derived from the Custom Device Name, and cannot be changed later.

   Tip: Examples of useful ExtraHop ID include unique identifiers, such as "Store_09045." The ExtraHop ID cannot contain spaces



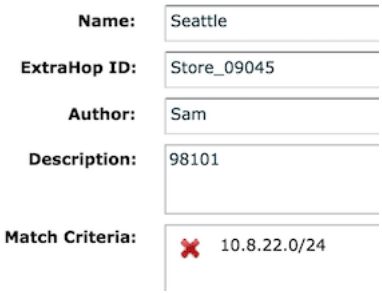
6. In the Description field, type information that will help identify this remote network in future searches. For example, type the branch office address so that you can search for this custom device by city or zip code.
7. In the lower left corner of the Custom Device Configuration page, click **Add Criteria**.

8. In the IP Address field, type a CIDR notation for the Seattle branch office subnet. For this example, we will type `10.8.22.0/24`.



9. You can leave port and VLAN fields blank.
10. Click **OK**.

    The CIDR block now appears in the Match Criteria section of the Custom Device Configuration page.



11. Click **OK** again.

    Note: Add your custom device to the watchlist to make sure your device receives Advanced Analysis.

Your custom device is created! It will take a few minutes for the custom device to discover devices on the remote network. As the ExtraHop system observes traffic that meets the match criteria (for example, the 10.8.22.0/24 subnet), metrics will become available for this custom device.

Next, let's create a dashboard to easily monitor custom device metrics.

Create a dashboard

You can create a dashboard to display specific charts and data for the custom device you created.

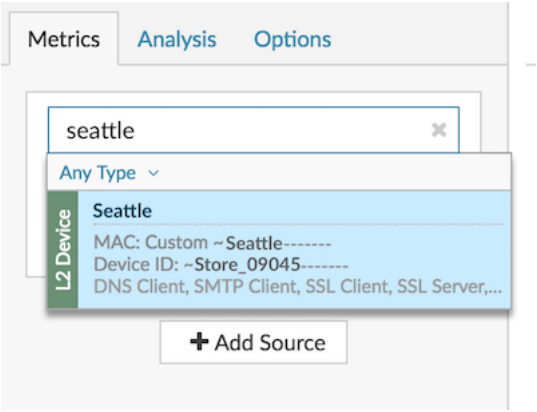
1. Click **Dashboards** at the top of the page and then click **New Dashboard** at the bottom left corner of the page.
2. On the bottom left of the Dashboard page, click **New Dashboard**.
3. In the Title field of the Dashboard Properties window, type a name for your dashboard. For this walkthrough, type `Seattle Branch Office Traffic`.
4. Click **Create**. When you create a new dashboard, a workspace opens in an editable layout mode. This workspace contains a single region and two empty widgets: a chart and a text box.
5. Text box widgets can include custom explanatory text about a dashboard or chart. For this walkthrough, however, we won't be adding text. Delete the text box by completing the following steps:
   a) Click the command menu ⋮ in the upper right corner of the text box widget and click **Delete**.
   b) Click **Delete Widget**.

Next, we'll add throughput metrics about traffic volumes to the empty chart.

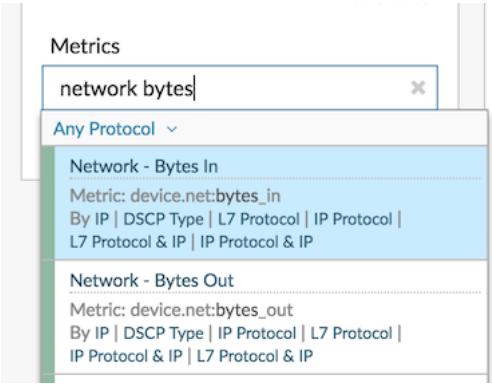
Add network throughput to your dashboard

Let's monitor the amount of network bytes coming into and out of the remote network.

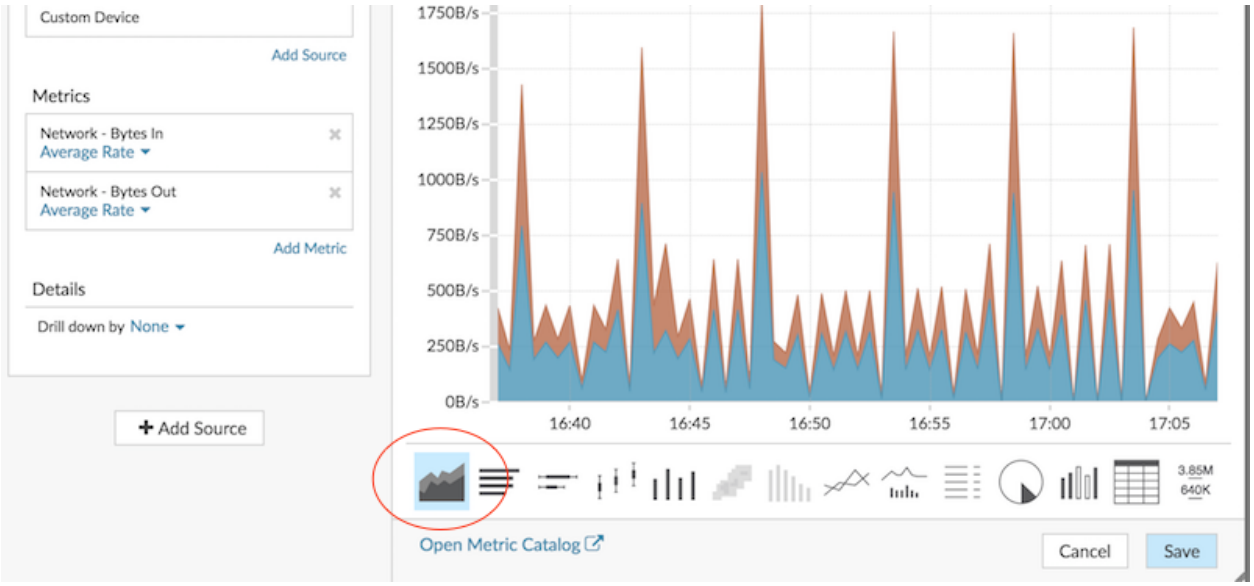
1. Click the empty chart widget in your newly created dashboard to open the Metric Explorer.
2. Click **Add Source**.
3. In the Sources field, type `Seattle` and then select the **Custom Device** from the results, as shown in the following example.



4. In the Metrics field, type `network bytes` to filter the results from all of the available metrics, and then click **Network Bytes In**.



5. Click **Add Metric**, type `network bytes`, and then click **Network Bytes Out**.
6. Click the **Area** chart.



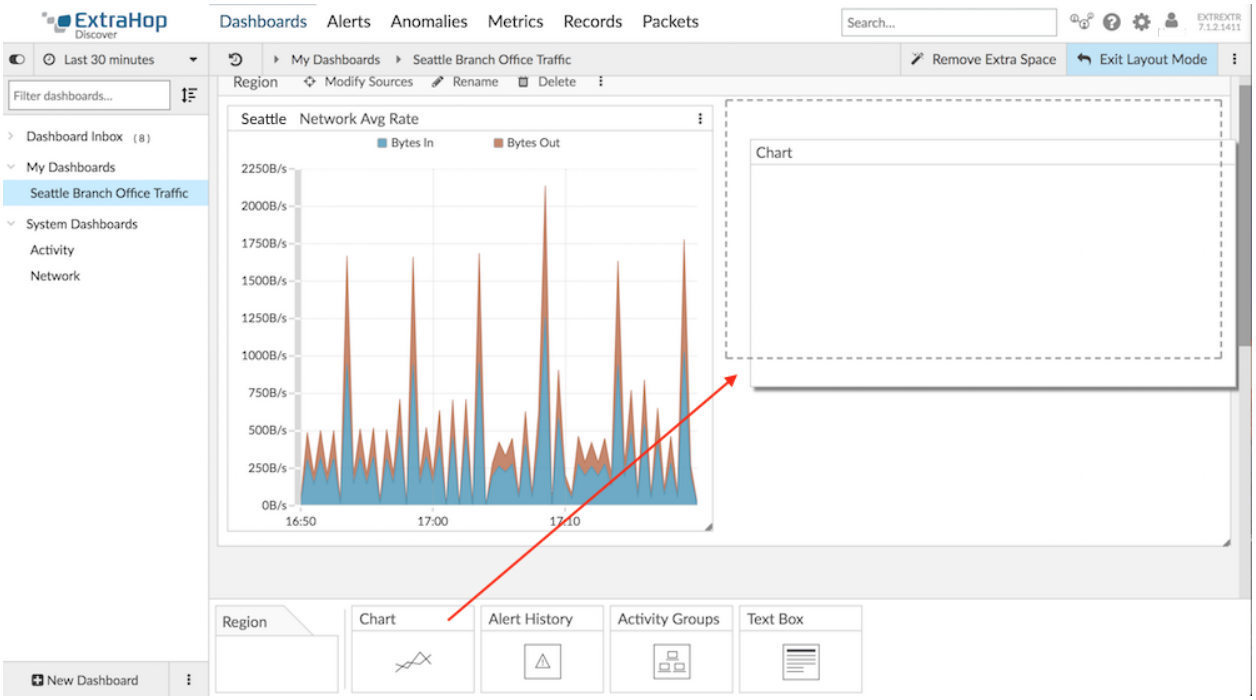
7. Click **Save**.

Next, we'll add the Round Trip Time metric to monitor network latency.

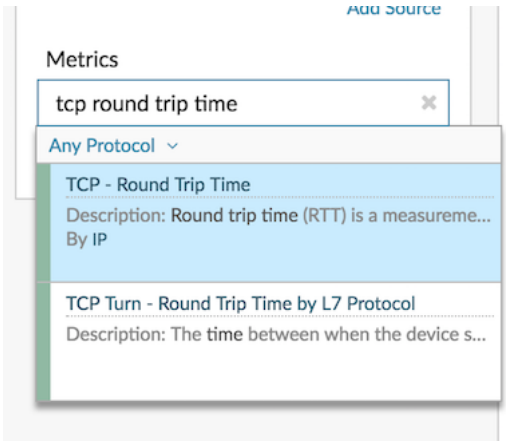
Add network latency to your chart

Now let's now monitor whether network latency is affecting the remote network.

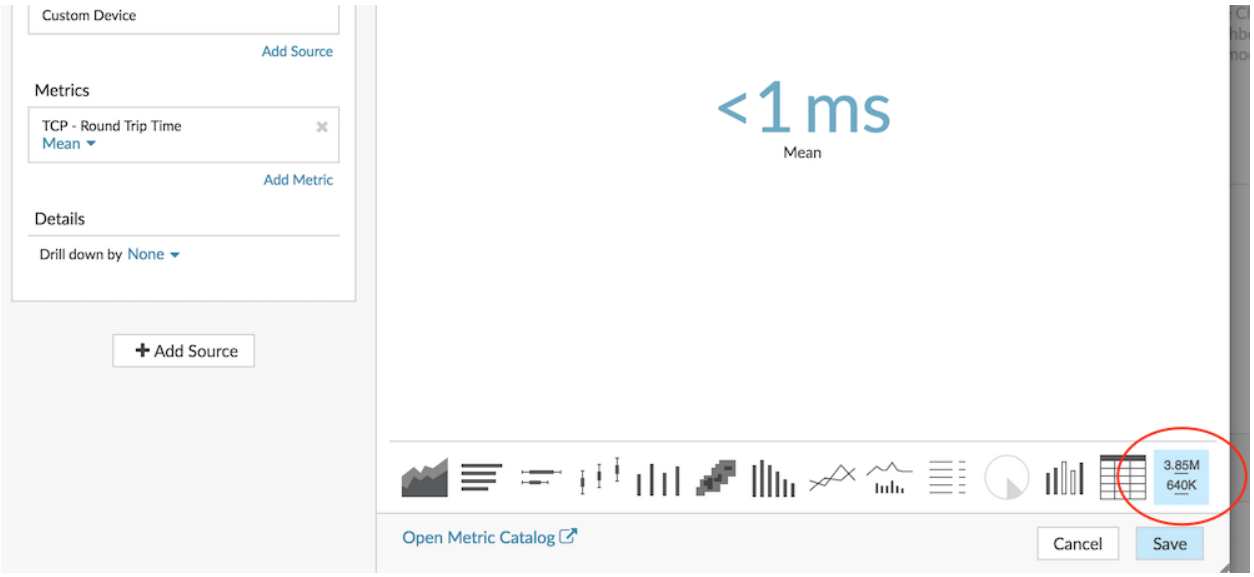
1. From the bottom of the page, click and drag a chart widget into the empty space next to the first chart.



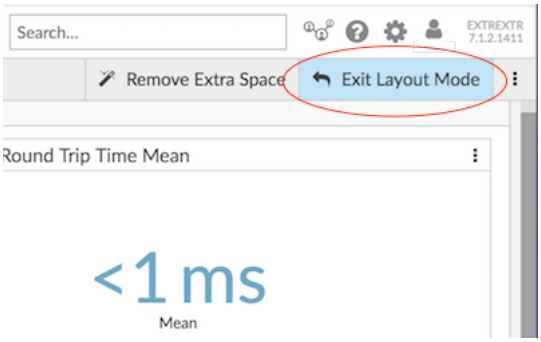
2. Click the empty chart.
3. Click **Add Source** and type `Seattle` and then click **Seattle**.
4. Type `tcp round trip time` to filter results and then click **TCP Round Trip Time**.



5. Click the **Value** chart.



6. Click **Save**.
7. In the upper right corner of the page, click **Exit Layout Mode**.



Your dashboard is complete! You can now keep an eye on network performance by completing the following tasks:

- Share a dashboard
- Add a dynamic baseline to a chart

Troubleshoot issues

You now have a couple of charts to consult when slow network performance is reported. The following table includes suggestions for interpreting chart data and then troubleshooting issues.

Potential Issue	Follow Up Action
A sudden increase in traffic	Investigate dashboard chart data to understand what is contributing to traffic. You can also investigate protocol page data. Click the chart title and then click the custom device name in the Go to... section. A protocol page for the custom device appears. Create an activity map to see device connections and volume of traffic between connections.

Potential Issue	Follow Up Action
	You can also compare two time intervals from different business hours to see the difference in metric values.
Slow application	Determine if the slow application is related to a client-side issue in the branch office, or if the issue is related to servers in the local data center. Click the chart title and then click the custom device name in the Go to... section. A protocol page for the custom device appears. In the Client Activity section in the left pane, click **HTTP**, **Database**, **DNS**, or **ICA** (Citrix) to investigate client-side Error metrics. In the Server Activity section, click protocols and investigate metrics such as Errors and Server Processing Time. These metrics show you that servers might be contributing to the issue.
Increase in traffic volume over time	Add a dynamic baseline to a chart to view trends in traffic data over time. Note that the Discover appliance starts to build a dynamic baseline after it is added to the chart. You cannot view a baseline of historic data.
Increase in network congestion or other data transmission issues	Investigate TCP metrics to see how the network is affecting application performance. Click the chart title and then click the custom device in the Go to… section of the drop-down menu. A protocol page for the custom device appears. Look for large values for the following metrics: • Retransmission Timeouts (RTOs In/Out) for network congestion • Round Trip Time (RTT) for network latency • Receive Window Throttling and Zero Windows for data transmission issues