# Classify IP addresses and trusted domains

Published: 2022-01-05

By providing details about your network specifications, you can improve the metrics and detections generated by your ExtraHop system. The Network Locality page enables you to classify the locality of IP addresses and add trusted domains that your devices regularly connect to.

**Note:** Network Locality settings must be configured on all sensors (Discover appliances) and Command appliances. For Reveal(x) 360, these settings are synchronized across all connected sensors; do not configure these settings on individual sensors.

**Before you begin**
You must have full write privileges to change these settings.

## Specify the locality for IP addresses

By adding a CIDR block to the Network Localities page, you can classify traffic from these IP addresses as internal or external to your network.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **Network Localities**.
3. Click **Add a CIDR Block**.
4. In the Network field, type a single IP address or CIDR block. You must enter a unique range of IP addresses.
5. Select **Internal** or **External**, based on which classification you want to apply to the CIDR block.
6. Optional: In the Description field, type information about why you are configuring the locality of this CIDR block.
7. Click **Save**.
8. To add more entries, click **Add CIDR**.

**Next steps**
Verify that the ExtraHop system no longer classifies an IP address as an external or internal by completing the following steps:

1. Click **Assets** at the top of the page. The Devices page appears, which lists all the protocols with traffic in the selected time interval.
2. From Devices by Protocol Activity, click the device count for TCP. A protocol page appears that displays metrics for every device on your network with TCP activity.
3. In the TCP Connections section, look for changes in the number of External Accepted and External Connected metrics. For example, if you classified a large CIDR block for a remote office as **Internal**, then the number of external connections should be lower.

## Filter IP addresses by locality

You can filter detail metric data by internal or external IP addresses.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Drill down on a metric from a dashboard or protocol page by client, server, or IP address.
   A detail metric page appears that displays metric data listed by IP address.
3. In the trifield filter, click **Any Field** and then click **Network Locality**, as shown in the following figure.

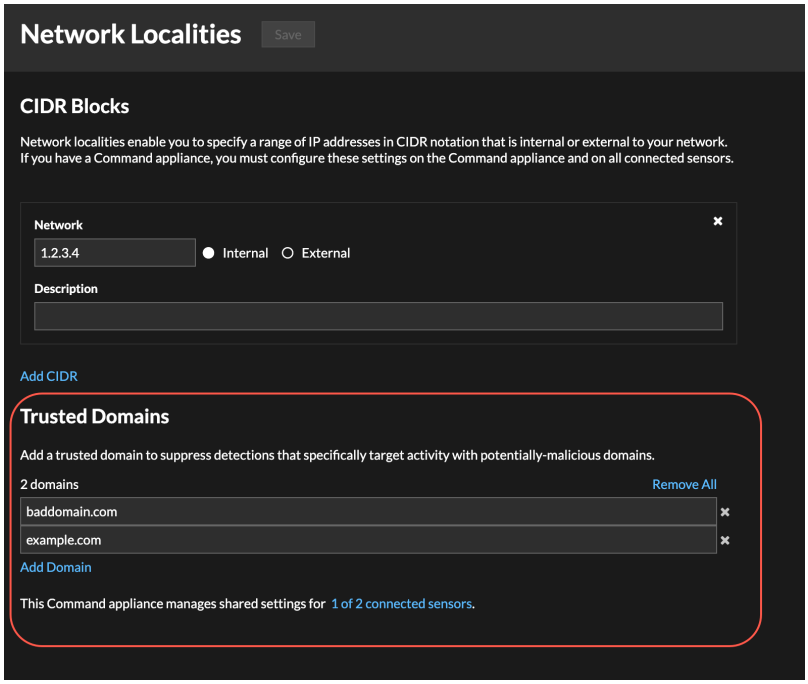

4. Click **All Locations** and then select **Internal** or **External**.
5. Click **Add Filter**.

Detail metric data for internal or external devices is displayed.

## Add a trusted domain

Certain detections are generated when a device makes a connection to an external domain. If you know that a domain is legitimate, add it to the Trusted Domains list, and future detections that target malicious domain activity are suppressed for that domain.

**Note:** If your ExtraHop deployment includes a Command appliance or Reveal(x) 360, and that system is configured to manage tuning parameters, these trusted domains will apply to all connected sensors.




1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. Click the System Settings icon and then click **Network Localities**.
3. Under Trusted Domains, click **Add Domain**.
4. Type a trusted domain name.

   The domain name must be an exact match to the domain you want to suppress. Wildcards and Regex are not supported. To add more than one trusted domain name, click **Add Domain**. Type a single domain name per field.
5. Click **Save**.