Find a device

Published: 2022-09-17

The ExtraHop system automatically discovers devices such as clients, servers, routers, load balancers, and gateways that are actively communicating with other devices over the wire. You can search for a specific device on the system and then view traffic and protocol metrics on a protocol page.

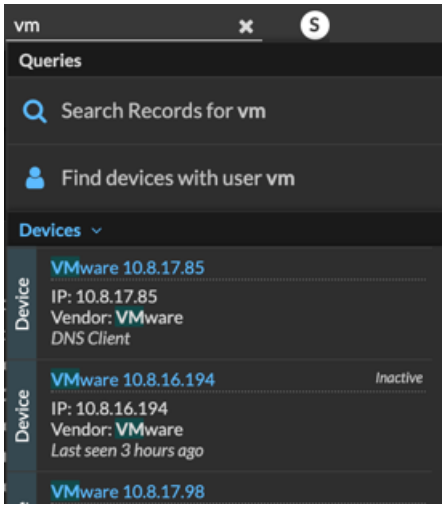
There are several ways to search for a device:

- Find a device from a global search
- Search for a device by details
- Search for devices by protocol activity
- Search for devices accessed by a specific user
- Search for peer devices

Find a device from a global search

You can search for devices from the global search field at the top of the page. Global search compares a search term to multiple device properties such as the hostname, IP address, known alias, vendor, tag, description, and device group. For example, if you search for the term `vm`, the search results might display devices that include `vm` in the device name, device vendor, or device tag.

1. Type a search term in the global search field at the top of the page.
2. Click **Any Type** and then select **Devices**.
   The search results are displayed in a list below the search field. Click **More Results** to scroll through the list.



   Matching devices with no activity during the specified time interval have an Inactive label.

   Tip: Devices inactive for more than 90 days are excluded from global search results. However, you can immediately exclude all devices that have been inactive for fewer than 90 days through the Administration settings.
3. Click a device name to open the Device Overview page and view device properties and metrics.

Search for a device by details

You can search for devices by information observed over the wire, such as IP address, MAC address, hostname, or protocol activity. You can also search for devices by customized information such as device tags.

The trifield search filter enables you to search by multiple categories at once. For example, you can add filters for device name, IP address, and role to view results for devices that match all of the specified criteria.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. At the top of the page, click **Assets**.
3. Click **Devices** in the left pane, and then click the **Active Devices** chart.
4. In the trifield filter, click **Name** and select one of the following categories:

Option	Description
Name	Filters devices by the discovered device name. For example, a discovered device name can include the IP address or hostname.
MAC Address	Filters devices by the device MAC address.
IP Address	Filters devices by IP address in IPv4, IPv6, or CIDR block formats.
Site	Filters devices associated with a connected site. Console only.
Discovery Time	Filters devices automatically discovered by the ExtraHop system within the specified time interval. For more information, see Create a device group based on discovery time.
Analysis Level	Filters devices by analysis level, which determines what data and metrics are collected for a device. You cannot create a dynamic device group for devices filtered by analysis level.
Model	Filters devices by make and model name. The following tips can help you find the device model you want: • Select the exact match operator (=) to view a drop-down list of existing models and model sets. • Select the exact match operator (=) and then select **Custom Models** to filter all devices assigned to a custom model set.
Activity	Filters devices by protocol activity associated with the device. For example, selecting HTTP Server returns devices with HTTP server metrics, and any other device with a device role set to HTTP Server. Also filters devices that accepted or initiated an external connection, which can help you

Option	Description
	determine whether devices are engaged in suspicious activity.
Cloud Account	Filters devices by the cloud service account associated with the device.
Cloud Instance ID	Filters devices by the cloud instance ID associated with the device.
Cloud Instance Type	Filters devices by the cloud instance type associated with the device.
High Value	Filters devices that are considered high value because they provide authentication services, support essential services on your network, or are user-specified as high value.
Currently Active	Filters devices by activity observed on a device in the last 30 minutes.
Network Locality Type	Filters devices by all internal or external network localities.
Network Locality Name	Filters devices by network locality name.
Role	Filters devices by the assigned device role, such as gateway, firewall, load balancer, and DNS Server.
Software	Filters devices by operating system software detected on the device.
Subnet	Filters devices by the subnet associated with the device.
Tag	Filters devices by user-defined device tags.
Vendor	Filters devices by the device vendor name, as determined by the Organizationally Unique Identifier (OUI) lookup.
Virtual Private Cloud	Filters devices by the VPC associated with the device.
VLAN	Filters devices by the device VLAN tag. VLAN information is extracted from VLAN tags, if the traffic mirroring process preserves them on the mirror port. Only available if the `devices_accross_vlans` setting is set to `False` in the Running Config file.
CDP Name	Filters devices by the CDP name assigned to the device.
Cloud Instance Name	Filters devices by the cloud instance name assigned to the device.
Custom Name	Filters devices by the custom name assigned to the device.
DHCP Name	Filters devices by the DHCP name assigned to the device.

Option	Description
DNS Name	Filters devices by any DNS name assigned to the device.
NetBIOS Name	Filters devices by the NetBIOS name assigned to the device.

5. Select one of the following operators; the operators available are determined by the selected category:

Option	Description
=	Filters devices that are an exact match of the search field for the selected category.
≠	Filters devices that do not exactly match the search field.
≈	Filters devices that include the value of the search field for the selected category.
≈/	Filters devices that exclude the value of the search field for the selected category.
starts with	Filters devices that start with the value of the search field for the selected category.
exists	Filters devices that have a value for the selected category.
does not exist	Filters devices that do not have a value for the selected category.

6. In the search field, type the string to be matched, or select a value from the drop-down list. The input type is based on the selected category.

   For example, if you want to find devices based on Name, type the string to be matched in the search field. If you want to find devices based on Role, select from the drop-down list of roles.

   Tip: Depending on the selected category, you can click the Regex icon in the text field to enable matching by regular expression.

7. Click **Add Filter**.
   The devices list is filtered to the specified criteria.

Next steps

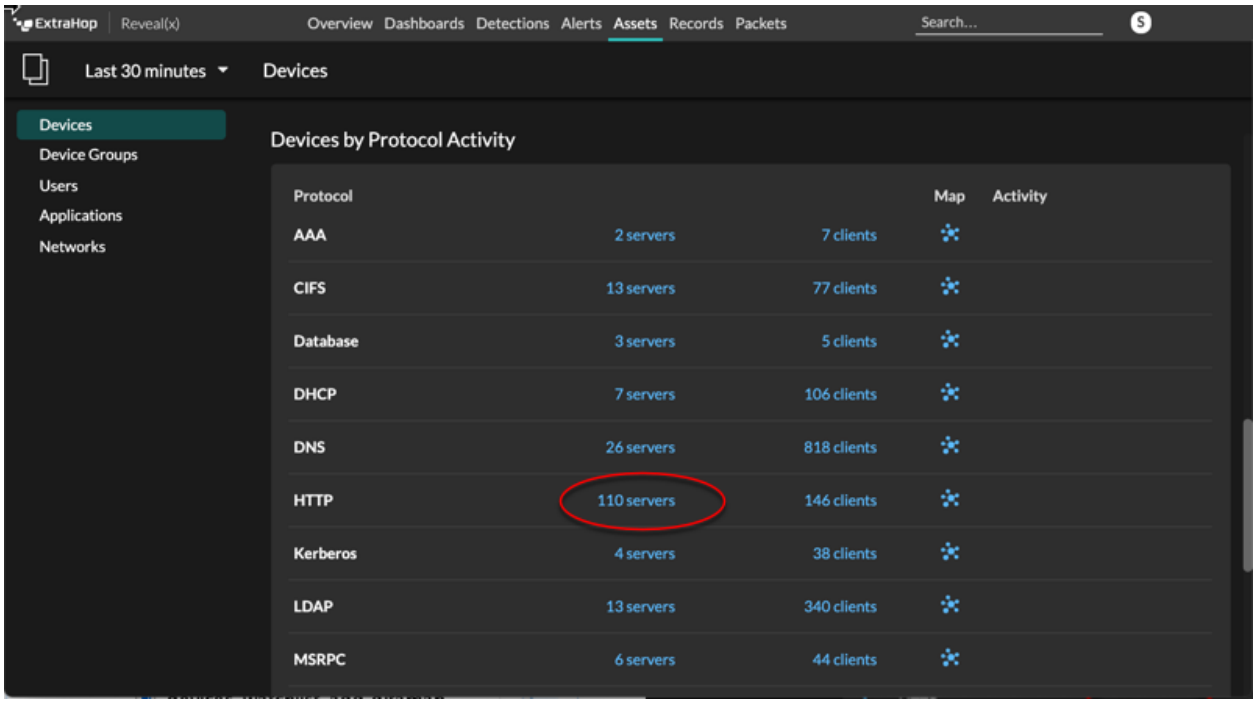
- Click a device name to view device properties and metrics on the Device Overview page.
- Click **Create Dynamic Group** from the upper right corner to create a dynamic device group based on the filter criteria.
- Click the command menu ⋮ and then select PDF or CSV to export the device list to a file.

Search for devices by protocol activity

The Devices page displays all protocols that are actively communicating on the ExtraHop system during the selected time interval. You can quickly locate a device that is associated with a protocol, or discover a decommissioned device that is still actively communicating over a protocol.

In the following example, we show you how to search for a web server within the group of HTTP servers.

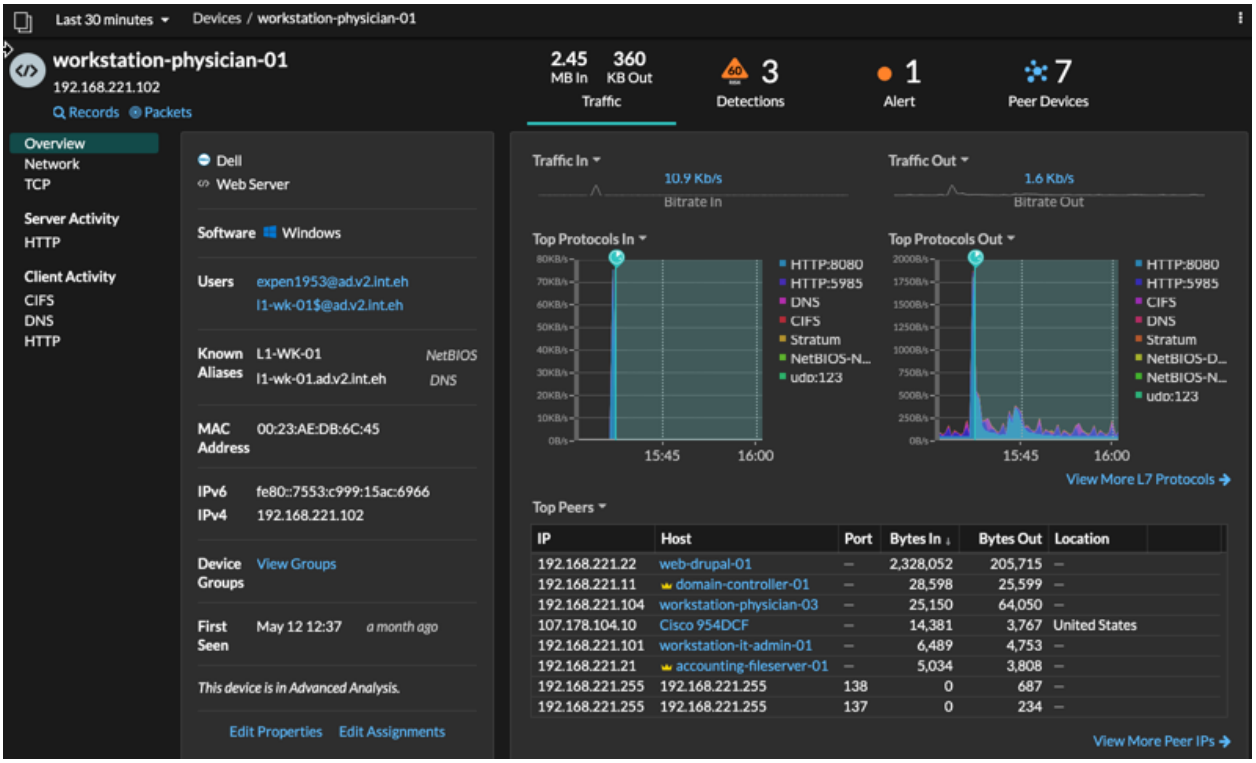
1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. At the top of the page, click **Assets**.
3. From the Devices by Protocol Activity chart, click the number of HTTP servers, as shown in the following figure.



Note: If you do not see the protocol you want, the ExtraHop system might not have observed that type of protocol traffic over the wire during the specified time interval, or the protocol might require a module license. For more information, see the I don't see the protocol traffic I was expecting? section in the License FAQ.

The page displays traffic and protocol metrics associated with the group of HTTP servers.

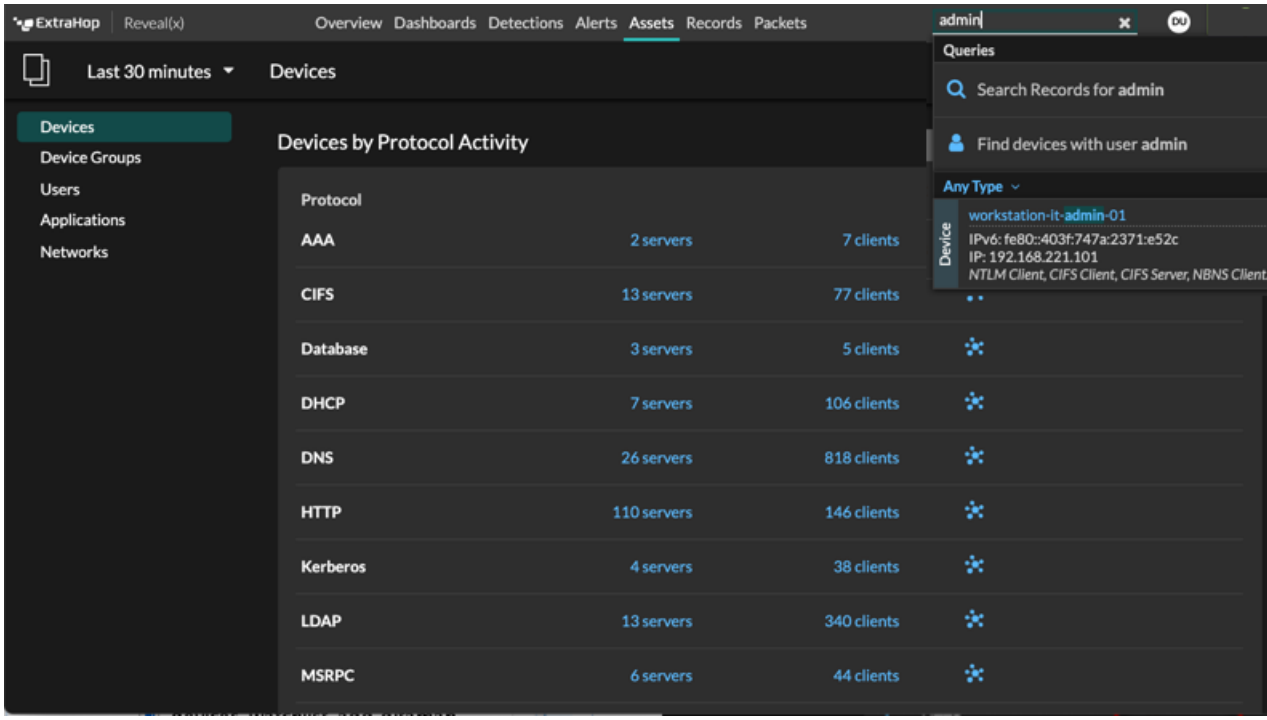
4. At the top of the page, click **Group Members**.
   The page displays a table that contains all of the devices that sent HTTP responses over the wire during the selected time interval.
5. From the table, click a device name.
   The page displays traffic and protocol metrics associated with that device, similar to the following image.



Search for devices accessed by a specific user

From the Users page, you can see active users and the devices they have logged in to the ExtraHop system during the specified time interval.

Tip: You can also search for users from the global search field at the top of the page.



This procedure shows you how to perform a search from the Users page.

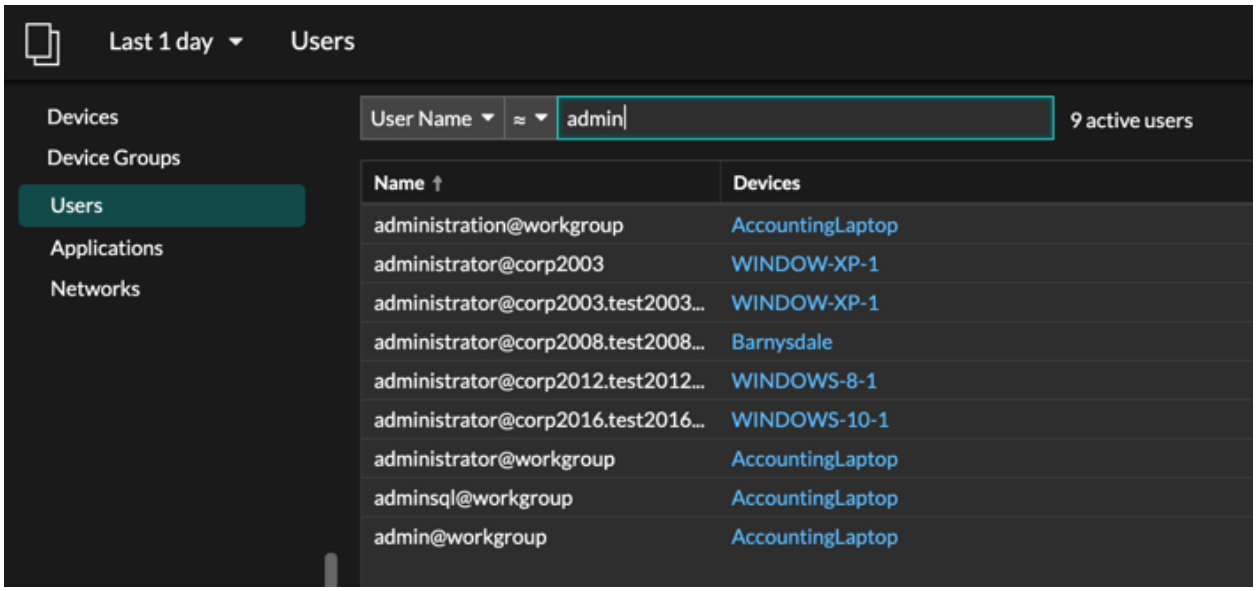
1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. At the top of the page, click **Assets**.
3. Click **Users** in the left pane.
4. From the search bar, select one of the following categories from the drop-down list:

Option	Description
User Name	Search by user name to learn which devices the user has accessed. The user name is extracted from the authentication protocol, such as LDAP or Active Directory.
Protocol	Search by protocol to learn which users have accessed devices communicating over that protocol.
Device Name	Search by device name to learn which users have accessed the device.

5. Select one of the following operators from the drop-down list:

Option	Description
=	Search for a name or device that is an exact match of the text field.
≠	Search for names or devices that do not exactly match the text field.
≈ (default)	Search for a name or device that includes the value of the text field.
≈/	Search for a name or device that excludes the value of the text field.

6. In the text field, type the name of the user or device you want to match or exclude.
The Users page displays a list of results similar to the following figure:



7. Click the name of a device to open the Device Overview page and view all of the users that have accessed the device during the specified time interval.

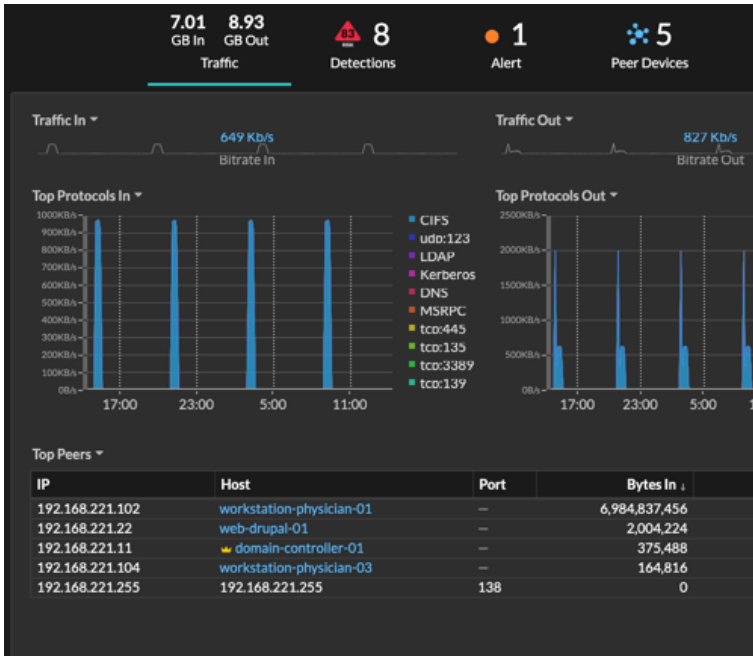
Search for peer devices

If you want to know which devices are actively talking to each other, you can drill down by Peer IPs from a device or device group protocol page.

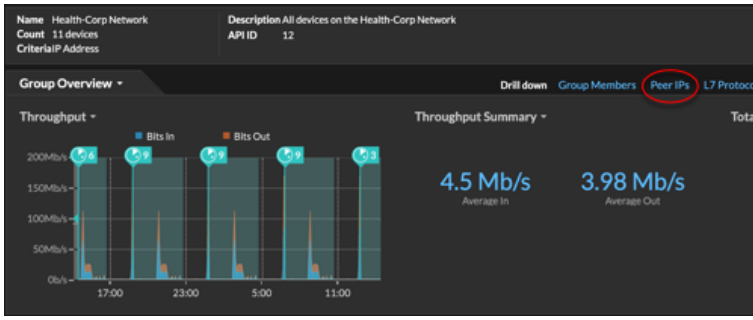
When you drill down by Peer IP address, you can investigate a list of peer devices, view performance or throughput metrics associated with peer devices, and then click on a peer device name to view additional protocol metrics.

1. Log in to the ExtraHop system through `https://<extrahop-hostname-or-IP-address>`.
2. At the top of the page, click **Assets** and then select **Device** or **Device Group** in the left pane.
3. Search for a device or device group, and then click the name from the list of results.
4. On the Overview page for the selected device or device group, click one of the following links:

Option	Description
For devices	Click **View More Peer IPs**, located at the bottom of the Top Peers chart.



For device groups	Click **Peer IPs**, located in the Details section near the upper right corner of the page.



Option	Description

A list of peer devices appears, which are broken down by IP address. You can investigate network bytes and packets information for each peer device, as shown in the following figure.