Devices

Published: 2020-02-23

The ExtraHop system automatically discovers and classifies devices that are actively communicating over the wire, such as clients, servers, routers, load balancers, and gateways. Each device receives the highest level of analysis available, based on your appliance configuration.

By clicking **Assets** in the top menu and then clicking **Devices**, you can see a list of the devices discovered on your network. You can search for a specific device, and then click the name to display an overview page that contains all of the discovered information and traffic and protocol metrics associated with the device.

It is important to know that devices listed in the ExtraHop system might not have a one-to-one correlation to the physical devices in your environment. For example, if a single physical device has multiple active network interfaces, that device is identified as multiple devices in the ExtraHop Web UI.

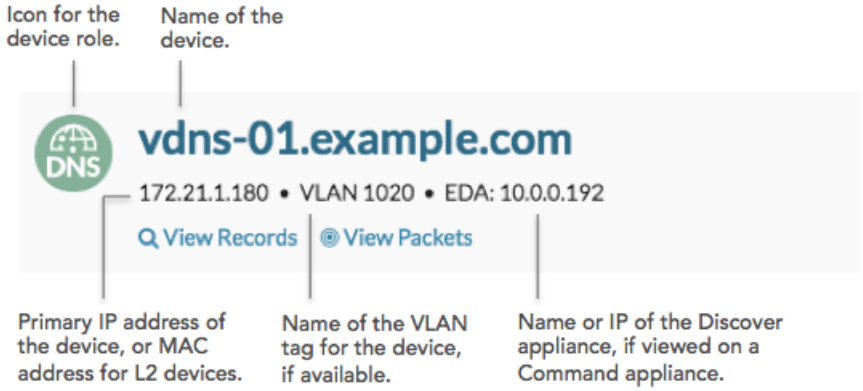
In addition to discovering and classifying individual devices, you can group device metrics or adjust the level of analysis that your devices receive.

Device Overview page

By clicking on a device name, you can view all of the information discovered by the ExtraHop system about the device on the Overview page. The Overview page is divided into three sections: a top-level summary, a properties panel, and an activity panel.

Device summary

The device summary provides information that identifies the device and its role on your network.

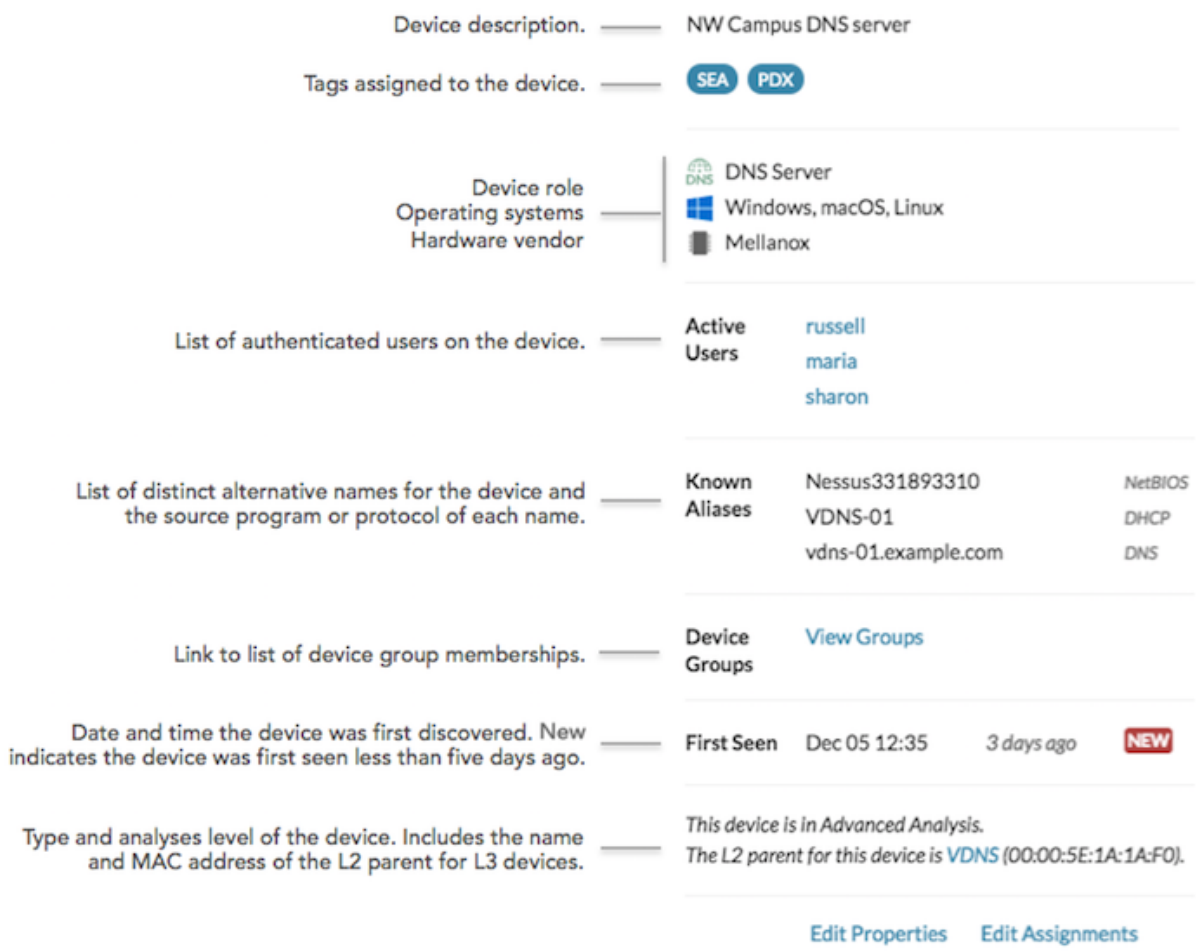


Here are some ways you can learn more about the device:

- Click the pencil icon to view or modify device properties such as device role, device group memberships, or tag assignments.
- Click **View Records** to go to the Records page, which is filtered to display records for this device. (Requires an Explore appliance or third-party recordstore.)
- Click **View Packets** to go to the Packets page, which is filtered to display packets for this device. (Requires a Trace appliance or packet capture disk.)

Device properties

The device properties section provides information that identifies known attributes and assignments for the device, such as tags, aliases, and the analysis level.

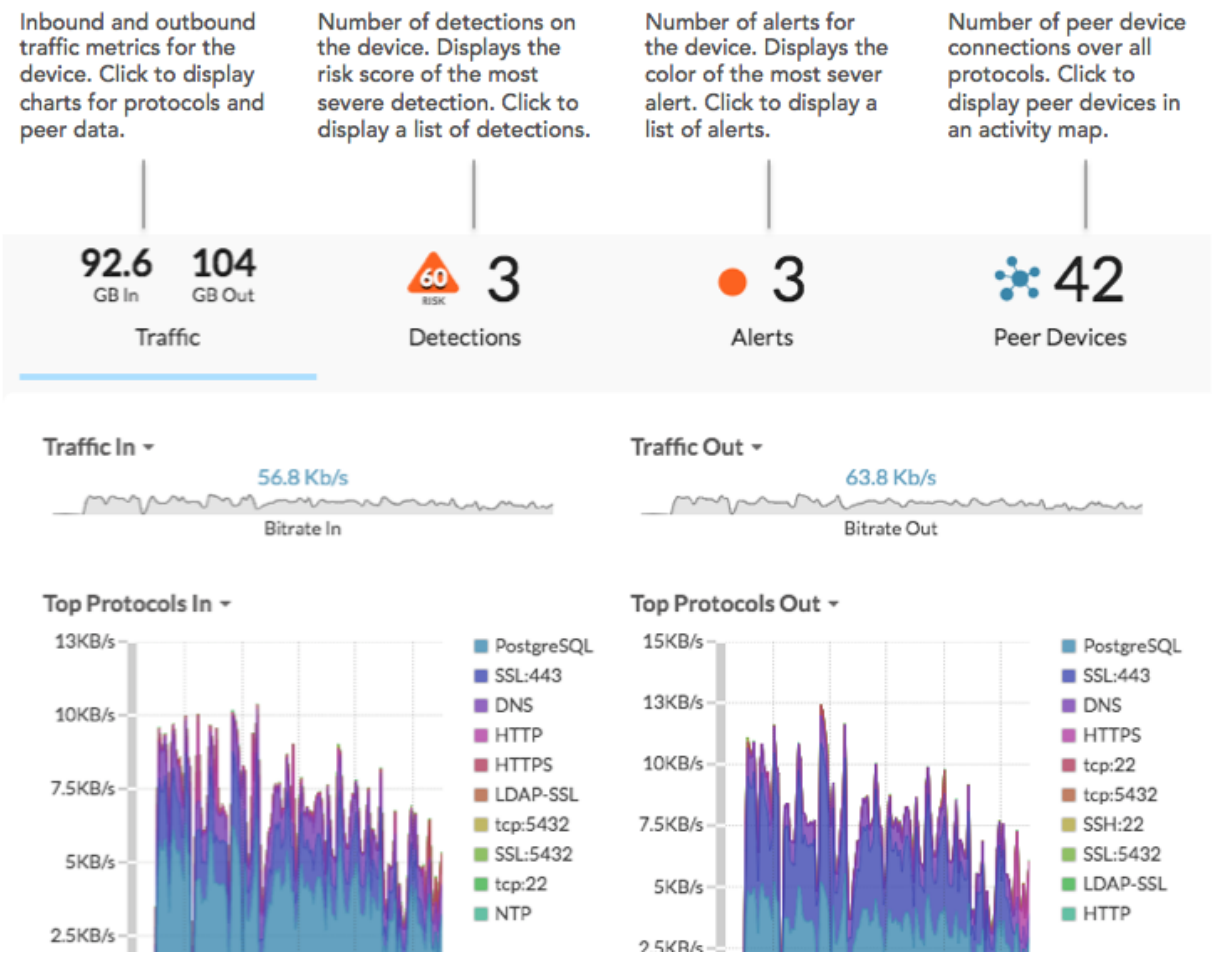


Here are some ways you can learn more about device properties:

- Click a tag to go to the Devices page, which is filtered by the name of the tag in the search bar.
- Click an active user name to go to the Users page, which is filtered by the user name in the search bar. The user name is extracted from the authentication protocol, such as LDAP or Active Directory.
- Click **View Groups** to view a list of device groups the device belongs to and to modify the group membership.
- Click **Edit Properties** to view or modify device properties such as device role, device group memberships, or tag assignments.
- Click **Edit Assignments** to view or modify which alerts and triggers are assigned to the device.

Device activity

The device activity section provides information about how the device is communicating with other devices on your network. Click on the type of activity you want to investigate from the top of the section to display the details in the content pane. For example, click **Alerts** to view a list of alerts that were issued for the device in the specified time interval.



Here are some ways you can investigate activity on the device:

- Click **Traffic**, then drill down on metrics in traffic charts.

  Note: Traffic charts are not displayed if the device is in Discovery Mode. You can configure analysis priority rules to elevate this device to Advanced Analysis or Standard Analysis.
- Click **Detections**, then click a detection name to view detection details.
- Click **Alerts**, then click an alert name to view alert details.
- Click **Peer Devices** to display an activity map, which is visual representation of the L4-L7 protocol activity between devices in your network. To modify the activity map with additional filters and steps, click **Open Activity Map**.

Tip: You can bookmark the Overview page to a specific activity view by setting the `tab` URL parameter to one of the following values:

- `tab=traffic`
- `tab=detections`
- `tab=alerts`
- `tab=peers`

For example, the following bookmark URL defaults to the detection activity view on the Overview page:

```
https://example-eda/extrahop/#/metrics/devices/device-id/overview/
&tab=detections
```

Grouping devices

Both custom devices and device groups are ways that you can aggregate your device metrics. Custom devices are user-created devices that collect metrics based on specified criteria, while device groups gather metrics for all of the specified devices in a group. With device groups, you can still view metrics for each individual device or group member. The metrics for a custom device are collected and displayed as if for a single device—you cannot view individual device metrics.

Both device groups and custom devices can dynamically aggregate metrics based on your specified criteria. We recommend selecting reliable criteria, such as the device IP address, MAC address, VLAN, tag, or type. While you can select devices by their name, if the DNS name is not automatically discovered, the device is not added.

	Device Groups	Custom Devices
Criteria	• IP address • Source port • Destination port • VLAN • Device and vendor MAC addresses • Device tags • Device	• IP address • Source port • Destination port • VLAN
Performance cost	Comparatively low. Because device groups only combine metrics that have already been calculated, there is a relatively low effect on metric collection. However, a high number of device groups with a large number of devices and complex criteria will take more time to process.	Comparatively high. Because the metrics for custom devices are aggregated based on user-defined criteria, large numbers of custom devices, or custom devices with extremely broad criteria, require more processing. Custom devices also increase the number of system objects to which metrics are committed.
View individual device metrics	Yes	No
Best practices	Create for local devices where you want to view and compare the metrics in a single chart. Device groups can be set as a metric source.	Create for devices that are outside of your local network, or for types of traffic that you want to organize as a single source. For example, you might want to define all physical interfaces on a server as a single custom device to better view metrics for that physical appliance as a whole.

Custom devices

The ExtraHop system automatically discovers local L3 devices based on observed ARP traffic that is associated with IP addresses. By default, all IP addresses that are observed outside of locally-monitored broadcast domains are aggregated at one of the incoming routers in your network.

To collect metrics for a segment of traffic across multiple IP addresses and ports, you can create a custom device from a Command or Discover appliance. You might create a custom device to track individual devices outside of your local broadcast domain or you might create a single custom device to collect metrics for several known IP addresses or CIDR blocks for a remote site or cloud service. A single custom device counts

as one device towards your licensed capacity for Advanced Analysis or Standard Analysis. Any triggers or alerts are also assigned to the custom device as a single device.

Create a custom device when you want to collect metrics for devices that are outside of your local network or when you have a group of devices that you want to aggregate metrics for as a single device. These devices can even be different physical interfaces that are located on the same device; aggregating the metrics for these interfaces can make it easier to understand how heavily taxed your physical resources are as a whole, rather than by interface.

After you create a custom device, all of the metrics associated with the IP addresses and ports are aggregated into a single L2 device. While typical L2 devices only collect MAC addresses and L2-L3 metrics, custom devices also collect L2-L7 metrics.

While custom devices aggregate metrics based on their defined criteria, the metric calculations are not treated the same as for discovered devices. For example, you might have a trigger assigned to a custom device that commits records to an Explore appliance. However, the custom device is not shown as either a client or a server in any transaction records. The ExtraHop system populates those attributes with the L2 or L3 device that corresponds to the conversation on the wire data.

Custom devices can affect the overall system performance, so you should avoid the following configurations:

- Avoid creating multiple custom devices for the same IP addresses or ports. Custom devices that are configured with overlapping criteria might degrade system performance.
- Avoid creating a custom device for a broad range of IP addresses or ports, which might degrade system performance.

Related topics

- Create a custom device (with guidance on performance impact)
- Delete or disable custom devices
- Add a device to the watchlist for Advanced Analysis (applies to custom devices)
- Walkthrough: Create a custom device to monitor remote office traffic
- REST API: Create a custom device

Device groups

Device groups are collections of devices that are configured either statically (where you add each device individually) or dynamically (where you add the criteria that is applied to matching devices). In addition, there are some built-in device groups that group devices by their discovery time, by their role, and by type.

There is no performance impact to collecting metrics with device groups. However, we recommend that you prioritize these groups by their importance to make sure that the right devices receive the highest level of analysis.

Device groups are a good choice when you have devices that you want to collectively apply as a source. For example, you could collect and display metrics for all of your high-priority production web servers in a dashboard.

By creating a device group, you can manage all of those devices as a single metric source instead of adding them to your charts as individual sources. However, note that any assigned triggers or alerts are assigned to each group member (or individual device).

Related topics

- Create a device group (static or dynamic)
- Remove devices from a static device group
- Display device group members in a chart
- Prioritize groups for Standard or Advanced Analysis
- Walkthrough: Monitor load balancer performance in a dashboard (showcases how to create a device group)

Device names and roles

After a device is discovered, the ExtraHop system tracks all of the wire data traffic associated with the device. The ExtraHop system discovers device names by passively monitoring naming protocols, including DNS, DHCP, NETBIOS, and Cisco Discovery Protocol (CDP).

A device can be identified by multiple names, which are all searchable. If a name is not discovered through a naming protocol, the default name is derived from device attributes (MAC address for L2 devices and the IP address for L3 devices). You can also create a custom name for a device.

Note: If a device name does not include a hostname, the ExtraHop system has not yet observed naming protocol traffic associated with that device. The ExtraHop system does not perform DNS lookups for device names.

Based on the type of traffic associated with the device or the device model, the ExtraHop system assigns a role to the device, such as a gateway, file server, database, or load balancer. Not all roles are automatically assigned to a device, however, you can manually assign or change a device role to any of the following roles:

Icon	Role	Description
	Database	A device that hosts a database instance.
	DHCP Server	A device that processes DHCP server activity.
	DNS Server	A device that processes DNS server activity.
	Domain Controller	A device that acts as a domain controller for Kerberos, CIFS, and MSRPC server activity.
	File Server	A device that responds to read and write requests for files over NFS and CIFS/SMB protocols.
	Firewall	A device that monitors incoming and outgoing network traffic and blocks traffic according to security rules. The ExtraHop system does not automatically assign this role to devices.
	Gateway	A device that acts as a router or gateway. The ExtraHop system looks for L2 devices associated with a large amount of unique IP addresses (past a certain threshold) when identifying gateways. Gateway device names include the router name such as Cisco B1B500. Unlike other L2 parent devices, you can add a gateway

Icon	Role	Description
		device to the watchlist for Advanced Analysis.
	IP Camera	A device that sends image and video data through the network. The ExtraHop system assigns this role based on the device model.
	Load Balancer	A device that acts as a reverse proxy for distributing traffic across multiple servers.
	Medical Device	A device designed for healthcare needs and medical environments that processes DICOM traffic.
	Mobile Device	A device that has a mobile operating system installed, such as iOS or Android.
	PC	A device such as a laptop, desktop, Windows VM, or macOS device that processes DNS, HTTP, and SSL client traffic.
	Printer	A device that enables users to print text and graphics from other connected devices.The ExtraHop system assigns this role based on the device model.
	VoIP Phone	A device that manages voice over IP (VoIP) phone calls.
	VPN Gateway	A device that connects two or more VPN devices or networks together to bridge remote connections. The ExtraHop system assigns this role to devices with a large number of external VPN peers.
	Vulnerability Scanner	A device that runs vulnerability scanner programs.
	Web Proxy Server	A device that processes HTTP requests between a device and another server.
	Web Server	A device that hosts web resources and responds to HTTP requests.

Icon	Role	Description
	Wi-Fi Access Point	A device that creates a wireless local area network and projects a wireless network signal to a designated area. The ExtraHop system assigns this role based on the device model.

Analyzing devices

Each device or device group receives the highest level of analysis possible, based on your license and your system configuration. In addition, if you have a Command appliance, you can manage your analysis priorities from a centralized location for all connected Discover appliances.

Learn more about how analysis priorities work and how you can optimize metrics for your high-priority devices.