Devices

Published: 2020-06-17

The ExtraHop system automatically discovers and classifies devices, also known as endpoints, 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 system configuration.

The ExtraHop system can discover and track devices by their MAC address (L2 Discovery) or by their IP addresses (L3 Discovery). Enabling L2 Discovery offers the advantage of tracking metrics for a device even if the IP address is changed or reassigned through a DHCP request. If L3 Discovery is enabled, it is important to know that devices 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 by the ExtraHop system.

After a device is discovered, the ExtraHop system begins to collect metrics based on the analysis level configured for that device. The analysis level determines the types of metrics that are generated and which features are available for organizing metric data.

Navigating devices

Click **Assets** from the top menu and then click **Devices** to display the following charts that provide insight about the active devices discovered on your network during the selected time interval:

Active Devices

Displays the total number of devices that have been discovered by the ExtraHop system. Click the number to view a list of all discovered devices. From the Active Devices list, you can search for specific devices or click a device name to view device details on the device Overview page.

New Devices

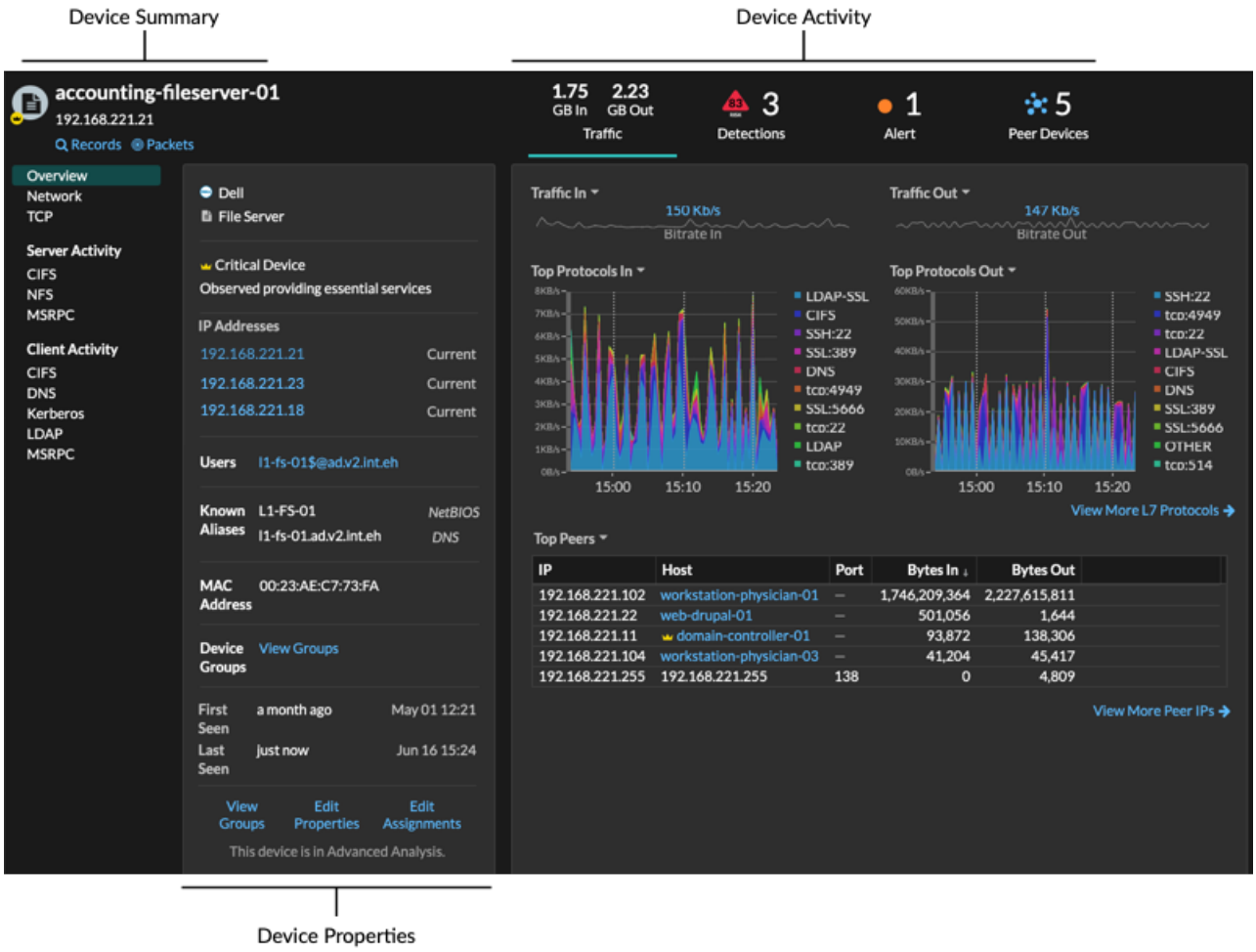
Displays the number of devices that have been discovered within the past month and the percentage rate of change. Click the number to view a list of all of these devices.

Devices by Role

Displays each type of device role that is active on your network and the number of devices assigned to each role. Click a device role to view a list of all devices assigned that role.

Device Overview page

By clicking on a device name, you can view all of the information discovered about the device by the ExtraHop system on the device Overview page. The device 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 such as the device name, the current IP address or MAC address, and the role assigned to the device. If viewing from a Command appliance, the name of the Discover appliance is displayed.

- Click **Records** to start a record query that is filtered by this device.
- Click **Packets** to start a packet query that is filtered by this device.

Device properties

The device properties section provides the following known attributes and assignments for the device.

Critical Device

A critical device icon is displayed if the device is observed to provide authentication or is critical to essential services.

IP Addresses

A list of IP addresses observed on the device at any time during the selected time interval. If L2 Discovery is enabled, the list might display both IPv4 and IPv6 addresses that are simultaneously observed on the device, or the list might display multiple IP addresses assigned through DHCP requests at different times. A timestamp indicates when the IP address was last observed on the device. Click an IP address to view other devices where the IP address has been seen.

Associated IP Addresses

A list of IP addresses, usually outside of the network, that are associated with the device at any time during the selected time interval. For example, a VPN client on your network might be associated with an external IP address on the public internet. A timestamp indicates when the IP address was last associated with the device. Click an associated IP address to view details such as the geographic location and other devices the IP address has been associated with.

Users

A list of authenticated users logged into the device. Click a user name to go to the Users page and view which other devices the user is logged into.

Known Aliases

A list of alternative device names and the source program or protocol.

Hardware and Software

The hardware or vendor make and model of the device and any operating systems running on the device.

Tags

The tags assigned to the device. Click a tag name to view the other devices that the tag is assigned to.

First and Last Seen

The timestamps from when the device was first discovered and when activity was last observed on the device. NEW is displayed if the device was discovered within the last five days

Analysis

The level of analysis that this device receives.

Here are some ways you can view and modify device properties:

- Click **View Groups** to view the device group membership for the device.
- Click **Edit Properties** to view or modify device properties such as device role, device group memberships, or device tags.
- 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 and which detections and alerts are associated with the device.

- Click **Traffic** to view charts for protocol and peer data, and then drill down on metrics in traffic charts.

  Note: Traffic charts are not available if the device analysis level is Discovery Mode. To enable traffic charts for the device, elevate the device to Advanced Analysis or Standard Analysis.
- Click **Detections** to view a list of detections, and then click a detection name to view detection details.
- Click **Alerts** to view a list of alerts, and then click an alert name to view alert details.
- Click **Peer Devices** to view 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 device Overview page to a specific activity view by setting the `tab` URL parameter to one of the following values:

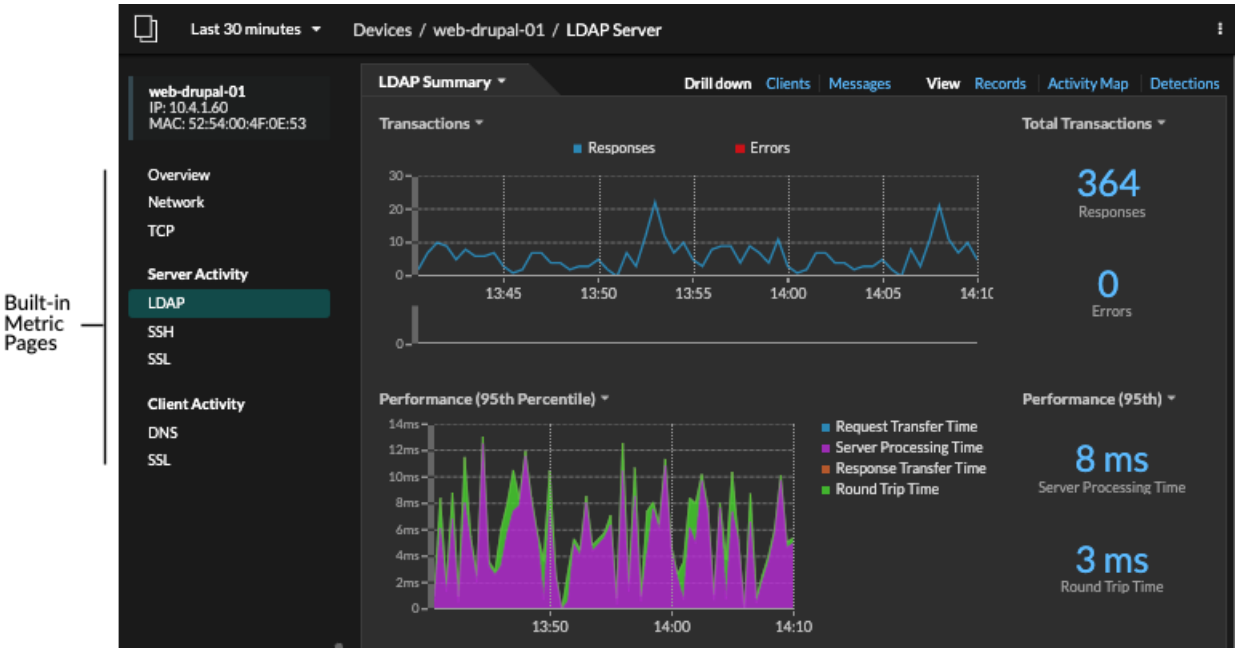
  - `tab=traffic`
  - `tab=detections`
  - `tab=alerts`
  - `tab=peers`

For example, the following URL always displays detection activity for the specified device:

```
https://example-eda/extrahop/#/metrics/devices//0026b94c03810000/
overview/&tab=detections
```

Device metrics

Metrics are real-time measurements of your network traffic that the ExtraHop system calculates from wire or flow data. Metrics collected from device traffic can be viewed in built-in charts and graphs from a device page.



Click a built-in metric page from the left pane to view top-level device metrics or client and server metrics by protocol. Click a chart to drill down to detail metric pages, which display metric values for a specific key (such as a client or server IP address).

The ExtraHop system provides thousands of built-in metrics. Here are some ways you can gain further insight about your devices

- Create a chart to visualize specific metrics and save the chart to a dashboard.
- Create an activity map to view peer device relationships over specified protocols.
- Write a trigger to create custom metrics or create an application container to collect metrics for specific devices.

IP address details

Type an IP address in the global search field or click an IP address link from a device Overview page to view details about an IP address.

The following information is displayed for an IP address seen on a device:

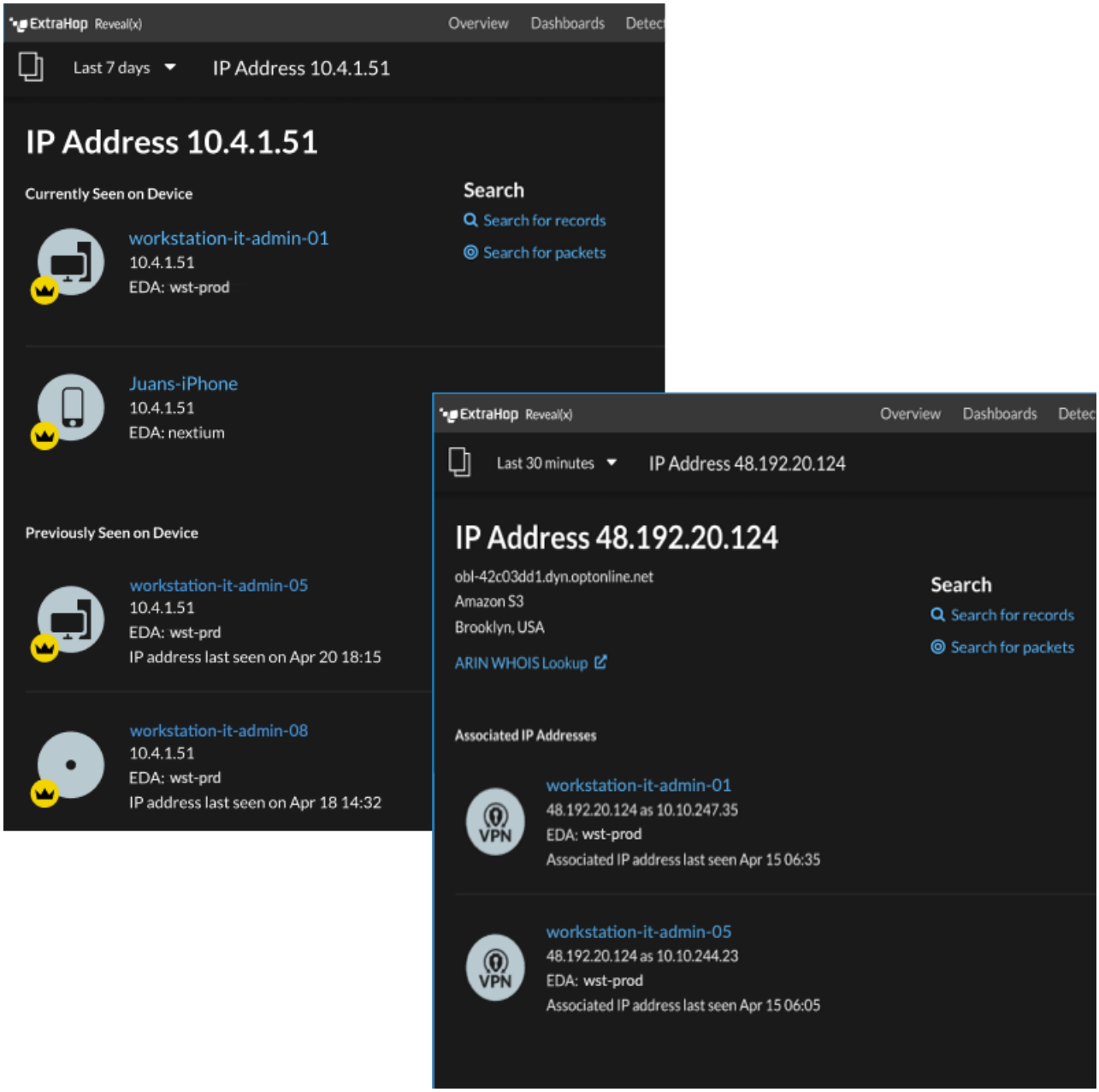
- Each device where the IP address is currently observed, regardless of the selected time interval.
- Each device where the IP address was previously observed within the selected time interval, including the timestamp from when the IP address was last seen on the device.

If L2 Discovery is enabled, both IPv4 and IPv6 addresses might be simultaneously observed on the device, or different IP addresses might be assigned to the device by DHCP over time.

The following information is displayed for an IP address associated with a device:

- The geolocation of the IP address and links to the ARIN Whois website.

- Each device where the associated IP address was seen outside of the network at any time during the selected time interval. For example, a VPN client on your network might be associated with an external IP address on the public internet.
- The IP address of the device as seen by the ExtraHop system on your network.
- The timestamp when the associated IP address was last seen on the device.



Here are some ways you can view additional IP address and device information:

- Hover over a device name to view device properties.
- Click a device name to view the device Overview page.
- Click **Search for Records** to start a record query that is filtered by the IP .
- Click **Search for Packets** to start a packet query that is filtered by this device.

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 server as a whole.

Custom devices

Custom devices enable you 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. You might create a custom device to track individual devices outside of your local broadcast domain or to collect metrics for several known IP addresses or CIDR blocks for a remote site or cloud service.

After you create a custom device, all of the metrics associated with the IP addresses and ports are aggregated into a single device that collects L2-L7 metrics. A single custom device counts as one device towards your licensed capacity for Advanced Analysis or Standard Analysis, which enables you to add a custom device to the watchlist. Any triggers or alerts are also assigned to the custom device as a single device.

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 a recordstore. 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 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.

If a large number of custom devices is affecting your system performance, you can delete or disable a custom device. The unique Discovery ID for the custom device always remains in the system. See Create a custom device to monitor remote office traffic to familiarize yourself with custom devices.

Device groups

A device group is a user-defined collection that can help you track metrics across multiple devices that are typically grouped by shared attributes such as protocol activity.

You can create a static device group that requires you to manually add or remove a device from the group. Or, you can create a dynamic device group that includes criteria that determines which devices are automatically included in the group. For example, you can create a dynamic device group based on the device discovery time that adds devices that are discovered during a specific time interval. In addition, there are some built-in device groups that dynamically group devices by their discovery time, device role, or 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).

Device names and roles

After a device is discovered, the ExtraHop system tracks all of the wire data traffic associated with the device to determine the device name and role.

Device names

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, such as MAC addresses and IP addresses. 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.

Device roles

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
	Custom Device	A user-created device that collects metrics based on specified criteria. The ExtraHop system automatically assigns this role when you create a custom device. You cannot manually assign the Custom role to a device.
	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.

Icon	Role	Description
	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 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 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.

Icon	Role	Description
	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 or on traffic observed over mDNS (multicast DNS).
	VoIP Phone	A device that manages voice over IP (VoIP) phone calls.
	VPN Client	An internal device that communicates with a remote IP address. If VPN client discovery is enabled, the ExtraHop system automatically assigns this role to internal devices communicating with remote IP addresses through a VPN gateway. You cannot manually assign the VPN Client role to a device.
	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.