Deploy the ExtraHop EFC 6392v NetFlow Sensor

Published: 2025-04-03

This guide explains how to deploy the EFC 6392v NetFlow virtual sensor.

The EFC 6392v is designed to connect to RevealX 360 and RevealX Enterprise and collect NetFlow records from your network. Packet analysis is not available.

System requirements

Your environment must meet the following requirements to deploy an EFC 6392v virtual sensor:

- You must have familiarity with administering Linux KVM or VMware VMware.
- You must have the ExtraHop deployment file, which is available on the ExtraHop Customer Portal.
- You must have an ExtraHop EFC 6392v sensor product key.
- You should upgrade to the latest patch for the Linux KVM or vSphere environment to avoid any known issues.

Virtual machine requirements

You must provision a hypervisor that most closely matches the following specifications for the virtual sensor.

Sensor	vCPUs	RAM	Disk
6100v	18	64 GB	1000 GB

Deployment overview

Collecting NetFlow records requires the following configuration setup.

- Deploy an ExtraHop sensor on VMware, Deploy an ExtraHop sensor on AWS, or Deploy an ExtraHop sensor on Azure.
- Configure interfaces.
- Configure NetFlow settings on the ExtraHop system.

Configure interfaces

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **Connectivity**.
3. In the Interfaces section, click the name of the interface you want to configure.
4. On the Network Settings for Interface *<interface number>* page, from the **Interface Mode** drop-down menu, select **Management + Flow Target**.
5. Disable all remaining interfaces, since the sensor cannot process NetFlow and wire data simultaneously:
   a) In the Interfaces section, click the name of the interface you want to configure.
   b) From the **Interface Mode** drop-down menu, select **Disabled**.
   c) Repeat until all additional interfaces are disabled.

6. Click **Save**.

Configure NetFlow settings

You must configure port and network settings on the EFC 6392v NetFlow virtual sensor before you can collect NetFlow records. The EFC 6392v sensor supports the following flow technologies: Cisco NetFlow v9.

You must log in as a user with System and Access Administration privileges to complete the following steps.

Required NetFlow v9 fields for EFC 6392v

All v9 fields must be present in records sent to the sensor.

Field	Description
Version	The version of NetFlow records exported in this packet; for version 9, this value is 0x0009
Count	Number of FlowSet records (both template and data) contained within this packet
SysUptime	Current time in milliseconds since the export device is started.
UNIX seconds	Current time in seconds that have elapsed since 00:00:00 Coordinated Universal Time, Thursday, 1 January 1970.
Sequence number	The incremental sequence counter of all export packets that are sent by this export device; this value is cumulative, and can identify any missed export packets. Note: This change applies to NetFlow Version 5 and Version 8 headers, where this number previously represented the total flows.
Source ID	The Source ID field is a 32-bit value that guarantees uniqueness for all flows that are exported from a particular device. (The Source ID field is the equivalent of the engine type and engine ID fields that are found in NetFlow Version 5 and Version 8 headers.) The format of this field is vendor-specific. In the Cisco implementation, the first two bytes are reserved for future expansion, and are always zero. Byte 3 provides uniqueness about the routing engine on the exporting device. Byte 4 provides uniqueness about the particular line card or Versatile Interface processor on the exporting device. Collector devices must create a combination of the source IP address plus the Source ID field to associate an incoming NetFlow export packet with a unique instance of NetFlow on a particular device.

For more information, see NetFlow V9 formats.

Configure the flow type and UDP port

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **NetFlow**.
3. In the Ports section, in the Port field, type the UDP port number.
   The default port for NetFlow is `2055`. You can add additional ports as needed for your environment.

Note: Port numbers must be 1024 or greater

4. From the Flow Type drop-down menu, select **NetFlow**.
5. Click the plus icon (**+**) to add the port.

Add approved networks

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **NetFlow**.
3. In the Approved Networks section, click **Add Approved Network**.
4. From the Flow Type drop-down menu, select **NetFlow**.
5. For IP address, type the IPv4 or IPv6 address.
6. For Network ID, type a name to identify this approved network.
7. Click **Save**.

Discover NetFlow devices

You can configure the ExtraHop system to discover NetFlow devices by adding a range of IP addresses.

Note: ExtraHop systems do not support sampled NetFlow. Including sampled NetFlow in your traffic might result in inaccurate device metrics, but device discovery should still function as normal.

Here are some important considerations about Remote L3 Discovery:

- With NetFlow, devices that represent the gateways exporting records are automatically discovered. You can configure the ExtraHop system to discover devices that are representing the IP addresses observed in NetFlow records by adding a range of IP addresses.
- Exercise caution when specifying CIDR notation. A /24 subnet prefix might result in 255 new devices discovered by the ExtraHop system. A wide /16 subnet prefix might result in 65,535 new devices discovered, which might exceed your device limit.
- If an IP address is removed from the Device Discovery settings, the IP address will persist in the ExtraHop system as a remote L3 device as long as there are existing active flows for that IP address or until the capture is restarted. After a restart, the device is listed as an inactive remote L3 device.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings section, click **NetFlow**.
3. In the NetFlow Device Discovery section, type the IP address in the IP address ranges field.

   You can specify one IP address or a CIDR notation, such as `192.168.0.0/24` for an IPv4 network or `2001:db8::/32` for an IPv6 network.

   Important: Every actively-communicating remote IP address that matches the CIDR block will be discovered as a single device in the ExtraHop system. Specifying wide subnet prefixes such as /16 might result in thousands of discovered devices, which might exceed your device limit.
4. Click the green plus icon (**+**) to add the IP address.

Next steps

You can add another IP address or range of IP addresses by repeating steps 3-4.

Post-deployment actions

Published: 2025-04-03

- Review the Sensor and console post-deployment checklist and configure additional settings.
- Connect to a sensor from a RevealX Enterprise console, if supported.