

Install the SSD for Packet Capture on the EH3000/6000/8000

This guide explains how to install the SSD for packet capture on the EH3000/6000/8000 ExtraHop appliances. You must have access to the ExtraHop Admin UI and write permission to the ExtraHop Web UI in order to complete the steps in this guide.

Installing the SSD in the ExtraHop Appliance

Follow these steps to install the SSD for packet capture in the ExtraHop appliance.

1. On the front of the appliance, pull open the last slot.
2. Insert the SSD for packet capture that you received from ExtraHop.

The SSD for packet capture is hot-swappable, so you do not need to power off the ExtraHop appliance to complete this process.

Enabling Packet Capture

Ensure that your ExtraHop license has packet capture enabled.

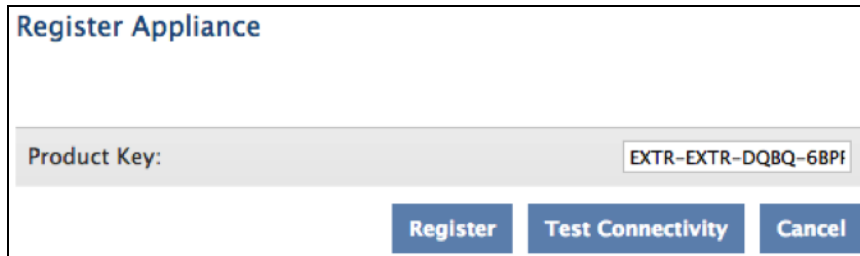
1. In the Admin UI, go to **System Settings** and click **License**.

System Settings	
Services	Change
Firmware	Change
System Time	Change
Shutdown/Restart	Change
License	Change

2. Go to the **Features** section and verify that packet capture is enabled. If packet capture is enabled, go to the next section. If your license does not have packet capture enabled, go to the next step.

Features	
Activity Map	Enabled
Device Safety Limit	1000
License Server Required	Enabled
Packet Capture	Enabled
SSL Decryption	Enabled
Triggers	Enabled

3. The ExtraHop requires a product key and a license in order to use packet capture. Contact ExtraHop Support (support@extrahop.com) to obtain your product key.
 - a. Go to **Manage License** and click **Register** to enter the product key.
 - b. Enter the product key and then click **Register**. The ExtraHop system now contacts the license server and validates the product key. After the product key is validated, the license is downloaded.



Register Appliance

Product Key:

- c. Refresh your browser to see the updated license.

The following example shows a properly licensed ExtraHop with packet capture on the **License Administration** page of the Admin UI:

License Administration	
System Information	
Dossier	9c73db77f22ea4c5cf25baa351a8a539
Serial	30HQQV1
Product Key	EXTR-EXTR-NTG2-NEJN
Platform	EH8000
Modules	
Name	Status
CIFS	Enabled
DB2	Enabled
DIAMETER	Enabled
FIX	Enabled
HTTP-AMF	Enabled
IBMMQ	Enabled
ICA	Enabled
Interfaces	
10G License	True
Features	
Activity Map	Enabled
Device Safety Limit	4000
License Server Required	Enabled
Packet Capture	Enabled (Dedicated Drive)
Triggers	Enabled

Outbound DNS connectivity is required to install the SSD for packet capture. If this is not available, contact support@extrahop.com to request a manual license.

4. In the Admin UI, go to **System Settings** and click **Disk**.
5. Go to the **Unused Disks** section and click **Enable**.

Unused Disks	
RAID Info	
Status	Unused
RAID Level	None
Disk #15	
Slot Number	15
Status	Unconfigured(good), Spun Up
Media Type	Solid State Device
SSD Assisted Packet Capture	Enable

[RAID Disk Details](#)

- Wait approximately 5 minutes. When the progress indicator disappears, the ExtraHop appliance is ready to use packet capture.
- The **Unused Disks** section is renamed to **Packet Capture** and the Status is Optimal.

Packet Capture	
RAID Info	
Status	Optimal
RAID Level	Primary-0, Secondary-0, RAID Level Qualifier-0
Span 0: Row 0	
Slot Number	15
Status	Online, Spun Up
Media Type	Solid State Device

Using Triggers to Define the Packet Capture

The ExtraHop system uses Application Inspection Triggers to gather custom metrics. These metrics are stored internally and can be used by other features, such as packet capture. Triggers are user-defined scripts that perform additional actions during well-defined events.

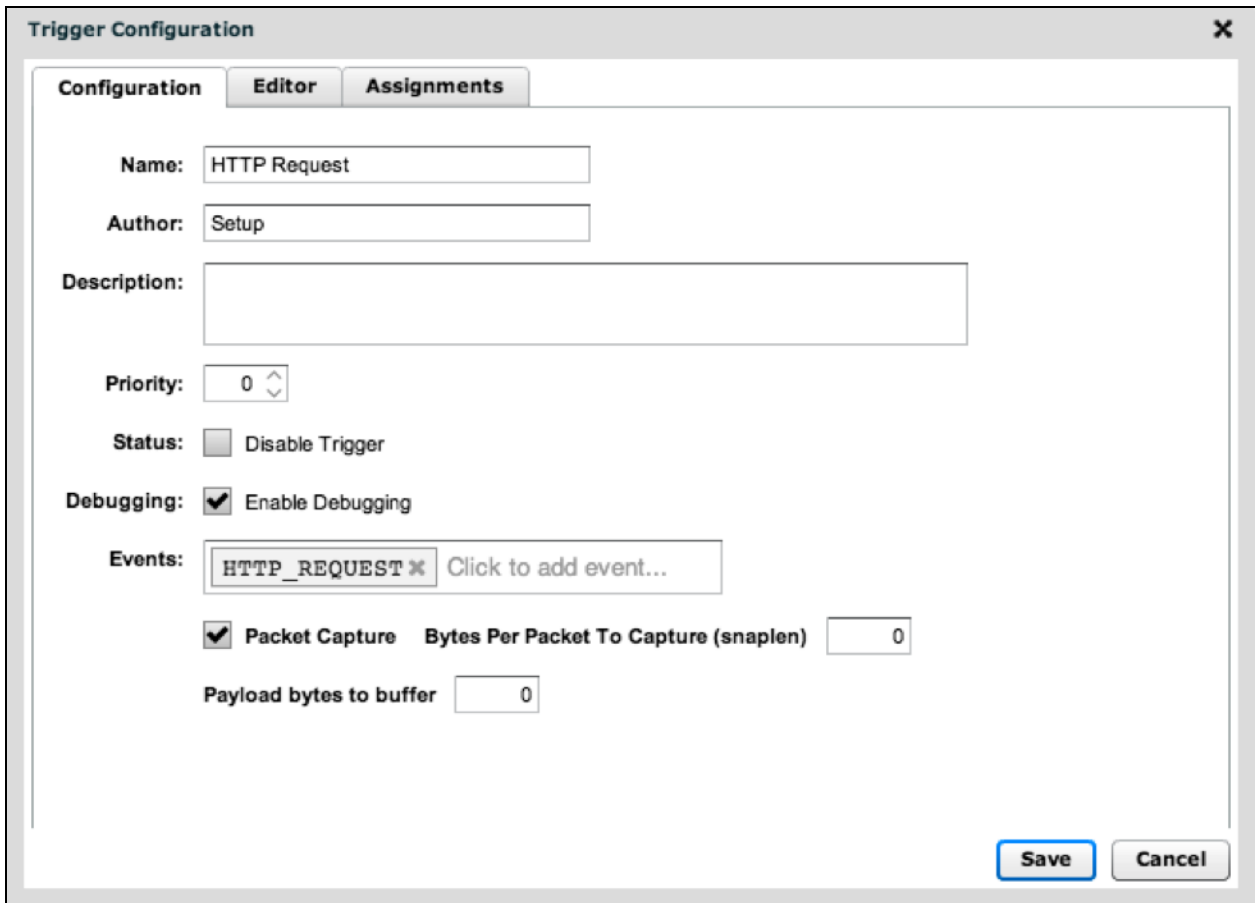
For information about writing triggers, refer to the following related documentation:

- ExtraHop Guide: Getting Started with Application Inspection Triggers*
- ExtraHop Application Inspection Triggers API*

To create a trigger, complete the following steps:

- In the Web UI, click **Settings**, click **Triggers**, and then click **New**.
- Enter a name for the trigger, select the event that will activate the trigger, and click the Packet Capture

checkbox.



Once you have tested the trigger to ensure it works, uncheck **Enable Debugging** to avoid excessive debug messages in the Runtime Log.

3. Click the **Editor** tab, enter your trigger source code, and click **Save**.
4. Click the **Assignments** tab and assign the trigger to a device or group of devices.

Viewing the Packet Capture Results

1. In the Admin UI, go to the **Packet Captures** section and click **View & Download Packet Captures**.



2. On the **Packet Captures** page, select a packet capture to download to your workstation. You can filter packet captures by name and the date of capture.

Packet Captures

Listing options » Name contains: Captured after:

Captured before: Captures per page:

8 packet captures. Showing page of 1

<input type="checkbox"/>	Name	Packets	Bytes	Duration	Start Time	End Time
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:54:34	2012-11-19 16:54:34
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:54:31	2012-11-19 16:54:31
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	1s	2012-11-19 16:31:41	2012-11-19 16:31:42
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:31:30	2012-11-19 16:31:30
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:31:10	2012-11-19 16:31:10
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:30:59	2012-11-19 16:30:59
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:30:39	2012-11-19 16:30:39
<input type="checkbox"/>	0.0.0.0.in-addr.arpa-0.0.0.0.in-addr.arpa	15	1260	<1s	2012-11-19 16:30:28	2012-11-19 16:30:28

3. Open the downloaded packet capture in a packet analyzer such as Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	69.171.229.16	208.79.144.52	TCP	70	http > 54216 [ACK] Seq=1 Ack=1 w
2	0.062000	69.171.229.16	208.79.144.52	TCP	1518	[TCP segment of a reassembled PE
3	0.062000	69.171.229.16	208.79.144.52	TCP	1518	[TCP segment of a reassembled PE
4	0.062000	69.171.229.16	208.79.144.52	TCP	1518	[TCP segment of a reassembled PE
5	0.063000	69.171.229.16	208.79.144.52	HTTP	1405	HTTP/1.1 200 OK (text/html)
6	0.065000	208.79.144.52	69.171.229.16	TCP	70	54216 > http [ACK] Seq=1 Ack=289
7	0.065000	208.79.144.52	69.171.229.16	TCP	70	54216 > http [ACK] Seq=1 Ack=568
8	75.681000	208.79.144.52	69.171.229.16	HTTP	996	GET /plugins/like.php?api_key=&l
9	75.698000	69.171.229.16	208.79.144.52	TCP	70	http > 54216 [ACK] Seq=5680 Ack=
10	75.746000	69.171.229.16	208.79.144.52	TCP	1518	[TCP segment of a reassembled PE
11	75.746000	69.171.229.16	208.79.144.52	TCP	1518	[TCP segment of a reassembled PE

Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

Ethernet II, Src: Cisco_b1:b5:00 (00:1e:7a:b1:b5:00), Dst: Hewlett-_87:36:09 (00:18:71:87:36:09)

802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 7

Internet Protocol Version 4, Src: 69.171.229.16 (69.171.229.16), Dst: 208.79.144.52 (208.79.144.52)

Transmission Control Protocol, Src Port: http (80), Dst Port: 54216 (54216), Seq: 1, Ack: 1, Len: 0

```

0000  00 18 71 87 36 09 00 1e  7a b1 b5 00 81 00 00 07  ..q.6... z.....
0010  08 00 45 00 00 34 66 02  40 00 57 06 32 82 45 ab  ..E..4f. @.W.2.E.
0020  e5 10 d0 4f 90 34 00 50  d3 c8 d9 aa c0 b7 31 6e  ...0.4.P .....ln
0030  54 e6 80 10 00 20 0f fe  00 00 01 01 08 0a 68 8a  T.... .. .....h.
0040  a6 b5 1f 93 b7 bc

```