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.

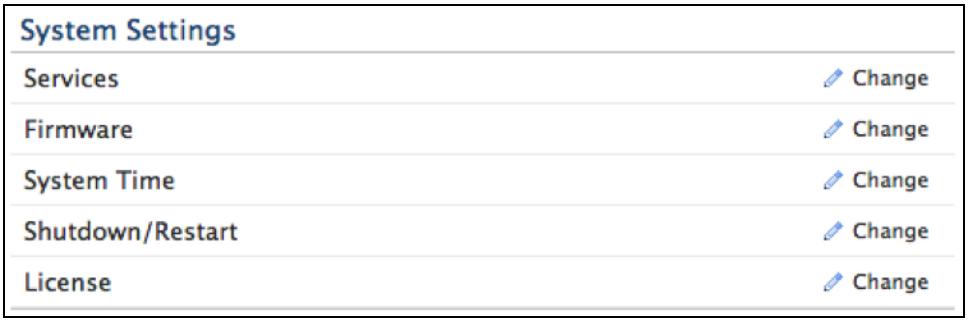
1. On the front of the appliance, pull open the last slot.
2. Insert the SSD for packet capture that you received from ExtraHop.

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

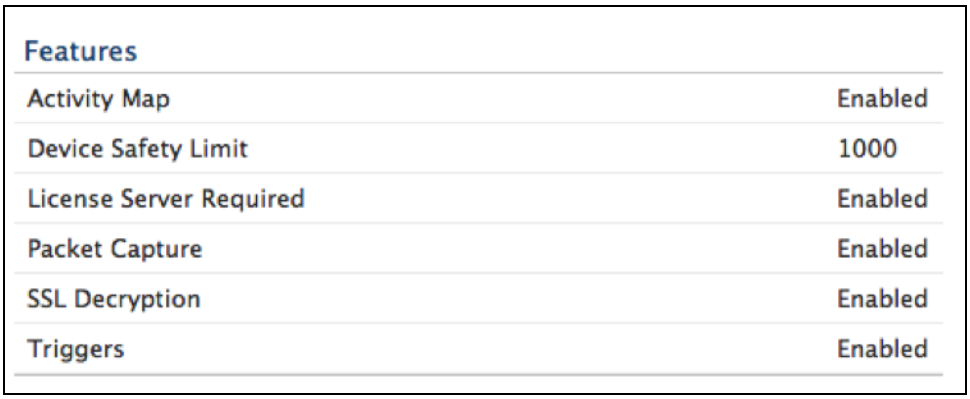
Enabling Packet Capture

Ensure that your ExtraHop license has packet capture enabled.

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



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.



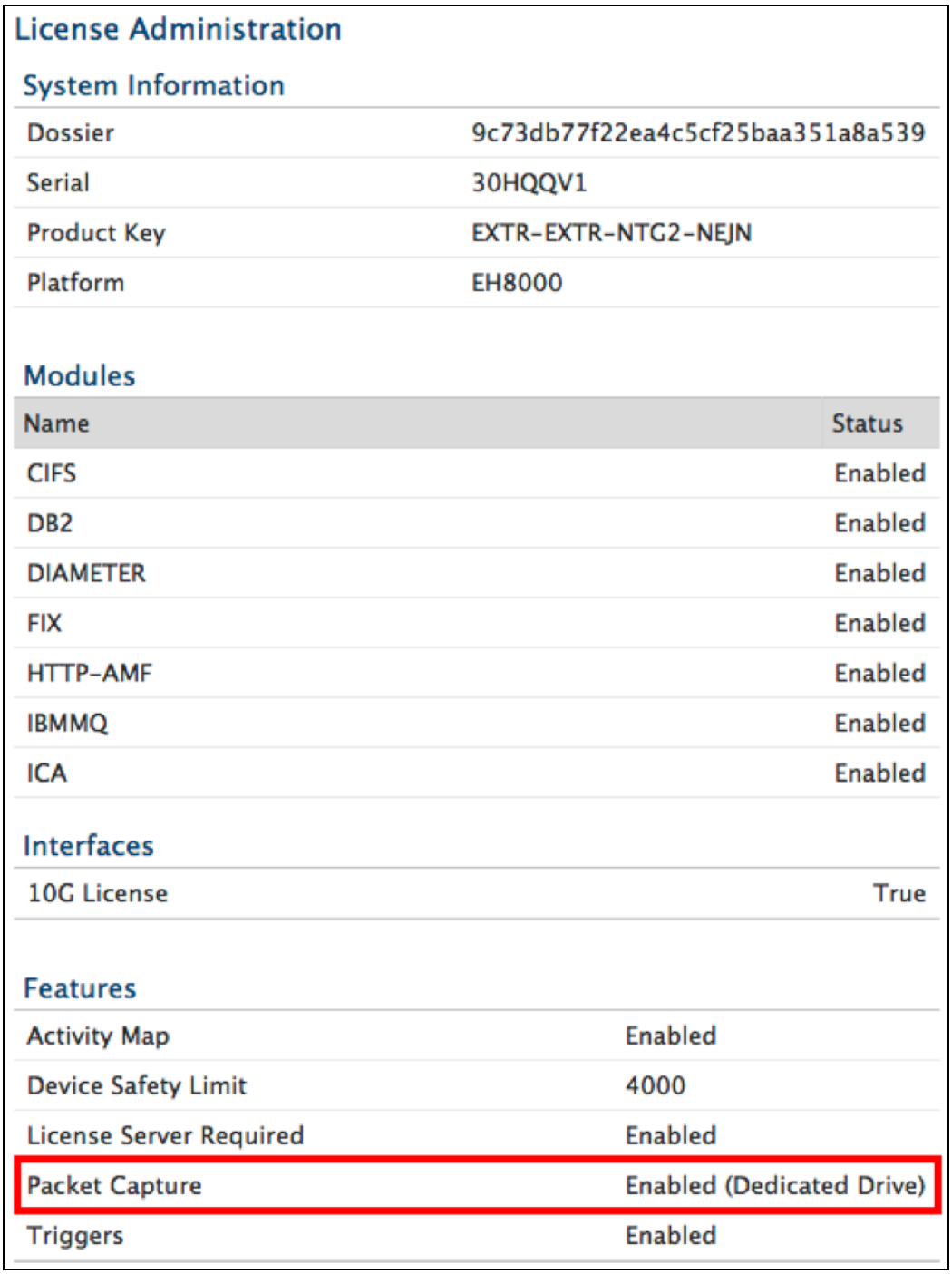
3. The ExtraHop requires a product key and a license in order to use packet capture. Contact ExtraHop Support (support@extrahop.com) to obtain your product key.

   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.

   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

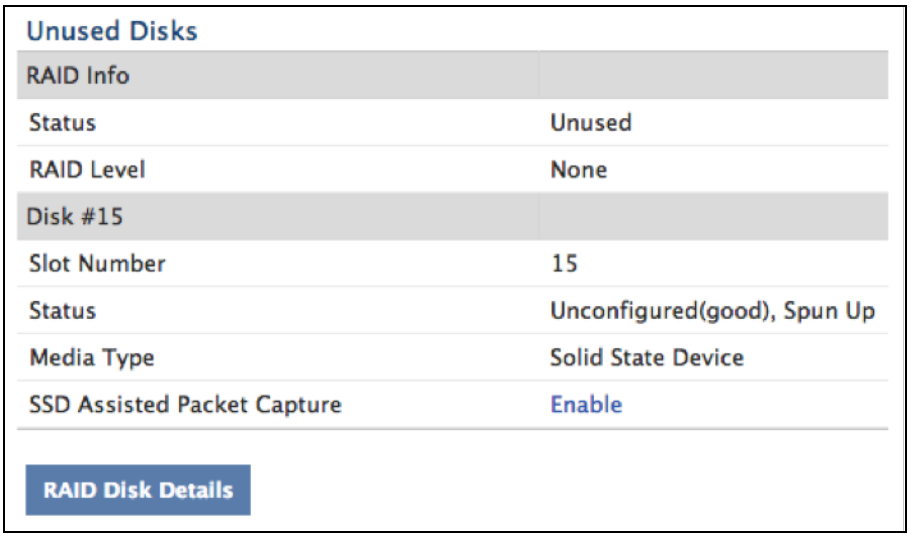
10G License	True

Features

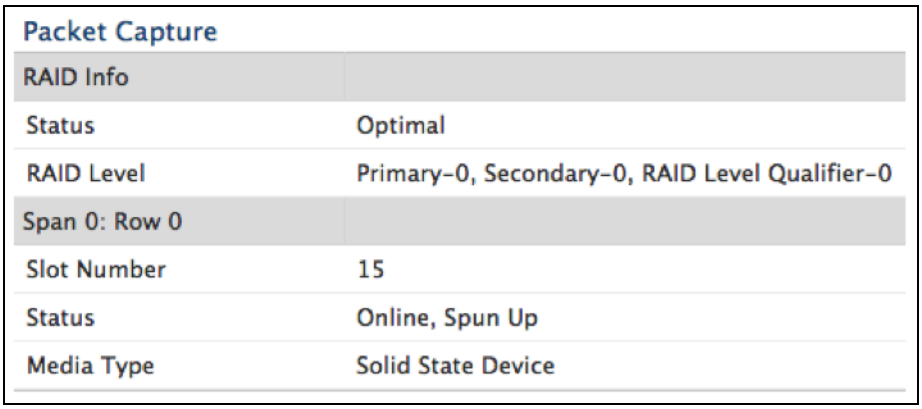
Activity Map	Enabled
Device Safety Limit	4000
License Server Required	Enabled
Packet Capture	Enabled (Dedicated Drive)
Triggers	Enabled

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**.



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



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.

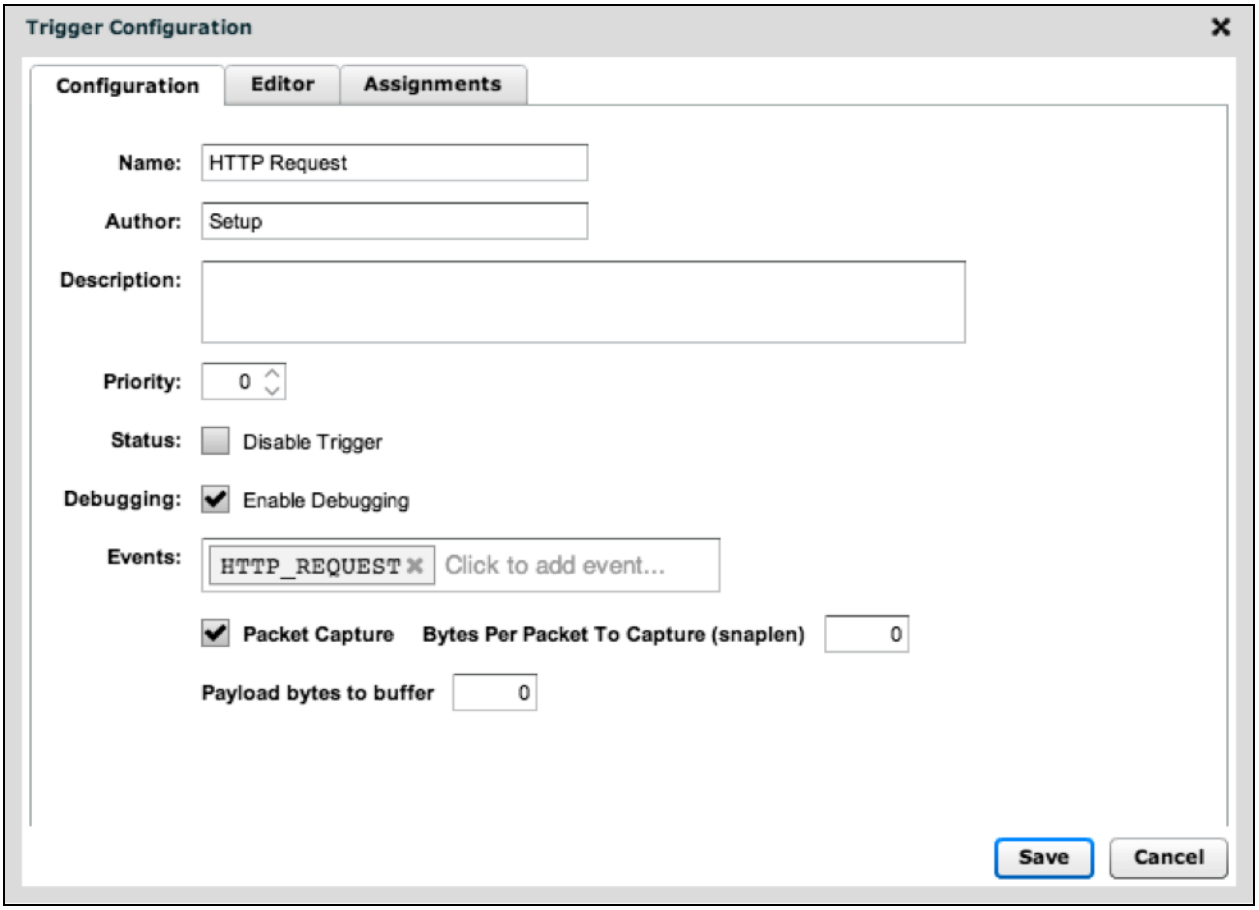
For information about writing triggers, refer to the following related documentation:

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

To create a trigger, complete the following steps:

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

checkbox.



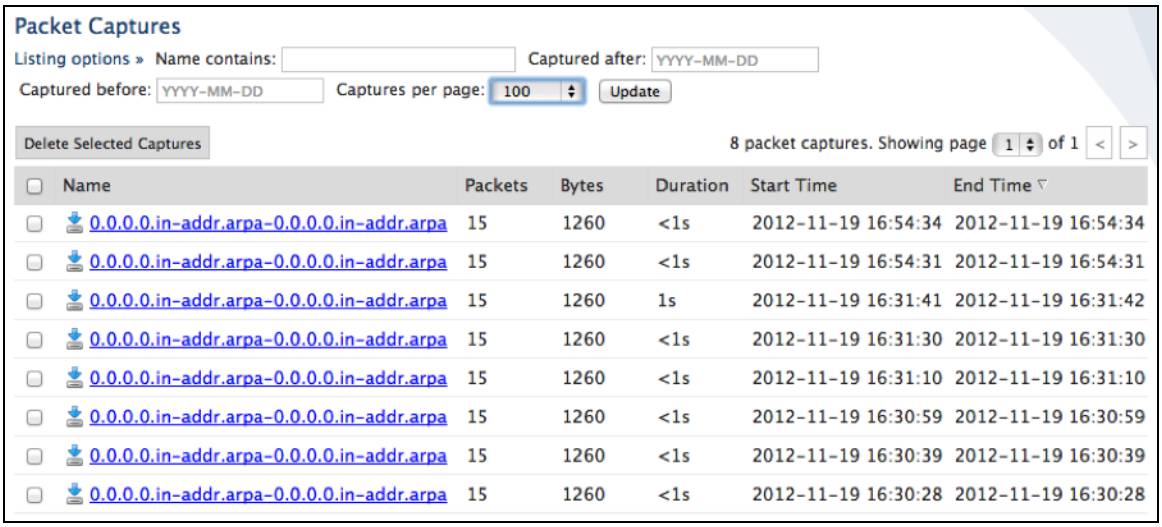
Once you have tested the trigger to ensure it works, uncheck **Enable Debugging** to avoid excessive debug messages in the Runtime Log.

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.



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