

Deploy the IDS sensor with VMware

Published: 2024-05-03

Published: 2024-05-03

Intrusion Detection System (IDS) sensors integrate with packet sensors to generate detections based on industry-standard IDS signatures. This guide explains how to deploy the IDS sensor with VMware.

Before you begin

- You must have familiarity with administering VMware. The images in this guide are from VMware version 6.7, and some of the menu selections might have changed.
- We recommend that you upgrade to the latest patch for the vSphere environment to avoid any known issues.

This guide explains how to deploy the following ExtraHop virtual sensors on the VMware ESXi/ESX platform:

- IDS 6280v

Virtual machine requirements


Your hypervisor must be able to support the following specifications for the virtual sensor.

- VMware ESX/ESXi server version 6.5 or later
- vSphere client to deploy the OVF file and to manage the virtual machine
- (Optional) If you want to enable packet captures, configure an additional storage disk during deployment
- The following table provides the server hardware requirements for each Discover appliance model:

Sensor	CPU	RAM	Disk
IDS 1280v	4 processing cores with hyper-threading support, VT-x or AMD-V technology, and 64-bit architecture. Streaming SIMD Extensions 4.2 (SSE4.2) and POPCNT instruction support.	8 GB	46 GB or larger disk for data storage (thick-provisioned) 250 GB or smaller disk for packet captures (thick-provisioned)
IDS 6280v	16 processing cores with hyper-threading support, VT-x or AMD-V technology, and 64-bit architecture. Streaming SIMD Extensions 4.2 (SSE4.2) and POPCNT instruction support.	64 GB	1 TB or larger disk for data storage (thick-provisioned) 500 GB or smaller disk for packet captures (thick-provisioned)

To ensure proper functionality of the virtual sensor:


- Make sure that the VMware ESX/ESXi server is configured with the correct date and time.
- Always choose thick provisioning. The ExtraHop datastore requires low-level access to the complete drive and is not able to grow dynamically with thin provisioning. Thin provisioning can cause metric loss, VM lockups, and capture issues.


- Do not change the default disk size on initial installation. The default disk size ensures correct lookback for ExtraHop metrics and proper system functionality. If your configuration requires a different disk size, contact your ExtraHop representative before you make any changes.
 - Do not migrate the VM. Although it is possible to migrate when the datastore is on a remote SAN, ExtraHop does not recommend this configuration. If you must migrate the VM to a different host, shut down the virtual sensor first and then migrate with a tool such as VMware VMotion. Live migration is not supported.
-  **Important:** If you want to deploy more than one ExtraHop virtual sensor, create the new instance with the original deployment package or clone an existing instance that has never been started.

Network requirements

The following table provides guidance about configuring network ports for the IDS sensor.

Sensor	Management	Monitor
IDS 6280v	One 1 GbE network port is required (for management). The management interface must be accessible on port 443. The management interface can be configured as an additional ERSPAN/RPCAP target.	A 10 GbE network port is recommended for the physical port mirror. The physical port mirror interface must be connected to the port mirror destination on the switch. The VMware ESX server must support network interface drivers. Optionally, you can configure 1-3 1 GbE network ports to receive packet monitor traffic.

 **Important:** To ensure the best performance for initial device synchronization, connect all sensors to the console and then configure network traffic forwarding to the sensors.

 **Note:** For registration purposes, the virtual sensor requires outbound DNS connectivity on UDP port 53 unless managed by an ExtraHop console.

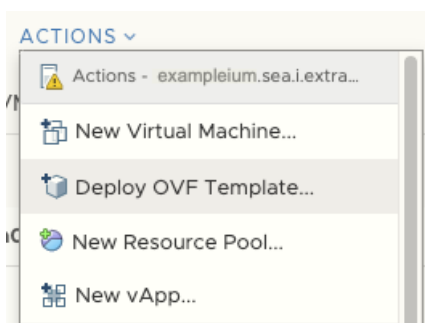
Deploy the OVA file through the VMware vSphere web client

ExtraHop distributes the virtual sensor package in the open virtual appliance (OVA) format.


Before you begin

If you have not already done so, download the ExtraHop virtual sensor OVA file for VMware from the [ExtraHop Customer Portal](#).

1. Start the VMware vSphere web client and connect to your ESX server.
2. Select the data center where you want to deploy the virtual sensor.
3. Select **Deploy OVF Template...** from the Actions menu.




4. Follow the wizard prompts to deploy the virtual machine. For most deployments, the default settings are sufficient.
 - a) Select Local file and then click **Choose Files**.
 - b) Select the OVA file on your local machine and then click **Open**.
 - c) Click **Next**.
 - d) Specify a name and location for the sensor and then click **Next**.
 - e) Select the destination compute resource location, verify that the compatibility checks are successful and then click **Next**.
 - f) Review the template details and then click **Next**.
 - g) For Disk Format, select **Thick Provision Lazy Zeroed** and then click **Next**.
 - h) Map the OVF-configured network interface labels with the correct ESX-configured interface labels and then click **Next**.
 - i) Verify the configuration and then click **Finish** to begin the deployment. When the deployment is complete, you can see the unique name you assigned to the ExtraHop VM instance in the inventory tree for the ESX server to which it was deployed.
5. The sensor contains a preconfigured bridged virtual interface with the network label, VM Network. If your ESX has a different interface label, you must reconfigure the network adapter on the virtual sensor before starting the sensor.
 - a) Select the Summary tab.
 - b) Click **Edit Settings**, select **Network adapter 1**, select the correct network label from the Network label drop-down list, and then click **OK**.
6. Select the virtual sensor in the ESX Inventory and then select **Open Console** from the Actions menu.
7. Click the console window and then press ENTER to display the IP address.

 **Note:** DHCP is enabled by default on the ExtraHop virtual sensor. To configure a static IP address, see the [Configure a Static IP Address](#) section.
8. In VMware ESXi, configure the virtual switch to receive traffic and restart to see the changes.

Configure a static IP address through the CLI

The ExtraHop system is configured by default with DHCP enabled. If your network does not support DHCP, no IP address is acquired, and you must configure a static address manually.

You can manually configure a static IP address for the ExtraHop system from the CLI.

 **Important:** We strongly recommend [configuring a unique hostname](#). If the system IP address changes, the ExtraHop console can re-establish connection easily to the system by hostname.

1. Access the CLI through an SSH connection, by connecting a USB keyboard and SVGA monitor to the physical ExtraHop appliance, or through an RS-232 serial (null modem) cable and a terminal emulator program. Set the terminal emulator to 115200 baud with 8 data bits, no parity, 1 stop bit (8N1), and hardware flow control disabled.

2. At the login prompt, type `shell` and then press ENTER.
3. At the password prompt, type `default`, and then press ENTER.
4. To configure the static IP address, run the following commands:

- a) Enable privileged commands:

```
enable
```

- b) At the password prompt, type `default`, and then press ENTER.
- c) Enter configuration mode:

```
configure
```

- d) Enter interface configuration mode:

```
interface
```

- e) Specify the IP address and DNS settings in the following format:

```
ip ipaddr <ip_address> <netmask> <gateway> <dns_server>
```

For example:

```
ip ipaddr 10.10.2.14 255.255.0.0 10.10.1.253 10.10.1.254
```

- f) Leave interface configuration mode:

```
exit
```

- g) Save the running configuration file:

```
running-config save
```

- h) Type `y` and then press ENTER.

Configure the system

Perform the following procedures to configure the IDS sensor.

1. [Register your ExtraHop system](#).
2. [Connect to ExtraHop Cloud Services](#).
3. Connect your console to the sensor.
 - To connect to a self-managed console, see [Connect an ExtraHop console to an ExtraHop sensor](#).
 - To connect to Reveal(x) 360, see [Connect to Reveal\(x\) 360 from self-managed sensors](#).
4. Join the IDS sensor to a site.
 - For Reveal(x) Enterprise
 1. On the Manage Connected Appliances page of the console, click **Actions** next to the IDS sensor and then click **Join Site** from the Appliance Actions drop-down list.
 2. From the Associated Site drop-down list, click the name of the site you want to join. You must join a site that has the same network feed as the IDS sensor.
 3. Click **Join Site**.
 - For Reveal(x) 360
 1. On the Reveal(x) 360 **Administration** > **Sensors** page, select the checkbox next to the name of the IDS sensor.
 2. On the Sensor Details pane, select the name of the site you want to join from the **Associated Site** drop-down list. You must join a site that has the same network feed as the IDS sensor.
 3. Click **Join Site**.

5. Optional: Select the IDS Detections [tuning parameter](#) to enable detections for inbound traffic from external endpoints.
By default, the ExtraHop system will only generate detections for internal traffic.
6. Complete the recommended procedures in the [post-deployment checklist](#).