Setting up ESET NOD32 Collector

https://campus.barracuda.com/doc/101056839/

This setup is for the XDR Collector only. If you are using a physical or virtual sensor, refer to Integrating with ESET NOD32 Antivirus.

To integrate the ESET NOD32 collector, do the following:

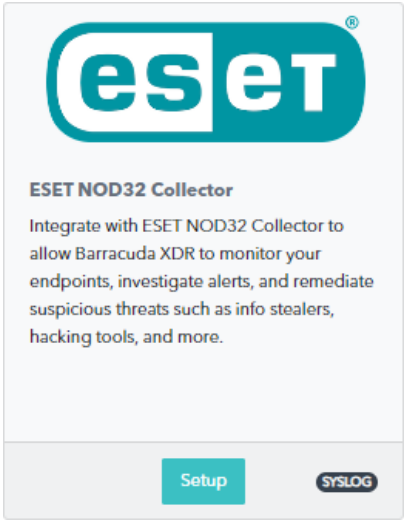
- **Enable the ESET NOD32 Collector**
- **Install the XDR Collector**
- **Configure ESET NOD32**

- **Open the port on the XDR Collector Host**

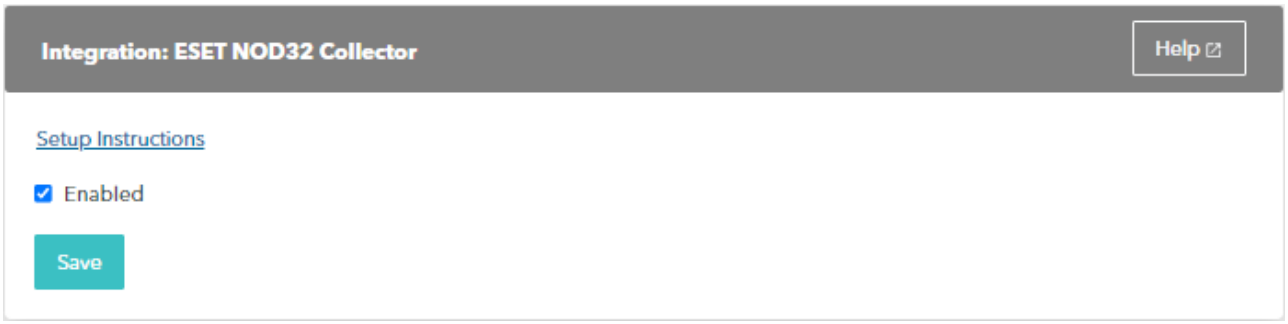
Enable the ESET NOD32 Collector

---

1. In **Barracuda XDR Dashboard**, navigate to **Administration** > **Integrations**.
2. On the **ESET NOD32 Collector** card, click **Setup**.



3. Select the **Enabled** check box.



4. Click **Save**.

Install the XDR Collector

When collecting logs from one or more integrated data sources, always set up the XDR Collector on a dedicated host server. Don't use an existing server because the amount of data produced by logs can impact critical infrastructure.

- If you haven't already set up the XDR Collector, do one of the following:
  - Setting up the XDR Collector for Windows
  - Setting up the XDR Collector for Linux

Configure ESET NOD32

If you have a Syslog server running in your network, you can configure ERA Server to send Notifications to your Syslog server. You can also enable Export logs to Syslog in order to receive certain events from client computers running ESET Endpoint Security, for example. Events from the following log categories are exported to Syslog server: Threat, Firewall, HIPS, Audit.

To enable the Syslog server

1. In ESET, click **Admin** > **Server Settings** > **Advanced Settings** > **Syslog Server**.
2. Click the slider bar next to **Use Syslog server**.
3. Specify the following mandatory settings:
   - **Host** (IP address or hostname of the destination for Syslog messages)
   - **Port number**: 9230
   - **Format of the log**: BSD (specification), Syslog (specification)
   - **Transport protocol for sending messages to Syslog** (UDP, TCP, TLS)
4. After making changes, click **Save**.

Open the port on the XDR Collector Host

Ensure incoming traffic is allowed on UDP port 9230.

Linux

```
sudo ufw allow 9230/udp
```

Windows

```
netsh advfirewall firewall add rule name="ESET NOD32 Events" dir=in
action=allow protocol=UDP localport=9230
```

Figures