Setting up Sophos XG Collector

https://campus.barracuda.com/doc/99621502/

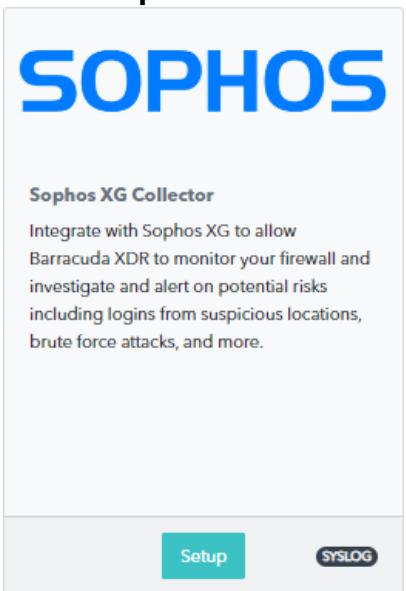
This setup is for the XDR Collector only. If you are using a physical or virtual sensor, refer to Integrating Sophos XG.

To set up Sophos XG Collector, follow the procedures below:

- **Enable Sophos XG Collector**
- **Install the XDR Collector**
- **Configure the Firewall**
- **Open port on the XDR Collector Host**

Enable Sophos XG Collector

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



3. Select the **Enable** check box.

4. Click **Save**.

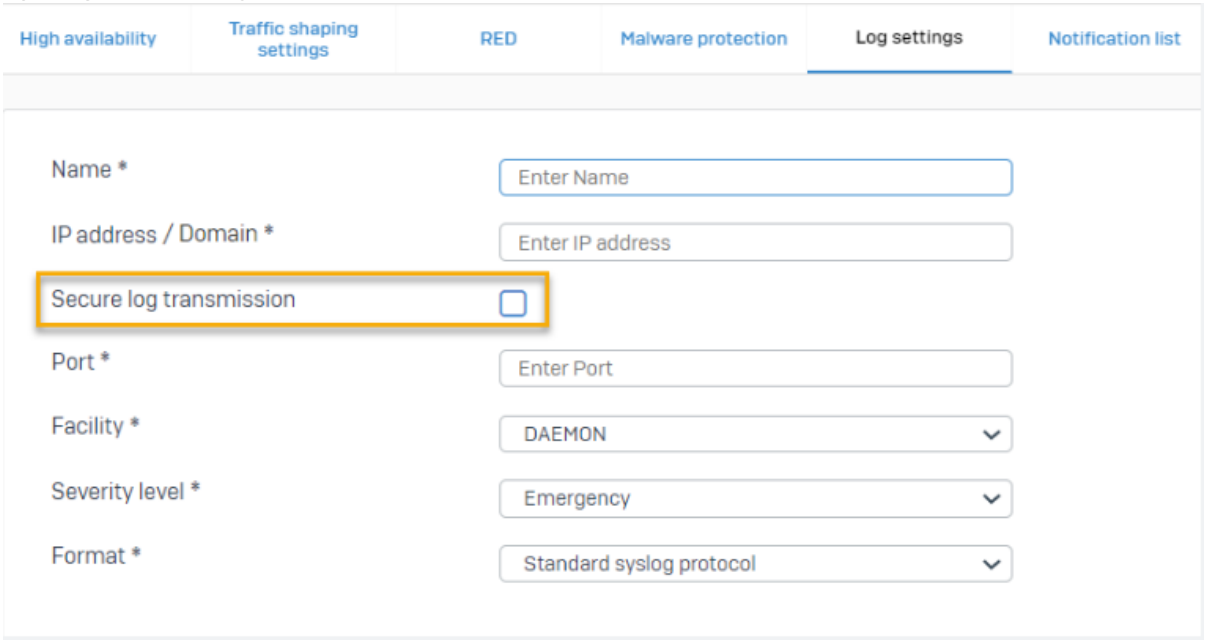
Install the XDR Collector

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 the Firewall

1. Go to **System Services** > **Log settings** and click **Add**.
2. Enter a name.
3. Specify the settings.



4. Type 9208 in **Port**.
   Your Syslog server must use port 9208.
5. Click **Save**.
6. Go to **Log settings** and select the logs you want to send to the syslog server.

For more information, see the Sophos Firewall Documentation.

Open port on the XDR Collector Host

Ensure incoming traffic is allowed on UDP port 9208.

Linux

```
sudo ufw allow 9208/udp
```

Windows

```
netsh advfirewall firewall add rule name=“Sophos XG Firewall Events” dir=in
action=allow protocol=UDP localport=9208
```

Figures

1. 2024-02-29_13-20-10.png
2. 2024-02-29_13-21-13.png
3. sophos-xg-syslog-server-config.png