Setting up Sophos UTM Collector

https://campus.barracuda.com/doc/99621497/

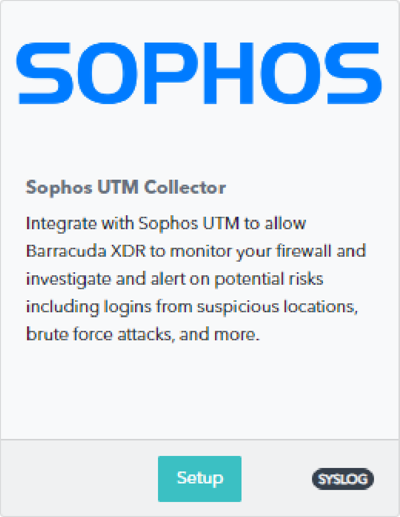
This setup is for the XDR Collector only. If you are using a physical or virtual sensor, refer to Integrating Sophos UTM.

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

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

Enable Sophos UTM Collector

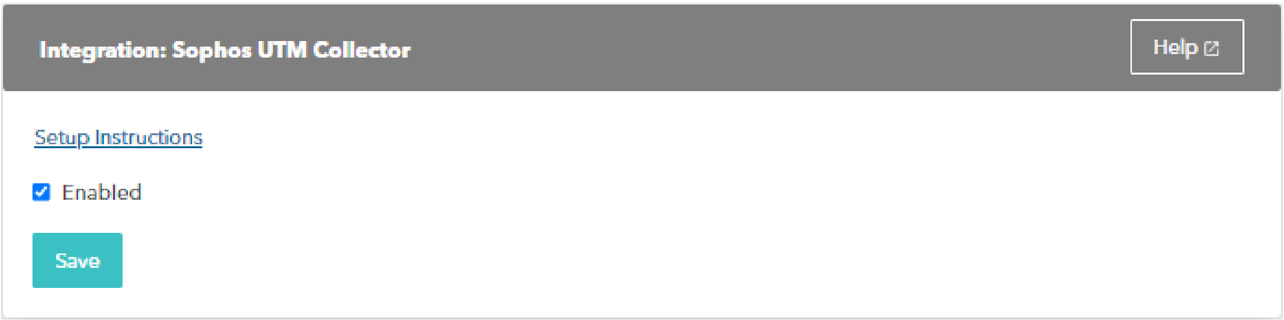
1. In **Barracuda XDR Dashboard**, navigate to **Administration** > **Integrations**.
2. On the **Sophos UTM Collector** card, click **Setup**.



Sophos UTM Collector

Integrate with Sophos UTM to allow Barracuda XDR to monitor your firewall and investigate and alert on potential risks including logins from suspicious locations, brute force attacks, and more.

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


Integration: Sophos UTM Collector

Setup Instructions

☑ Enabled

4. Click **Save**.

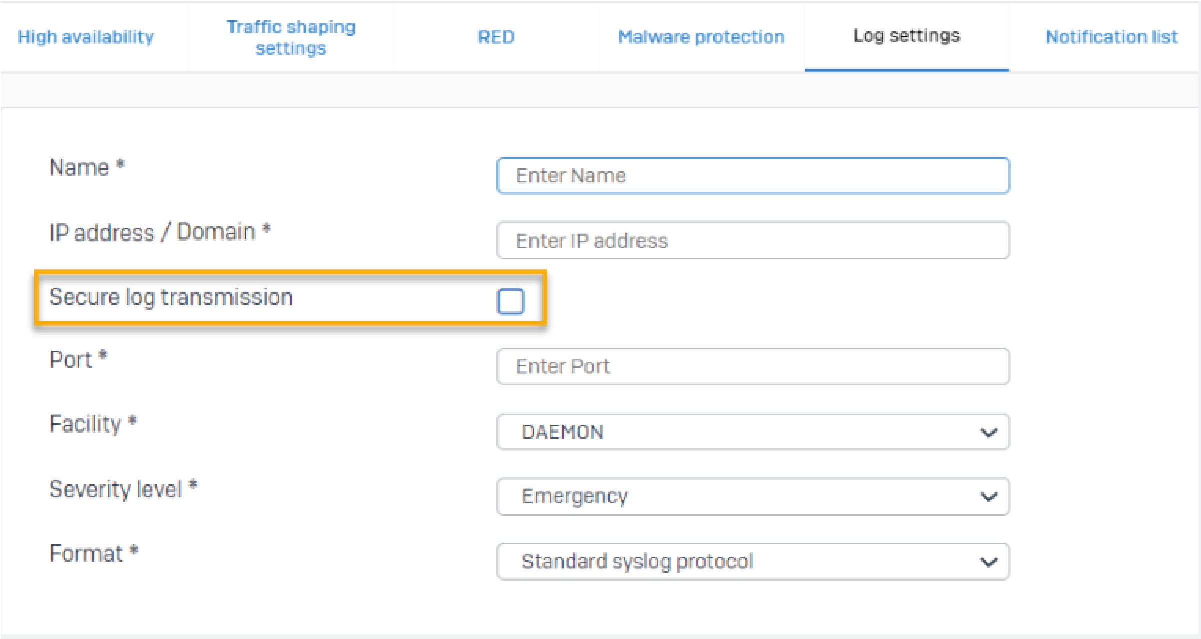
Install the XDR Collector

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. In **Sophos UTM Firewall**, click **System services** > **Log settings**.
2. Click **Add**.
3. Enter a name.
4. Specify the settings like the graphic below.



Name * Enter Name

IP address / Domain * Enter IP address

Secure log transmission □

Port * Enter Port

Facility * DAEMON

Severity level * Emergency

Format * Standard syslog protocol

5. Type *9207* in the **Port** field .
6. Click **Save**.
7. 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 the Port on the XDR Collector Host

Ensure incoming traffic is allowed on UDP port 9207.

Linux

```
sudo ufw allow 9207/udp
```

Windows

```
netsh advfirewall firewall add rule name="Sophos UTM Firewall Events" dir=in
action=allow protocol=UDP localport=9207
```

Figures