

Setting up Sophos UTM Collector

<https://campus.barracuda.com/doc/29817/>

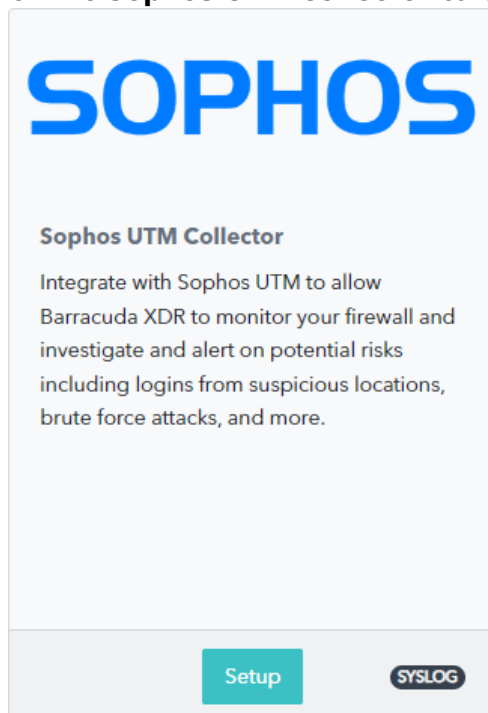
This setup is for the XDR Collector only. If you are using a physical or virtual sensor, refer to [Integrating Sophos UTM](#).

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

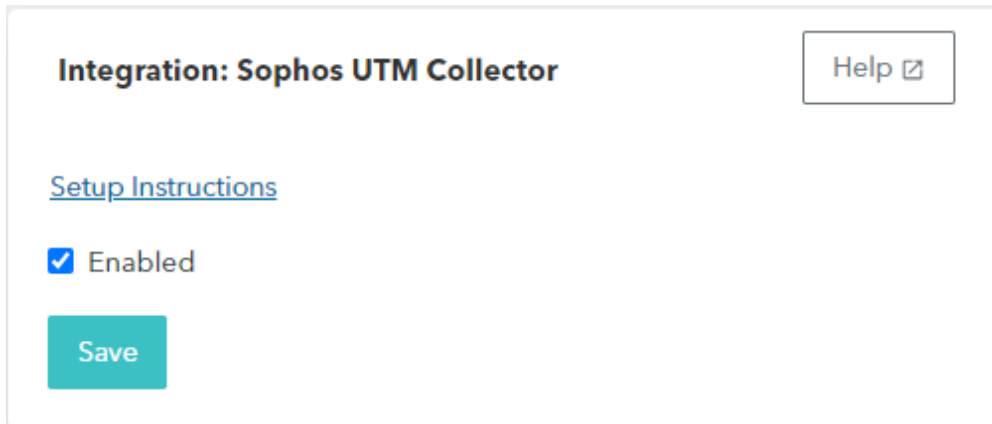
- **Enable Sophos UTM Collector**
- **Install the XDR Collector**
- **Configure the Firewall**
- **Open the port on the XDR Collector Host**

Enable Sophos UTM Collector

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



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 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.

High availability	Traffic shaping settings	RED	Malware protection	Log settings	Notification list
<div><div>Name *</div><div>Enter Name</div></div> <div><div>IP address / Domain *</div><div>Enter IP address</div></div> <div><div>Secure log transmission</div><div><input type="checkbox"/></div></div> <div><div>Port *</div><div>Enter Port</div></div> <div><div>Facility *</div><div>DAEMON</div><div>▼</div></div> <div><div>Severity level *</div><div>Emergency</div><div>▼</div></div> <div><div>Format *</div><div>Standard syslog protocol</div><div>▼</div></div>					

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

1. SophosUTMCard.png
2. SophosUTMEdit.png
3. SophosUTMStep4.png

© Barracuda Networks Inc., 2025 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.