Setting up the Broadcom Endpoint Security Collector

https://campus.barracuda.com/doc/99621413/

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

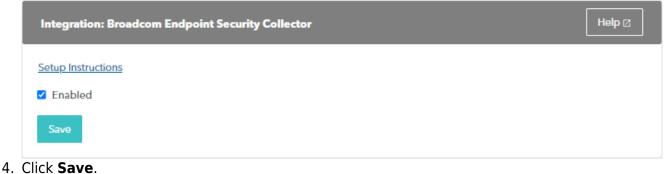To set up the Broadcom Endpoint Security Collector, do the following steps, below:

- **Enable the Broadcom Endpoint Security Collector integration**
- **Install the XDR Collector**
- **Configure the Firewall**
- **Open the port on the XDR Collector Host**

Enable the Broadcom Endpoint Security Collector

1. In **Barracuda XDR Dashboard**, navigate to **Administration > Integrations**.
2. On the **Broadcom Endpoint Security 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

- To add a syslog server to the Broadcom Endpoint Security Firewall follow the steps that can be found in Broadcom Endpoint Security Firewall Documentation
- When entering the necessary information for each syslog server that is added, make sure that the port is pointing to 9231, not to the default port that is mentioned in the documentation.

Open the port on the XDR Collector Host

Ensure incoming traffic is allowed on UDP port 9231.

Linux

```
sudo ufw allow 9231/udp
```

Windows

```
netsh advfirewall firewall add rule name="Broadcom Endpoint Security Events"
dir=in action=allow protocol=UDP localport=9231
```

Figures

1. 2024-02-29_11-10-24.png
2. 2024-02-29_11-11-04.png