Setting up F5 BIG-IP Collector
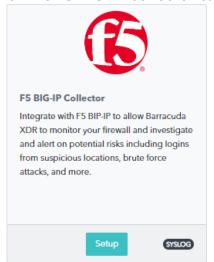
https://campus.barracuda.com/doc/101712556/

This setup is for the XDR Collector only. If you are using a physical or virtual sensor, refer to Integrating F5 BIG-IP.

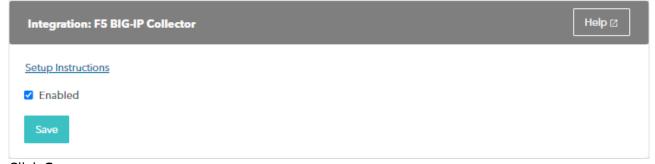To set up F5 BIG-IP collector, do the following:

- **Enable F5 BIG-IP collector**
- **Install the XDR Collector**
- **Configure the firewall**
- **Open the port on the XDR Collector Host**

Enable F5 BIG-IP Collector

1. In **Barracuda XDR Dashboard**, navigate to **Administration** > **Integrations**.
2. On the **F5 BIG-IP Collector** card, click **Setup**.

F5 BIG-IP Collector

Integrate with F5 BIP-IP 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.

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

Configuring the Firewall

To add a Syslog server to the F5 BIG-IP Firewall follow the steps that can be found in the F5 BIG-IP Documentation.

When entering the necessary information for each syslog server that is added, make sure that the port is pointing to 9256, 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 9256.

Linux

```
sudo ufw allow 9256/udp
```

Windows

```
netsh advfirewall firewall add rule name="F5 BIG-IP Events" dir=in
action=allow protocol=UDP localport=9256
```

Figures

1. 2024-02-29_11-24-08.png
2. 2024-02-29_11-24-45.png