Install the Falcon Sensor for Linux

1. Download the Falcon sensor installer from Hosts > Sensor Downloads.
2. Copy your Customer ID Checksum (CID), displayed on Sensor Downloads.
3. Run the installer, substituting <installer\_package> with your installer's file name.
   * Ubuntu: sudo dpkg -i <installer\_package>
   * RHEL, CentOS, Amazon Linux: sudo yum install <installer\_package>
   * SLES: sudo zypper install <installer\_package>
4. Set your CID on the sensor, substituting <CID> with your CID.This step is not required for versions 4.0 and earlier.
   * All OSes: sudo /opt/CrowdStrike/falconctl -s --cid=<CID>
5. Start the sensor manually. This step is not required for versions 4.0 and earlier.
   * Hosts with SysVinit: service falcon-sensor start
   * Hosts with Systemd: systemctl start falcon-sensor
6. Confirm the sensor is running.
   * All OSes: ps -e | grep falcon-sensor

You'll see output similar to this:

[root@centos6-installtest ~]# sudo ps -e | grep falcon-sensor   905 ?         00:00:02 falcon-sensor

Optional: Prepare a Host as a Master Image

If you're preparing a host as a "master" device for cloning or virtualization, you must remove your "master" host's agent ID (AID).

Run this command after installing: sudo /opt/CrowdStrike/falconctl -d -f --aid

When your cloned devices or virtual machines first contact the CrowdStrike cloud, they'll be automatically assigned a unique AID. If multiple devices use the same AID, the Falcon console will process all their events as though they came from a single device.

Optional: Configure a Proxy

If your hosts use a proxy, configure the Falcon sensor to use it:

* Configure proxy: sudo /opt/CrowdStrike/falconctl -s --aph=<proxy host> --app=<proxy port>
* Confirm config: sudo /opt/CrowdStrike/falconctl -g --aph --app
* Enable proxy: sudo /opt/CrowdStrike/falconctl -s --apd=FALSE
* Disable proxy: sudo /opt/CrowdStrike/falconctl -s --apd=TRUE

Uninstall the Falcon Sensor for Linux

Run these commands to uninstall the Falcon sensor from your host:

* Ubuntu: sudo apt-get purge falcon-sensor
* RHEL, CentOS, Amazon Linux: sudo yum remove falcon-sensor
* SLES: sudo zypper remove falcon-sensor

### Verify that the Sensor is Running

1. Check running processes to verify the Falcon sensor is running: ps -e | grep -e falcon-sensor
2. Check kernel modules to verify the Falcon sensor's kernel modules are running: lsmod | grep falcon
3. Check the Falcon sensor's configurable options: sudo /opt/CrowdStrike/falconctl -g

Optional parameters:

* + --aid: the sensor's agent ID
  + --cid: your Customer ID
  + --apd: the sensor's proxy status (enabled or disabled)
  + --aph: the sensor's proxy host
  + --app: the sensor's proxy port

The sensor requires these runtime services:

* network
* systemd
  + local-fs
  + sysinit
  + multi-user
  + shutdown

### Verify the Sensor Files on Disk

If the sensor is not running, verify that the sensor's application files exist on your host:

$ sudo ls -al /opt/CrowdStrike /opt/CrowdStrike/falcon-sensor

This should be a symlink to either:

* the original sensor installation at /opt/CrowdStrike/falcon-sensor
* a sensor update package with a release build number, such as /opt/CrowdStrike/falcon-sensor3000

### Verify that the Sensor is Connected to the Cloud

There are two ways to verify that a sensor is connected to the CrowdStrike cloud:

* Falcon console: Search for the host in Hosts > Host Management. To view a complete list of newly installed sensors, use the Sensor Report.
* From the host: Check network statistics using the command line: sudo netstat -tapn | grep falcon

If the Falcon sensor is communicating with the cloud, you'll see output like this:

tcp        0      0    192.0.2.176:35382       ec2-54-148-96-12:443           ESTABLISHED 3228/falcon-sensor

## Sensor Logging

Providing logs to our support team can help diagnose sensor issues. Logs are stored within your host's syslog.

Syslog locations vary, but are specified in /etc/syslog.conf or rsyslog.conf, with these being the most common:

* /var/log/messages
* var/log/syslog
* /var/log/rsyslog
* /var/log/daemon

grep for the string falcon for sensor logs:

example: sudo grep falcon /var/log/messages | tail -n 100

Logs are kept according to your host's log rotation settings. For assistance gathering or reviewing logs, contact Support.