

Sensor Deployment and Maintenance

06/08/2026

Copyright © CrowdStrike

1. Deploy Falcon Sensor for Linux Using CLI

1.1. Overview

1.2. Before you begin

1.2.1. Installing the Falcon sensor

1.2.2. Verifying sensor installation

1.2.2.1. Verifying user mode

Deploy Falcon Sensor for Linux Using CLI

Use this procedure to perform a standard installation of Falcon sensor for Linux on an endpoint or node using a sensor installer that you run from the command line interface (CLI).

Overview

Deploying Falcon sensor for Linux on the host provides runtime protection for the host and, if applicable, the containers running on the host.

To install the Falcon sensor on an endpoint or node, perform these procedures:

1. Install the Falcon sensor
2. Verify the installation
3. Optionally, configure the Falcon sensor with post-installation options

For information about other installation considerations, see Installation Options for Falcon Sensor for Linux.

Before you begin

Before you install the Falcon sensor for Linux, refer to these topics to make sure you are installing the correct sensor, your environment meets system requirements, you are using the correct deployment method and installation type, you are aware of any additional installation options your installation requires:

- Choose the Right Sensor
- Falcon Sensor for Linux System Requirements
- Plan Your Falcon Sensor for Linux Deployment
- Installation Options for Falcon Sensor for Linux

Installing the Falcon sensor

1. Download the Falcon sensor installer from Host setup and management > Deploy > Sensor Downloads .
2. Copy your Customer ID Checksum (CID), displayed on Sensor Downloads.
3. Run the installer, substituting `<installer_filename>` with your installer's file name.

   Installing the sensor requires `sudo` privileges.

   - Ubuntu: `sudo dpkg -i <installer_filename>`
   - For RHEL, CentOS, Amazon Linux, choose either:
     - `sudo yum install <installer_filename>`
     - `sudo dnf install <installer_filename>`
   - SLES: `sudo zypper install <installer_filename>`
4. Set your CID on the sensor, substituting `<CID>` with your CID.
   - All OSes: `sudo /opt/CrowdStrike/falconctl -s --cid=<CID>`

5. Optional. Set the cloud where the endpoint's CID resides. (recommended)

   After installation, the sensor must connect to the CrowdStrike cloud where the endpoint's CID resides.

   You can let the sensor discover the CID's cloud automatically, or you can specify the cloud where the CID resides.

   Note: Automatic cloud discovery might take longer, especially if your network security tools restrict access to some CrowdStrike cloud endpoints. For optimal performance, particularly with ephemeral hosts, we recommend explicitly specifying the cloud.

   To specify the CrowdStrike cloud, run this command, choosing exactly one value for the `--cloud` option:

   - All OSes: `sudo /opt/CrowdStrike/falconctl -s --cloud={us-1 | us-2 | eu-1 | us-gov-1 | us-gov-2}`

   Note: Network requirements. To ensure efficient sensor provisioning, we strongly recommend that you allow all CrowdStrike cloud domains when you configure your networking security tools. If you're using a proxy, ensure it properly handles connection failures to CrowdStrike endpoints. For more info, see Networking requirements.

6. Start the sensor manually.

   - Hosts with SysVinit: `sudo service falcon-sensor start`
   - Hosts with Systemd: `sudo systemctl start falcon-sensor`

Verifying sensor installation

You can verify the sensor installation by using the Falcon console or a terminal on the host:

Falcon console	Host

After the sensor is installed, the host connects to the CrowdStrike cloud. You can confirm a sensor installation by reviewing your hosts in the Falcon console.
 	
Search for the host in Host setup and management > Manage endpoints > Host management.
 	
To view a complete list of newly installed sensors, use Dashboards and reports > Reports > Sensor report.
	To validate that the Falcon sensor for Linux is running on a host, run this command at a terminal:
	
	`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`

Verifying user mode

To see the hosts that are currently in user mode, go to the Host management page. See Host and Host Group Management.

To see Linux hosts online within the last 24 hours and that reported being in user mode, run this query:

```
#event_simpleName=/(OsVersionInfo|ConfigStateUpdate|SensorHeartbeat)/
| event_platform=Lin
| groupBy([cid, aid], function=([selectLast([ConfigStateData, OSVersionString, SensorStateBitMap])]))
| ConfigStateData match {
/1400000000c4/ => isInUserMode:=true ;
* => isInUserMode:=false ;
}
```

```
| bitfield:extractFlags(field="SensorStateBitMap", output=[[1, isInRFM]])
| case {
isInUserMode=false AND isInRFM=false | message := "Kernel Mode Enabled" ;
isInUserMode=false AND isInRFM=true | message := "Kernel Mode Enabled(RFM)" ;
isInUserMode=true AND isInRFM=false | message := "User Mode Enabled" ;
isInUserMode=true AND isInRFM=true | message := "User Mode Enabled(RFM)" ;
}
| OSVersionString = /^Linux\s(?<hostName>\S+)\s(?<kernelVersion>\S+)\s/i
| aid=?aid hostName=?hostName message=?message
| select([aid, hostName, Version, kernelVersion, isInRFM, isInUserMode, message])
```