

# CrowdStrike

## Installing the Falcon Sensor for Linux

### 1. Download the Falcon sensor installer

- Navigate to:  
Host Setup and Management > Deploy > Sensor Downloads  
URL (if you're in the Falcon UI): <https://falcon.us-2.crowdstrike.com/hosts/sensor-downloads>

### 2. Copy your Customer ID Checksum (CID)

- You'll find this value on the **Sensor Downloads** page.

### 3. Run the installer

- Replace <installer\_filename> with the actual file name you downloaded.
- Use the following command based on your operating system (requires `sudo` privileges):

#### Ubuntu/Debian:

```
sudo dpkg -i <installer_filename>
```

#### RHEL/CentOS/Amazon Linux:

```
sudo yum install <installer_filename>
```

or (if using DNF):

```
sudo dnf install <installer_filename>
```

#### SLES (SUSE Linux Enterprise Server):

```
sudo zypper install <installer_filename>
```

### 4. Set your CID

- Replace <CID> with the value you copied in step 2:

```
sudo /opt/CrowdStrike/falconctl -s --cid=<CID>
```

### 5. Start the sensor manually

#### For systems using SysVinit:

```
bash
CopyEdit
sudo service falcon-sensor start
```

**For systems using Systemd:**

```
sudo systemctl start falcon-sensor
```

## Tagging for Linux

To assign tags, use the `--tags` flag with `falconctl`:

```
bash
CopyEdit
sudo /opt/CrowdStrike/falconctl -s --tags="tag1,tag2,tag3"
```

- Tags must be comma-separated
- Tags should not contain spaces
- You can set multiple tags at once

## Verifying Falcon Sensor Installation (Linux)

### Method 2: Using the Terminal on the Host

To validate that the Falcon sensor is running on the host:

```
sudo ps -e | grep falcon-sensor
```

If the sensor is running, you'll see output similar to:

```
905 ?          00:00:02 falcon-sensor
```

This confirms that the process is active.

.


---

### Optional: Check service status (Systemd-based systems)

```
sudo systemctl status falcon-sensor
```

Tagging:

## Uninstalling the Falcon Sensor for Linux

 Important:

**Uninstalling the sensor** requires `sudo` privileges.

**If Uninstall and Maintenance Protection is enabled, you must retrieve a maintenance token before proceeding.**

---

### Step 1: Handle Maintenance Protection (If Enabled)

If **Uninstall and Maintenance Protection** is enabled:

1. Retrieve the maintenance token:
  - Refer to the Falcon console under:  
  
Host Setup and Management > Manage Endpoints
  - See the section: "**Making changes to a single host**" or "**Making changes to multiple hosts**" (for bulk operations).
2. Run this command with your token:

```
sudo /opt/CrowdStrike/falconctl -s --maintenance-token=<maintenance_token>
```

---

## **Step 2: Uninstall the Falcon Sensor**

Run the appropriate command for your Linux distribution:

### **Ubuntu/Debian:**

```
sudo apt-get purge falcon-sensor
```

### **RHEL / CentOS / Amazon Linux:**

```
sudo yum remove falcon-sensor
```

or (if using DNF):

```
sudo dnf remove falcon-sensor
```

### **SLES (SUSE Linux Enterprise Server):**

```
sudo zypper remove falcon-sensor
```

---

## ☒ **Optional: Confirm the Sensor is Removed**

Check that the `falcon-sensor` process is no longer running:

```
bash
CopyEdit
ps -e | grep falcon-sensor
```

**You should see no output if the sensor is successfully removed.**

## **SCP Command to Transfer Falcon Sensor**

```
scp <path_to_installer>/<installer_filename> <username>@<remote_host>:/tmp/
```

### **Example:**

```
scp falcon-sensor_6.58.0-14812.amd64.deb ubuntu@192.168.1.10:/tmp/
```

- Replace:
  - `<path_to_installer>` — local path to the installer
  - `<installer_filename>` — the name of the sensor installer file

- `<username>` — your SSH username on the remote host
- `<remote_host>` — IP or hostname of the Linux machine