How to Confirm that your CrowdStrike installation was successful
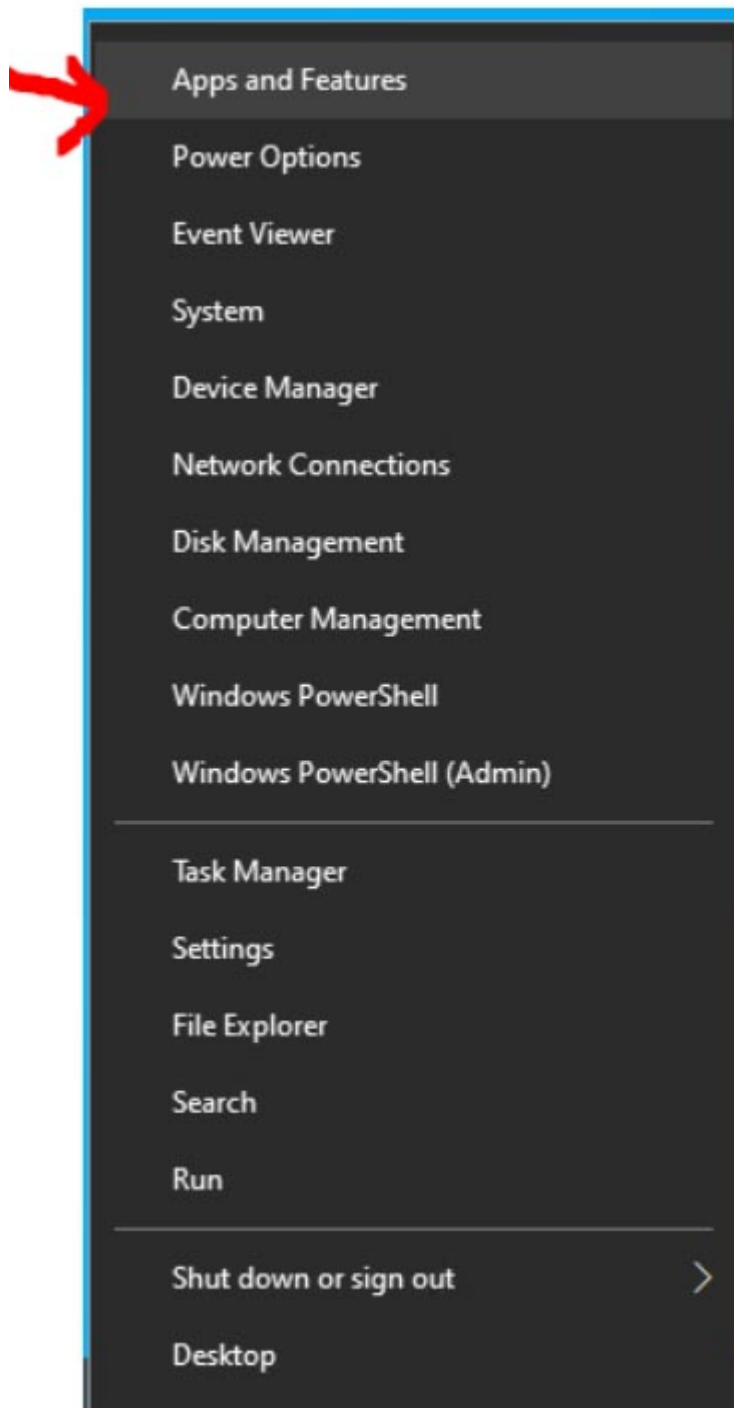
patricia falcon - 2022-05-10 - Comments (0) - Virtual Private Network

Since the CrowdStrike agent is intended to be unobtrusive to the user, knowing if it's been installed may not be obvious. This document provides details to help you determine whether or not CrowdStrike is installed and running for the following OS. *Note that the check applies both to the Falcon and Home versions*.
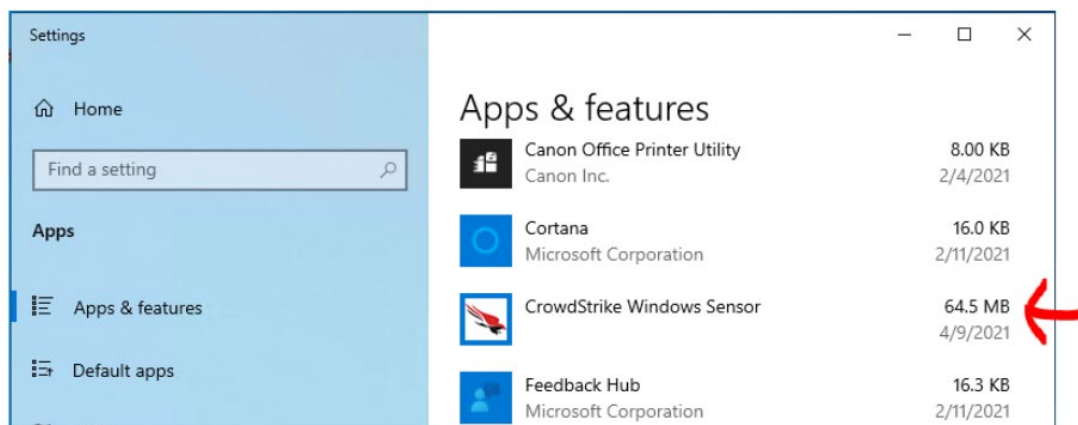
- **Windows**
- **Mac**
- **Linux**

Windows Machines

1. Right-click on the Start button, normally in the lower-left corner of the screen. Select Apps and Features.

Apps and Features

Power Options

Event Viewer

System

Device Manager

Network Connections

Disk Management

Computer Management

Windows PowerShell

Windows PowerShell (Admin)

Task Manager

Settings

File Explorer

Search

Run

Shut down or sign out

Desktop

2. In the new window that opens, scroll down until you locate "CrowdStrike Windows Sensor" in the list of installed apps.

3. If you cannot find an entry for "CrowdStrike Windows Sensor", CrowdStrike is NOT installed.

Command Line

To validate that the sensor is running on a Windows host via the command line, run this command at a command prompt:

```
sc query CSFalconService
```

If you see STATE: 4 RUNNING, CrowdStrike is installed and running.

macOS Machines

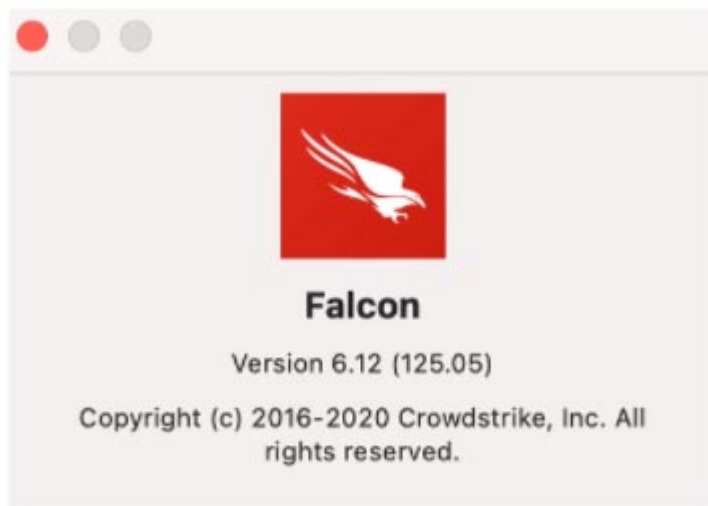**Launching the Application**

1. Go to your **Applications** folder.

Note: If you cannot find the Falcon application, CrowdStrike is **NOT** installed.
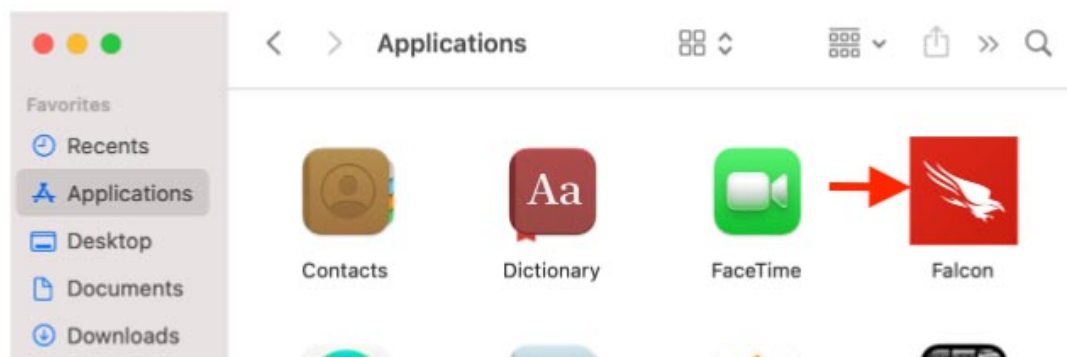
2. Locate the **Falcon** app and double-click it to launch it.

3. The application should launch and display the version number.

Command Line

You can also confirm the application is running through Terminal. Launch Terminal and input this command:

```
sudo /Applications/Falcon.app/Contents/Resources/falconctl stats agent_info
```

If Terminal displays command not found, Crowdstrike is not installed.

Linux Machines

To confirm the sensor is running, run the following command in terminal:

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

If you see a similar output as below, CrowdStrike is running.

```
[user@test ~]# sudo ps -e | grep falcon-sensor 635 ? 00:00:03 falcon-sensor
```