CrowdStrike Falcon - Installation Instructions

Prerequisite
You must have administrator rights to install the CrowdStrike Falcon Host Sensor.

Manual Installation

1. Get an installer from our CrowdStrike Falcon product page (This installer is provisioned for use at MIT.)
2. Launch the downloaded file
   - On Windows the name will be like FalconSensorWinOS.exe
   - On OSX the name will be like FalconSensorMacOSX.pkg
3. Accept the Falcon License Agreement
4. When prompted, click Yes or enter your computer password, to give the installer permission to run.
   - On Mac OS High Sierra, you may get a "System Extension Blocked" message. To enable CrowdStrike, you must approve the kernel extension from CrowdStrike in the Security & Privacy pane of the Mac OS System Preferences.

You are done! After installation, the sensor will run silently.

Normal operation

When installation is finished, the sensor runs silently. If it sees clearly malicious programs, it can stop the bad programs from running. If it sees suspicious programs, IS&T’s Security team will contact you.

To confirm the sensor is installed and running properly:

- **Windows**
  - Navigate to the command line and type:
    
    ```
    sc query csagent
    ```
  - Look for the STATE: RUNNING statement in the response:

    ```
    SERVICE_NAME: csagent
    TYPE : 2FILE_SYSTEM_DRIVER
    STATE : 4 RUNNING
    (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE : 0 (0x0)
    SERVICE_EXIT_CODE : 0 (0x0)
    CHECKPOINT : 0x0
    WAIT_HINT : 0x0
    ```

- **Mac OS**
  - Navigate to the Terminal command line and type:
    
    ```
    sysctl cs
    ```
  - You should see a lot of useful information, including:
    - `cs.version` - your currently installed sensor version
    - `cs.sensorid` - your unique sensor id
    - `cs.comms.cloud_ip` - the CrowdStrike IP your sensor is connected to
    - `cs.comms.cloud_connection_state`: if everything is working correctly, this should be 102
  - Version 4.18.8013 and above:
    - Network information previously obtained by executing `sysctl cs.comms` is now obtained by executing `sudo /Library/CS/falconctl stats`
The output of `sudo /Library/CS/falcon stats` will provide more detailed information on
  - Cloud connection state
  - Activity
  - Events sent and received

**Can it be uninstalled?**

- **Windows**
  - Go to the Control Panels, select Uninstall a Program, and select CrowdStrike Falcon Sensor

- **Mac OS**
  - This depends on the version of the sensor you are running. You can check using the `sysctl cs` command mentioned above, but unless you are still using Yosemite you should be on 4.x at this point.
    - Sensor version 3.9 and earlier, navigate to the Terminal command line and type:
      
      ```bash
      sudo sh /Library/CS/uninstall.sh
      ```
    - Sensor version 3.10 and later, navigate to the Terminal command line and type:
      
      ```bash
      sudo /Library/CS/falconctl uninstall
      ```
    - You can also unload/load the sensor if you think you are having problems:
      
      ```bash
      sudo /Library/CS/falconctl load
      sudo /Library/CS/falconctl unload
      ```

**More information**

If you have any questions about CrowdStrike, please contact the IS&T Security team at security@mit.edu