CrowdStrike Falcon - Installation Instructions

CrowdStrike Falcon - Installation Instructions

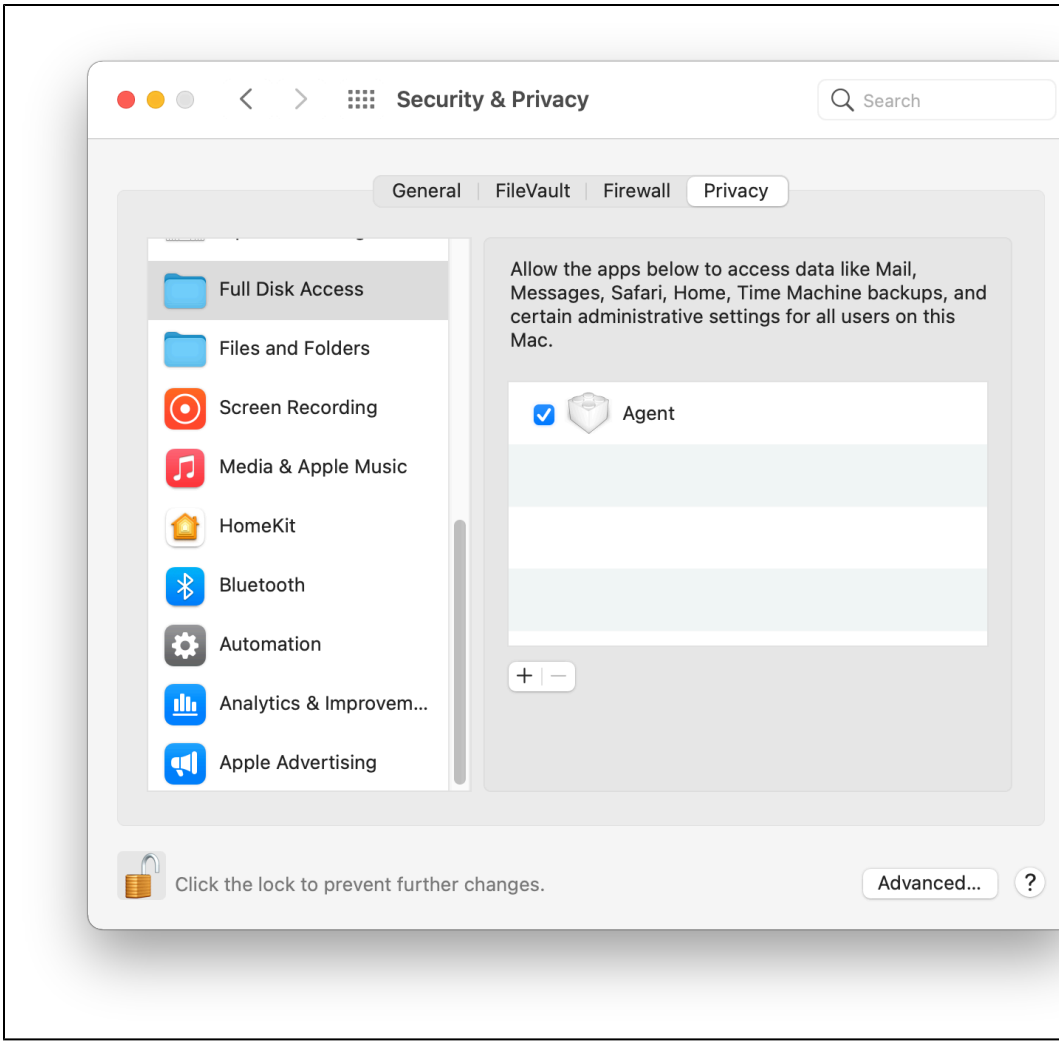
On this page:

Prerequisites

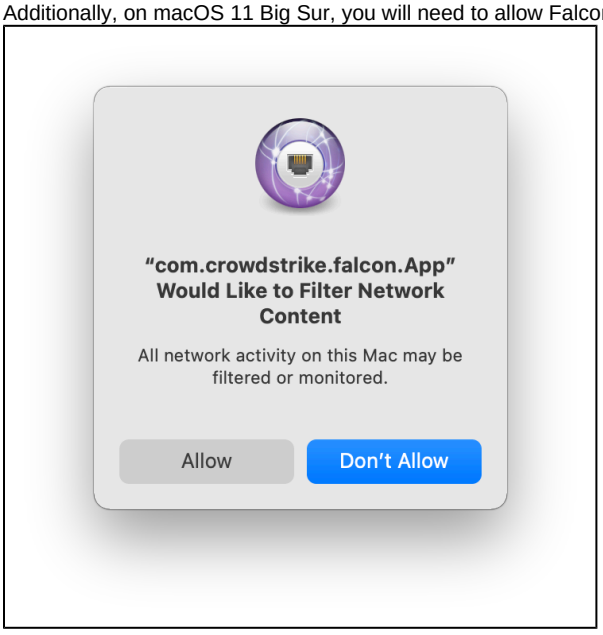
- You must have administrator rights to install the CrowdStrike Falcon Host Sensor.
- Your device must be running a supported operating system. The list of operating systems that CrowdStrike supports can be found on their FAQ.

Manual Installation

1. Get an installer from our MIT IS&T CrowdStrike Falcon product page (This installer is provisioned for use at MIT. Do not attempt to download directly from CrowdStrike.)
2. Launch the downloaded file
    - On Windows the name will be like **FalconSensorWinOS.exe**
    - On OSX the name will be like **FalconSensorMacOSX.pkg**
    - On Linux the name will be like **CrowdStrike_LinuxDeb_x86.tar.gz** or **CrowdStrike_LinuxRPM_x86.tar.gz** depending on the distribution
        - Do not attempt to install the package directly. Extract the package and use the provided installer.
        - For example:
          ```
          $ sudo tar xvzf CrowdStrike_LinuxDeb_<version>.tar.gz
          $ cd CrowdStrike; sudo ./MIT-CrowdStrike-Install-Deb.sh
          ```
3. Accept the Falcon License Agreement
4. When prompted, click Yes or enter your computer password, to give the installer permission to run.
    - On macOS 10.14 Mojave and greater, you will need to provide full disk access to the installer to function properly. Open System Preferences -> Security & Privacy -> Privacy -> Full Disk Access. Click the plus sign.
        - **Version 6** - Open System Preferences -> Security & Privacy -> Privacy -> Full Disk Access.
            - **macOS Big Sur and greater** - Check the box next to "Agent" which will already be listed but unchecked.



- Additionally, on macOS 11 Big Sur, you will need to allow Falcon to filter network content.



- Reboot your Mac after these changes.

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

Normal operation

When installation is finished,(on Windows you will not be notified when the install 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
```

- **macOS**
  - Version **6.11** and above:
    - The Falcon binary now lives in the applications folder at /Applications/Falcon.app
    - The output of `sudo /Applications/Falcon.app/Contents/Resources/falconctl stats` will provide more detailed information including connection state to the CrowdStrike cloud.

- **Linux**
  - Use one of the following commands to verify the service is running
    - `$ sudo ps -e | grep falcon-sensor`
      `108019 ? 00:00:58 falcon-sensor`
    - `$ sudo systemctl is-active falcon-sensor`
      `active`
    - `$ sudo service falcon-sensor status`

```
Redirecting to /bin/systemctl status falcon-sensor.service
? falcon-sensor.service - CrowdStrike Falcon Sensor
Loaded: loaded (/usr/lib/systemd/system/falcon-sensor.service; enabled; vendor preset:
disabled)
Active: active (running) since Thu 2019-10-31 11:00:47 EDT; 11min ago
Process: 108012 ExecStart=/opt/CrowdStrike/falcond (code=exited, status=0/SUCCESS)
Process: 108010 ExecStartPre=/opt/CrowdStrike/falconctl -g --cid (code=exited,
status=0/SUCCESS)
Main PID: 108016 (falcond)
CGroup: /system.slice/falcon-sensor.service
??108016 /opt/CrowdStrike/falcond
??108019 falcon-sensor
```

Can it be uninstalled?

In order to uninstall current versions of CrowdStrike, you will need to obtain a maintenance token, which is unique to each system. To obtain this token, email security@mit.edu from your MIT account stating that you need a maintenance token to uninstall CrowdStrike. You will also need to provide your unique agent ID as described below. The Security Team may be able to find your host by a combination of hostname, IP address and/or MAC address.

You can retrieve the host's device ID or AID (agent ID) locally by running the following commands at a Command Prompt/Terminal.

- Windows:
  `reg query HKLM\System\CurrentControlSet\services\CSAgent\Sim\ /f AG`

- Mac sensor version 6.x:
  `sudo /Applications/Falcon.app/Contents/Resources/falconctl stats | grep agentID`

Once the Security Team provides this maintenance token, you may proceed with the below instructions.

- 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 6.x at this point. Note for those unfamiliar with sudo that you will be prompted for a password, which is the password for the account you are logged in as, to allow the command to run with elevated privilege. *The Falcon Agent will also require Full Disk access for the uninstall*. *On macOS 13 and above, Terminal will need to be added to App Management.*
  - `Sensor version 6.x and above, navigate to the Terminal command line and type:`

    - `sudo /Applications/Falcon.app/Contents/Resources/falconctl uninstall --maintenance-token`
    - Enter *token-from-security-team* when prompted
    - You can also unload/load the sensor if you think you are having problems:
      `sudo /Applications/Falcon.app/Contents/Resources/falconctl load`
      `sudo /Applications/Falcon.app/Contents/Resources/falconctl unload --maintenance-token`
    - Enter *token-from-security-team* when prompted
- Linux
    - `sudo service falcon-sensor stop`
    - Remove the package using the appropriate rpm or deb package command. The package name will be like `falcon-sensor-4.18.0-6403.el7.x86_64`

More information

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