Falcon Sensor for Mac Deployment Guide

CROWDSTRIKE CONFIDENTIAL

Last updated: Aug 04, 2020

Contents:

System Requirements

Installing the Falcon sensor for Mac requires elevated privileges.

Operating Systems

Supported OSes	Nearing End of Support	Unsupported OSes
• macOS Catalina 10.15* and later *(sensor 5.19.9906 and later)* • macOS Mojave 10.14† and later *(sensor 4.13.7501 and later)*	• macOS High Sierra 10.13‡ and later *(last supported on version 5.34.11501)*	All previous versions of OS X, including: • macOS Sierra 10.12 and later • OS X El Capitan 10.11 *(last supported on version 4.12.7401)* • OS X Yosemite 10.10 *(last supported on version 3.5.5603)*

We do not support hosts running in containers, such as Docker.

***macOS 10.15 Catalina and later:** Apple requires Full Disk Access (FDA) to be granted to falcond in order to work properly. This is a Catalina requirement by Apple for files and folders containing personal data. This requirement is applicable to all 3rd-party software which need to access files across all users of the machine (e.g. backup software).

> **Failure to complete this prerequisite step will result in the Falcon sensor for Mac not having full visibility to all files from all users.**

†**macOS 10.14 Mojave:** Beginning with sensor 5.20.10105, we recommend you grant Full Disk Access (FDA) to falcond. Without this access, upcoming Mac sensor releases will not have full visibility into some userspace file paths. The sensor will still record access to these files without FDA, which is what our detects are based on; however, FDA provides additional telemetry and more robust detections.

‡**macOS 10.13 High Sierra and later:** Apple requires kernel extensions to be approved before being loaded. We recommend that you use Apple's MDM to approve the com.crowdstrike.sensor kernel extension before installing. If your organization is unable to use MDM, then follow the OS prompts to manually approve the kernel extension after licensing. Manual approval must happen on the host, as Apple prevents admins from remotely approving kernel extensions.

> Note: See our End of OS Support Tech Alert for macOS High Sierra 10.13

Networking Requirements

Proxy Support

The Falcon sensor for Mac supports these types of proxy connections:

- Auto Proxy Discovery
- Automatic Proxy Configuration (PAC)
- Web Proxy (HTTP)

CrowdStrike does not support Proxy Authentication.

Avoid Interference with Certificate Pinning

The Falcon sensor uses certificate pinning to defend against man-in-the-middle attacks. Some network configurations, such as deep packet inspection, interfere with certificate validation.

To prevent interference with certificate validation, disable deep packet inspection (also called "HTTPS interception," "TLS interception," or "SSL inspection") or similar network configurations. Other common sources of interference with certificate pinning include antivirus systems, firewalls, or proxies.

Allow TLS traffic

Depending on your network environment, you may need to allow ("whitelist") TLS traffic between your network and our cloud's network addresses:

US-1 (most customers):

- ts01-b.cloudsink.net
- lfodown01-b.cloudsink.net

US-GOV-1:

- ts01-laggar-gcw.cloudsink.net
- lfodown01-laggar-gcw.cloudsink.net

EU-1:

- ts01-lanner-lion.cloudsink.net
- lfodown01-lanner-lion.cloudsink.net

US-2:

- ts01-gyr-maverick.cloudsink.net
- lfodown01-gyr-maverick.cloudsink.net

If your network requires allowing by IP address instead of FQDN, see Cloud IP Addresses for a list of IP addresses we use.

> We use AWS for some communications between hosts and the CrowdStrike cloud.

Standard Installation

Installing the Falcon Sensor for Mac

1. Download the sensor installer from Hosts > Sensor Downloads. Use the Chrome browser.
2. Copy your customer ID checksum (CCID) from Hosts > Sensor Downloads.
3. Run the sensor installer on your device using one of these two methods:
   - Double-click the `.pkg` file.
   - Run this command at a terminal, replacing `<installer_filename>` with the path and file name of your installer package:

     ```
     sudo installer -verboseR -package <installer_filename> -target /
     ```
4. When prompted, enter administrative credentials for the installer.
5. Run `falconctl`, installed with the Falcon sensor, to provide your customer ID checksum (CCID).

   ```
   sudo /Library/CS/falconctl license 0123456789ABCDEFGHIJKLMNOPQRSTUV-WX
   ```
   - This command is slightly different if you're installing with uninstall protection.
   - In this example, replace `0123456789ABCDEFGHIJKLMNOPQRSTUV-WX` with your CID.
6. Approve the Kernel Extension:
   1. MDM Sensor Installation with KEXT Approval
   2. Manual KEXT Approval
      1. Also use these steps if your MDM (Mobile Device Management) doesn’t support kext allowlisting or you use DevOps/scripts to deploy the product
7. Grant Full Disk Access (Catalina/Mojave Only):
   1. MDM Full Disk Access
   2. Manual Full Disk Access

Approving Kernel Extensions

What happens if CrowdStrike kernel extensions aren’t approved?

When CrowdStrike kernel extensions are not approved:

- Those systems do not appear in Falcon console
- You will not see any events from such macOS systems
- If you try to add your CID, you might get this error:

  ```
  Error: System policy prevents loading of CrowdStrike kernel extension ID com.crowdstrike.sensor
  ```
- If you run the “falconctl license” terminal command again, you might get this error:

  ```
  Error: This machine is already licensed
  ```

MDM SENSOR INSTALLATION WITH KEXT APPROVAL

When you manage macOS systems by MDM such as JAMF, you can approve the kernel extension in advance. To do so, refer to this article from Apple. As mentioned in the Apple article, in the MDM create a Kernel Extension Policy to allow loading of kernel extensions associated with the CrowdStrike. To do so, we recommend the following:

1. If your macOS systems don't have kernel extension policy, use your MDM tool to create one (Apple's instructions) with **CrowdStrike's team Identifier X9E956P446**, and apply it to the macOS systems before installing CrowdStrike Falcon.

2. If your macOS already has MDM kernel extension policy then add CrowdStrike's team ID **X9E956P446** under AllowedTeamIdentifiers.

3. If your Macs have an MDM policy that is shown as pending, reboot the Mac.

At any time, you can check kernel extension is approved and loaded by running the following terminal command in macOS:

```
kextstat | grep crowd
```

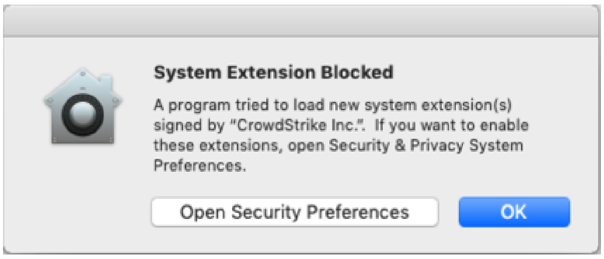
If `com.crowdstrike.sensor` is displayed, it indicates that kernel extensions are approved and loaded successfully.

MANUAL KEXT APPROVAL

This scenario is also applicable if your MDM (Mobile Device Management) doesn't support kext allowlisting or you use DevOps/scripts to deploy the product.

1. Follow installation steps mentioned above.

2. After entering the credential for installation, you're prompted to approve kernel extension from **Security & Privacy** pane as shown below.



System Extension Blocked

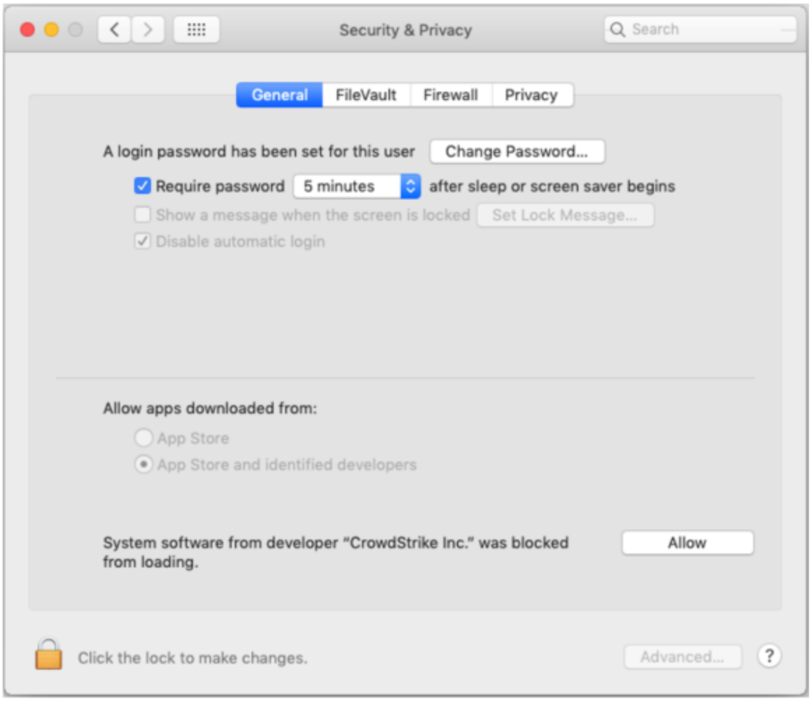
A program tried to load new system extension(s) signed by "CrowdStrike Inc.". If you want to enable these extensions, open Security & Privacy System Preferences.

When this screen is displayed the end-user must approve the kernel extension from CrowdStrike. If you don't see the prompt, approve the kernel extension from System Preferences:

1. On the Mac where you're installing the sensor, click the upper-left **Apple icon** > **System Preferences**

2. Click **Security & Privacy**

3. On the General tab, click **Allow** to approve CrowdStrike kernel extension



A login password has been set for this user

☑ Require password 5 minutes after sleep or screen saver begins

□ Show a message when the screen is locked

☑ Disable automatic login

Allow apps downloaded from:

○ App Store

● App Store and identified developers

System software from developer "CrowdStrike Inc." was blocked from loading.

Click the lock to make changes.

> **Note:** This approval prompt is only present in the Security & Privacy preferences pane for 30 minutes after the alert. Until the user approves the kernel extension, future load attempts will cause the approval prompt to reappear but will not trigger another user alert. If you don't see this approval option, restart the machine to get the approval prompt again.
>
> Kernel extension approval is required only once. If the Falcon sensor is subsequently reinstalled or updated, you will not see another approval prompt.

Grant Full Disk Access

Full Disk Access should be enabled for all macOS Catalina hosts, and is recommended for macOS Mojave hosts running sensor 5.20.10105 or later.

MACOS CATALINA

Beginning with macOS Catalina, Apple requires full disk access to be granted to falcond in order to work properly. This is a Catalina requirement by Apple for files and folders containing personal data. This requirement is applicable to all 3rd-party software which need to access files across all users of the machine (e.g. backup software).

Failure to complete this prerequisite step will result in the Falcon sensor for Mac not having full visibility to all files from all users.

- Providing Full Disk Access to falcond needs to be done exactly once on each host after upgrading to Catalina from earlier macOS releases.
- Subsequent updates of Falcon do not require this step to be repeated.
- *New manual installations* of the Falcon Sensor for Mac from 5.20+ will only require Step B.

MACOS MOJAVE

Beginning with sensor 5.20.10105, we recommend you grant Full Disk Access (FDA) to falcond. Without this access, upcoming Mac sensor releases will not have full visibility into some userspace file paths. The sensor will still record access to these files without FDA, which is what our detects are based on; however, FDA provides additional telemetry and more robust detections.

- Compared to Catalina, fewer paths are protected on Mojave, so not granting Full Disk Access on Mojave is less impactful to available telemetry and detections compared to Catalina.
- Full Disk Access for falcond will allow upcoming Mac sensor releases to access file paths which are restricted by default:
  - on Mojave, these file paths include Mail, Messages, Safari, Home, and Time Machine backups.
  - on Catalina, these file paths include the above plus additional paths including access to Desktop, Documents, Downloads, iCloud Drive, Third-party cloud storage, Removable volumes, Network volumes
- Mojave installations only require FDA Step B.

MDM FULL DISK ACCESS

Refer to documentation provided by your MDM provider to grant full disk access to falcond.

> To grant full disk access in Jamf, see Jamf's article Preparing Your Organization for User Data Protections on macOS 10.14.

MANUAL FULL DISK ACCESS

You will need to provide full disk access via Security Preferences on each host. Administrator account permission is needed for these steps. Step A is valid for Mac sensor 5.19 on Catalina; after 5.20 is released only Step B will be needed.

Step A: Manually change the permissions of the /Library/CS folder to make that folder visible in Security Preferences (needed in Step B)

1. Navigate to **/Library** in Finder (use Cmd-Shift-G in dialog to type in path)
2. Ctrl-click **CS** directory and choose **Get Info**
3. Click the **lock** icon in the lower-left corner
4. Enter your device password
5. Under **Sharing & Permissions:** for "everyone" select **Read only**

Step B: Provide full disk access to falcond on the host

1. Open Apple **System Preferences**
2. Open **Security & Privacy**
3. Select the **Privacy** tab
4. If privacy settings are locked:
5. Click the **lock** icon in the lower-left corner
    1. Enter your device password
6. In the left pane, select **Full Disk Access**
7. In the right pane, click the + icon
8. Navigate to **/Library/CS/falcond** (use Cmd-Shift-G in dialog to type in path)
9. Click **Open**
10. Click **Quit Now**
11. Click the **lock** in the lower-left corner to re-lock privacy settings

Verifying Sensor Installation

To validate that the Falcon sensor for Mac is running on a host, run this command at a terminal:

Sensor 5.34 or earlier: `sysctl cs.`

Sensor 5.36 or later: `sudo /Library/CS/falconctl stats`

The output shows a list of details about the sensor, including its agent ID (AID), version, customer ID, and more. If your output is different, see Troubleshooting an Installation.

Uninstall Protection for the Falcon Sensor

Protect sensors from unauthorized uninstallation using sensor update policies. Enable **Uninstall and maintenance protection** in sensor update policies to protect hosts. For more info, read our Groups & Policies Guide.

Sensor upgrades with uninstall protection enabled and cloud updates disabled

Use this upgrade path if your organization is unable to use cloud-managed updates. Use bulk maintenance mode to upgrade using other tools, like JAMF.

1. Download the sensor installer from **Hosts > Sensor Downloads**. Use the Chrome browser.

2. In the sensor update policy you want to update, turn on **Bulk maintenance mode**. Make sure the **Sensor version updates off** build version is selected and **Uninstall and maintenance protection** is turned on.

3. Retrieve the bulk maintenance token to include in the deployment package. This token does not change, so you won't need to modify your deployment package each time you enter bulk maintenance mode.

4. Create a script named `falcon_maintenance_token.py`.

5. Add this to the Python script, replacing `<your bulk maintenance token here>` with your actual bulk maintenance token:

   ```
   #!/usr/bin/env python

   from __future__ import print_function

   mtoken = "<your bulk maintenance token here>"

   try:

      while True:

          print(mtoken)

   except IOError:

      pass
   ```

6. Run or configure your deployment tool to run the following commands, replacing `<installer_filename>`:

   -
     ```
     ./falcon_maintenance_token.py | sudo /Library/CS/falconctl unload --maintenance-token
     ```

   -
     ```
     sudo installer -verboseR -package <installer_filename> -target /
     ```

7. For increased security, turn off bulk maintenance mode after completing your upgrades. This restores the per-sensor maintenance token and disables the bulk maintenance token.

Advanced Installation Methods

Managing Sensor Tags

Sensor tags are optional user-defined identifiers you can use to group and filter hosts.

ASSIGNING SENSOR TAGS

Assign tags to a host using the `grouping-tags` command. This command is case sensitive.

Tags can include these characters:

- letters (`a-z`,`A-Z`)
- numbers (`0-9`)
- hyphens (`-`)
- underscores (`_`)
- forward slashes (`/`)

Tags can't include spaces ( ) or commas (,).

To assign multiple tags, separate each tag with commas. All tags for a host, including comma separators, cannot exceed 256 characters.

For example, to add the tags Washington/DC_USA and Production to a host, use this syntax:

```
sudo /Library/CS/falconctl grouping-tags set "Washington/DC_USA,Production"
```

To see the tags currently assigned to a host, use the `get` argument:

```
sudo /Library/CS/falconctl grouping-tags get
```

Tags take effect the next time the sensor is restarted. To restart the sensor run the following commands from a terminal:

```
sudo /Library/CS/falconctl unload
```

```
sudo /Library/CS/falconctl load
```

REMOVING SENSOR TAGS

To remove all tags from a host:

```
sudo /Library/CS/falconctl grouping-tags clear
```

Tags take effect the next time the sensor is restarted. To restart the sensor run the following commands from a terminal:

```
sudo /Library/CS/falconctl unload
```

```
sudo /Library/CS/falconctl load
```

Installing to a CID that requires installation tokens

Installation tokens prevent unauthorized hosts from being accidentally or maliciously added to your customer ID (CID). Installation tokens are an optional security measure for your CID. To use installation tokens, you create one or more tokens in the Falcon console or via the API, enable the token requirement, and then provide the tokens to sensors at installation time.

When you install a sensor after enabling **Require tokens**, the `falconctl` command must include an active token. These examples show two equally accepted ways to include a sample installation token, `ABCD1234`:

- As a single command, append the installation token with no argument: `sudo /Library/CS/falconctl license 0123456789ABCDEFGHIJKLMNOPQRSTUV-WX ABCD1234`
- As two separate commands:

```
sudo /Library/CS/falconctl provisioning-token ABCD1234
sudo /Library/CS/falconctl license 0123456789ABCDEFGHIJKLMNOPQRSTUV-WX
```

Installing the Sensor on A Virtual Machine Template

Follow these steps to set up a virtual machine template with a Falcon sensor.

> These steps are required so that each VM created from the template has a unique agent ID (AID). Otherwise, the Falcon console will display activity from all these hosts as if the activity came from a single host.

1. Install the sensor normally.
2. Open a terminal.
3. Run this command to unload (stop) the sensor:
   - With **Uninstall and maintenance protection** enabled: `sudo /Library/CS/falconctl unload --maintenance-token`
   - With **Uninstall and maintenance protection** disabled: `sudo  /Library/CS/falconctl unload`
   - When prompted, enter your maintenance token to continue.
4. Run both of these commands to remove files used to associate the host's AID:

   ```
   sudo rm /Library/CS/registry.base
   ```

   ```
   sudo rm /Library/CS/registry.tdb
   ```
5. Shut down the virtual machine.
6. Use your virtualization software to convert the VM to a template image.

When each VM created from this template first connects to the CrowdStrike cloud, we automatically assign the VM a unique AID.

MODIFYING YOUR VM TEMPLATE

If you modify your template later, ensure your template doesn't connect to the CrowdStrike cloud while the sensor is installed. Follow these steps so that your template is not assigned an AID.

1. Uninstall the sensor before you enable networking on the template.
2. Modify your template as needed.
3. Disable networking in your template again.
4. Install the Falcon sensor on your template.
5. Snapshot your VM template and clone it as needed.

Uninstalling the Falcon Sensor for Mac

Move the host to a sensor update policy with **Uninstall and maintenance protection** turned off, then uninstall the sensor. For more info, read our Groups and Policies Guide.

Run this command at a command line:

- With **Uninstall and maintenance protection** disabled: `sudo  /Library/CS/falconctl uninstall`
- With **Uninstall and maintenance protection** enabled: `sudo /Library/CS/falconctl uninstall --maintenance-token`
    - If the sensor is offline and **Uninstall and maintenance protection** is enabled, use the **Reveal Maintenance Token** button on the Host Management page to get the single-use token required to uninstall the sensor. Enter this token when prompted by `falconctl`.
    - If the sensor is offline and **Bulk Maintenance Mode** is enabled, reveal the bulk maintenance token within the policy. Enter this token when prompted by falconctl.

Troubleshooting an Installation

CROWDSTRIKE CONFIDENTIAL

Verify that the Sensor Appears in the Falcon Console

Once the sensor is installed, the host connects to the Falcon console. You can confirm a sensor installation by reviewing your hosts.

To view a complete list of newly installed sensors, use the Sensor Report in the Falcon console.

Verify that the Sensor is Running

To validate that the Falcon sensor for Mac is running on a host, run this command at a terminal:

Sensor 5.34 or earlier: `sysctl cs.`

Sensor 5.36 or later: `sudo /Library/CS/falconctl stats`

The output shows a list of details about the sensor, including its agent ID (AID), version, customer ID, and more.

Verify that Sensor Components Were Installed

To see a list of the kernel extensions installed with the CrowdStrike sensor, run this command at a terminal:

```
kextstat | grep crowd
```

The output shows the `com.crowdstrike.sensor` kernel extension:

```
190    0 0xffffff7f8351e000 0xef000    0xef000    com.crowdstrike.sensor (53.03) F356DB5C-4044-3DD9-810E-0620678E4A20 <189 43 7 5
4 3 2 1>
```

If the kernel extensions were not installed, verify that the kernel extensions are approved.

Troubleshooting General Sensor Issues

CROWDSTRIKE CONFIDENTIAL

Verify that the Sensor is Connected to the Cloud

1. Run this terminal command to determine if the host can connect to the cloud:

```
sudo /Library/CS/falconctl stats
```

2. In the output, look for the Cloud Info section. A value of `State: connected` indicates the host is connected to the CrowdStrike cloud. Any other result indicates that the host can't connect to the CrowdStrike cloud. Review our Networking Requirements and check your network configuration.

```
Cloud Info

     IP: ts01-b.cloudsink.net

     Port: 443

     State: connected Cloud Activity

     Attempts: 1

     Connects: 1
```

3. In the output, look for the Events Sent section and the SensorHeartbeatMacV4 event. Ensure that sensor heartbeats are being sent every two minutes. The verifies the connection is established and negotiated with the cloud.

```
Events Sent                                              1m        5m        1h        4h        8h        12h       1d

SensorHeartbeatMacV4                                     1         3         30        121       167       167       167
```

4. In the output, look for the Event Sums and Acknowledgement Sums sections. The ignored, resent and resend limit counts should all be low. If they are high it may indicate issues in the connection to the cloud.

```
        Event Sums                                          1m        5m        1h        4h        8h        12h       1d
        Sent                                           51        141       1855      7872      21333     21333     21333
        Received                                       9         10        76        266       705       705       705
        Ignored                                        0         0         0         0         0         0         0
        Resent                                         16        22        22        22        22        22        22
        Resend Limit                                   0         0         0         0         0         0         0
        Overflow                                       0         0         0         0         0         0         0

    Acknowledgement Sums                               1m        5m        1h        4h        8h        12h       1d
        Sent                                           7         8         74        264       703       703       703
        Received                                       51        141       1855      7872      21333     21333     21333
        Ignored                                        0         0         0         0         0         0         0
        Resent                                         0         0         0         0         0         0         0
        Resend Limit                                   0         0         0         0         0         0         0
        Overflow                                       0         0         0         0         0         0         0
```

ENDPOINT FIREWALLS