Falcon Sensor for Mac Deployment Guide (version 6.11 and later)

CROWDSTRIKE CONFIDENTIAL

Last updated: February 2, 2021

Contents:

Overview

CROWDSTRIKE CONFIDENTIAL

This deployment information applies to Falcon sensor for Mac version 6.11 and later. For deployment information that applies to earlier Falcon sensor versions, see Falcon sensor for Mac deployment guide (version 5.x and earlier).

Understanding important recent sensor updates

SENSOR VERSION 6.11 AND LATER

Falcon sensor for Mac version 6.11 and later supports system extensions. For macOS Big Sur 11.0 and later, kernel extensions are no longer needed. For hosts on macOS Mojave 10.14 through macOS Catalina 10.15, Falcon sensor continues to use kernel extensions.

The new system extension version of the sensor is identical in functionality to any previous sensor versions. The events, detections, and configurability remain the same.

> **Note:** The CrowdStrike kernel extension is needed to support the BIOS visibility prevention policy settings regardless of OS version. See Host authorizations.

For Falcon sensor for Mac version 6.11 and later, the installation and data file locations have changed.

Additionally, there is an important recommendation to use an MDM solution to sync profiles prior to deployment. This streamlines the deployment and avoids manual authorization steps on hosts.

FILE LOCATIONS

Falcon sensor for Mac version 6.11 and later is installed as an application bundle. This version includes these file location changes:

- Falcon sensor application bundle: `/Applications/Falcon.app`
- Data files needed by the sensor: `/Library/Application Support/CrowdStrike/Falcon`
- The `falconctl` binary: `/Applications/Falcon.app/Contents/Resources/falconctl`

> **Note**: `falconctl` retains the same functionality as previous versions

> **Note:** In upgrades from sensor versions earlier than 6.11, the former `/Library/CS` folder is automatically removed after its contents are migrated to the new locations.

RUNNING PROCESSES

Falcon sensor for Mac version 6.11 and later uses system extensions. As a result, there's a change to what processes the sensor uses to run. When running on macOS Big Sur 11.0 and later, the only running process for the sensor is `com.crowdstrike.falcon.Agent`. This is the system extension.

To find the state of the system extension, run the command `systemextensionsctl list`

Custom health check scripts or VPN compliance checks may need to be updated using these new processes.

To check for sensor health, run `/Applications/Falcon.app/Contents/Resources/falconctl stats`

UNDERSTANDING FUTURE MACOS UPGRADES

Falcon sensor for Mac version 6.11 and later includes awareness of an upgrade on the host to a macOS version that allows for system extensions. For example, when upgrading macOS Mojave 10.14 or Catalina 10.15 to Big Sur 11.0 and later, the sensor reconfigures itself to remove the use of a kernel extension and Falcon's daemon and to install the system extension instead. This allows OS upgrades to happen without the need to reinstall the sensor.

Prerequisite: using MDM to sync profiles before installing or upgrading

We provide a profile with all necessary authorizations to properly run the sensor on all supported versions of macOS. This profile is attached to the Tech Alert Preparing for macOS Falcon Sensor 6.11. We strongly recommend you use an MDM solution to distribute the profile to your endpoints prior to the deployment process. You can upload this profile to an MDM server and push it out to all endpoints. This profile is also backwards compatible with sensor versions earlier than 6.11 so you can deploy it any time prior to installing or upgrading to sensor version 6.1x.

This profile includes:

- Authorization for the Falcon system extension, which is required for hosts running macOS Big Sur 11.0 and later. Apple requires system extensions to be approved before they can be loaded.
- Configuration for the Falcon network filter extension, which is required for hosts running macOS Big Sur 11.0 and later.
- Full Disk Access (FDA) to Falcon. This is a recommendation for macOS Mojave 10.14 and a requirement for macOS Catalina 10.15 and later.
- Authorization for the CrowdStrike kernel extension. This is required for hosts running macOS Mojave 10.14 through macOS Catalina 10.15, and to support the BIOS visibility prevention policy settings regardless of OS version. Similar to system extensions, Apple requires kernel extensions to be approved before they can be loaded.

For improved security and privacy, Apple doesn't allow profiles to be deployed outside of an MDM solution. **If you don't use an MDM solution to distribute the necessary profile to endpoints prior to installation or upgrade to sensor version 6.11 and later, multiple authentication confirmations from the OS occur on the host and must manually be approved.** See Alternate installation method: Installing without using an MDM to sync profiles.

These authorizations are only required once. Subsequent upgrades using the built-in upgrade functionality of the sensor will not require additional confirmation approvals on the host.

System Requirements

Installing the Falcon sensor for Mac requires elevated privileges.

Supported Operating Systems

Falcon Sensor is currently supported on these macOS versions:

- macOS Big Sur 11.0 and later (sensor 6.11.12404 and later) for hosts with Intel processors. Big Sur support for hosts with M1 ARM processors will be added in a future sensor version.
  - Falcon sensor for Mac version 6.11 does not have visibility into network events on Big Sur. This limitation is due to an issue in Apple's Network Extensions framework. This issue is resolved in sensor version 6.12.
  - macOS Big Sur 11.1 and later: if installing Falcon sensor for the first time on the host, use Falcon sensor for Mac version 6.14 or later.
- macOS Catalina 10.15 and later (sensor 5.19.9906 and later)
- macOS Mojave 10.14 and later (sensor 4.13.7501 and later)

Falcon does not support hosts running in containers, such as Docker.

Host authorizations

The Falcon sensor for Mac requires these additional authorizations on each host:

- Authorization for the Falcon system extension, which is required for hosts running macOS Big Sur 11.0 and later. Apple requires system extensions to be approved before they can be loaded.
- Authorization for the Falcon network filter extension, which is required for hosts running macOS Big Sur 11.0 and later.
- Full Disk Access (FDA) to Falcon. This is a recommendation for macOS Mojave 10.14 and a requirement for macOS Catalina 10.15 and later.
- Authorization for the CrowdStrike kernel extension, which is required for hosts running macOS Mojave 10.14 through macOS Catalina 10.15, and to support the BIOS visibility prevention policy settings regardless of OS version. Similar to system extensions, Apple requires kernel extensions to be approved before they can be loaded.

The profile we provide includes these authorizations. See Prerequisite: using MDM to sync profiles before installing or upgrading.

If you don't use an MDM solution to load the provided profile previous to deployment, you must perform manual authorizations on each host during installation. See Alternate installation method: Installing without using an MDM to sync profiles.

Networking Requirements

Proxy Support

The Falcon sensor for Mac uses proxies as configured in System Preferences.

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 on port 443 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.

Installing the Falcon Sensor for Mac

There are two methods to successfully install the sensor:

- Recommended installation method: Use an MDM solution to distribute the profile we provide to your endpoints prior to the deployment process. This streamlines the deployment and avoids manual authorization steps on hosts.
- Alternate installation method: If you don't use an MDM to distribute the profile we provide, multiple authentication confirmations from the OS occur on the host and must manually be approved.

Recommended installation method: Using an MDM to sync profiles

1. Download the MDM profile from the Tech Alert Preparing for macOS Falcon Sensor 6.11 and deploy it to the hosts. This step can be performed any time prior to sensor deployment.

   Caution: If you do not use an MDM to sync profiles, you must perform manual steps during the installation. See Alternate installation method: Installing without using an MDM to sync profiles.

2. Download the sensor installer from Hosts > Sensor Downloads. Use the Chrome browser.
3. Copy your customer ID checksum (CCID) from Hosts > Sensor Downloads.
4. 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 /
     ```

5. When prompted, enter administrative credentials for the installer.
6. Run `falconctl`, installed with the Falcon sensor, to provide your customer ID checksum (CCID). This command is slightly different if you're installing with uninstall protection. In this example, replace `0123456789ABCDEFGHIJKLMNOPQRSTUV-WX` with your CID.

   ```
   sudo /Applications/Falcon.app/Contents/Resources/falconctl license 0123456789ABCDEFGHIJKLMNOPQRSTUV-WX
   ```

Alternative installation method: Installing without using an MDM to sync profiles

Note: We strongly recommend you use an MDM solution to distribute the profile we provide to your endpoints prior to the deployment process. See Recommended installation method: using an MDM to sync profiles

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:
   1. Double-click the `.pkg` file.
   2. 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. For macOS Mojave 10.14 through macOS Catalina 10.15, after entering the credential for installation, you're asked to approve the kernel extension on each host. The Apple message on the host identifies the CrowdStrike kernel extension as a blocked system extension signed by CrowdStrike Inc.:

    1. In the message, click **Open Security Preferences**. If the message no longer appears on the host, click the Apple icon and open System Preferences, then click **Security & Privacy**.
    2. On the **General** tab, click **Allow** to allow the CrowdStrike kernel extension.

       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.
    3. Kernel extension approval is required only once. If the Falcon sensor is subsequently reinstalled or updated, you will not see another approval prompt.

6. Run `falconctl`, installed with the Falcon sensor, to provide your customer ID checksum (CCID). This command is slightly different if you're installing with uninstall protection. In this example, replace `0123456789ABCDEFGHIJKLMNOPQRSTUV-WX` with your CID:

   ```
   sudo /Applications/Falcon.app/Contents/Resources/falconctl license 0123456789ABCDEFGHIJKLMNOPQRSTUV-WX
   ```

7. For macOS Big Sur 11.0 and later, after providing your CID with the license command, you're asked to approve the system extension on each host:

    1. In the message, when asked to filter network content, click **Allow**.
    2. When the System Extension Blocked message appears, click **Open Security Preferences**.
    3. On the **General** tab, click **Allow** to allow the Falcon system extension. You may need to click the lock icon to enable you to make security changes.If you do not approve the Falcon system extension when prompted on the host, run the `falconctl` load command to load Falcon again and show the prompts on the host for approval:

       ```
       sudo /Applications/Falcon.app/Contents/Resources/falconctl load
       ```

8. Full Disk Access is recommended for Mojave and required for Catalina and later. You must grant Full Disk Access on each host. Administrator account permission is required:

    1. Click the Apple icon and open System Preferences, then click **Security & Privacy.**
    2. On the **Privacy** tab, if privacy settings are locked, click the lock icon and specify the password.
    3. In the left pane, select **Full Disk Access.**
    4. For macOS Big Sur 11.0 and later, in the right pane, select the **Agent** check box.
    5. For all macOS versions, in the right pane, click the plus icon.
    6. In finder, find **Falcon** in the list of applications.
    7. Click **Open** and then click **Quit Now**

8. Click the lock icon to re-lock privacy settings.

Post-installation steps

Verifying Sensor Installation

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

```
sudo /Applications/Falcon.app/Contents/Resources/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 /Applications/Falcon.app/Contents/Resources/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.

Managing Sensor Grouping Tags

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

> Note: For information on Falcon grouping tags, which are managed through the Falcon console or CrowdStrike API, see Using grouping tags. Falcon grouping tags can't be specified at the sensor CLI and can't be used with sensor images or templates.

ASSIGNING SENSOR GROUPING 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 /Applications/Falcon.app/Contents/Resources//falconctl grouping-tags set "Washington/DC_USA,Production"
```

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

```
sudo /Applications/Falcon.app/Contents/Resources/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 /Applications/Falcon.app/Contents/Resources/falconctl unload
```

```
sudo /Applications/Falcon.app/Contents/Resources/falconctl load
```

REMOVING SENSOR GROUPINGTAGS

To remove all tags from a host:

```
sudo /Applications/Falcon.app/Contents/Resources/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 /Applications/Falcon.app/Contents/Resources/falconctl unload
```

```
sudo /Applications/Falcon.app/Contents/Resources/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 /Applications/Falcon.app/Contents/Resources/falconctl license 0123456789ABCDEFGHIJKLMNOPQRSTUV-WX ABCD1234
```

- As two separate commands:

```
sudo /Applications/Falcon.app/Contents/Resources/falconctl provisioning-token ABCD1234
sudo /Applications/Falcon.app/Contents/Resources/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 /Applications/Falcon.app/Contents/Resources/falconctl unload --maintenance-token
     ```

   - With **Uninstall and maintenance protection** disabled:

     ```
     sudo /Applications/Falcon.app/Contents/Resources/falconctl unload --maintenance-token
     ```

   - 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/Application Support/CrowdStrike/Falcon/registry.base
   ```

   ```
   sudo rm /Library/Application Support/CrowdStrike/Falcon/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.