


# Sensor Deployment and Maintenance

06/08/2026

Copyright © CrowdStrike

# 1. Falcon Sensor for Mac Deployment

## 1.1. Overview

## 1.2. System requirements

### 1.2.1. Supported operating systems

### 1.2.2. Host authorizations

#### 1.2.2.1. Using MDM profiles provided by CrowdStrike

#### 1.2.2.2. Creating an MDM profile with necessary properties

##### 1.2.2.2.1. Approving Full Disk Access using MDM

### 1.2.3. Networking requirements

#### 1.2.3.1. Internet access

#### 1.2.3.2. Allow TLS traffic

#### 1.2.3.3. Avoid interference with certificate pinning

#### 1.2.3.4. Proxy support

### 1.2.4. Supported sensor languages

## 1.3. Best practices for sensor deployment

## 1.4. Installing the Falcon sensor for Mac

### 1.4.1. Recommended installation method: Using an MDM to sync profiles

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

## 1.5. Post-installation steps

### 1.5.1. Verifying sensor installation

#### 1.5.1.1. Falcon console

#### 1.5.1.2. Host

### 1.5.2. Enabling uninstall protection for the Falcon sensor

### 1.5.3. Managing sensor grouping tags

#### 1.5.3.1. Assigning sensor grouping tags

#### 1.5.3.2. Viewing a host's sensor grouping tags

##### 1.5.3.2.1. Falcon console

##### 1.5.3.2.2. Host

#### 1.5.3.3. Removing sensor grouping tags

## 1.6. Advanced installation options

### 1.6.1. Installing to a CID that requires installation tokens

### 1.6.2. Installing the sensor on a virtual machine template

#### 1.6.2.1. Modifying your VM template

## 1.7. Uninstall the Falcon sensor for Mac

## 1.8. Troubleshooting

### 1.8.1. Verifying the Falcon system extension was installed

### 1.8.2. Verifying that the sensor is running

### 1.8.3. Verifying the sensor is connected to the CrowdStrike cloud

#### 1.8.3.1. Endpoint firewalls

### 1.8.4. Providing troubleshooting info to Support

## 1.9. Logs

### 1.9.1. Normal log contents

## 1.10. Reduced functionality mode: Mac hosts

### 1.10.1. Checking if a sensor is in RFM

### 1.10.2. Resolving RFM for Mac hosts

## 1.11. Sensor safe mode: Mac hosts

### 1.11.1. Checking if a sensor is in safe mode

### 1.11.2. Resolving safe mode for Mac hosts

# Falcon Sensor for Mac Deployment

Install, uninstall, and troubleshoot issues with the Falcon sensor for Mac.

## Overview

Falcon sensor for Mac stops breaches by unifying true next-generation antivirus (NGAV) endpoint detection and response (EDR), managed threat hunting, and threat intelligence automation, using a single lightweight sensor.

## System requirements

Installing the Falcon sensor for Mac requires administrator privileges, also known as elevated privileges.

### Supported operating systems

The Falcon sensor for Mac is supported on these macOS versions:

| macOS version | Minimum sensor version | Falcon end-of-support date |
|---|---|---|
| macOS Tahoe 26 | 7.29<br>Intel CPUs and Apple silicon native support included | December 31, 2028 |
| macOS Sequoia 15 | All supported sensor versions<br>Intel CPUs and Apple silicon native support included | December 31, 2027 |
| macOS Sonoma 14 | All supported sensor versions<br>Intel CPUs and Apple silicon native support included | December 31, 2026 |

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

### Host authorizations

Apple requires system extensions to be approved before they can be loaded. The Falcon sensor for Mac requires these additional authorizations on each host:

- Full Disk Access (FDA) to Falcon
  Important: If Full Disk Access is not enabled, the sensor enters reduced functionality mode (RFM). See Reduced functionality mode: Mac hosts.
- Falcon system extension
  - Falcon non-removable system extension (macOS Sequoia 15 and later)
- Falcon network filter extension

If you use profiles provided by CrowdStrike, these authorizations are already configured for you. Apple doesn't allow profiles to be deployed outside of an MDM solution. We strongly recommend you use an MDM solution to distribute the profile to your endpoints prior to the deployment process. 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.

We recommend using one of these MDM profile options:

- Using MDM profiles provided by CrowdStrike: We provide profiles with all necessary authorizations.
- Creating an MDM profile with necessary properties: Refer to the necessary profile parameters to create your own profile.

Important: If you don't use an MDM solution to distribute the necessary profile to endpoints, multiple macOS authentication confirmations occur on the host that must be manually approved. See Alternative installation method: Installing without using an MDM to sync profiles.

Using MDM profiles provided by CrowdStrike

For endpoints on Intel or M1 processors, we provide profiles with all necessary authorizations to properly run the sensor on all supported versions of macOS. We strongly recommend you use an MDM solution to distribute profiles to your endpoints prior to the deployment process. You can upload profiles to an MDM server and distribute them to your endpoints.

Download one or more MDM profiles from the attachments in the CrowdStrike Customer Center article on using MDM with the Falcon sensor for Mac. For US-GOV-1 and US-GOV-2 customers, see CrowdStrike Government Customer Center article on using MDM with the Falcon sensor for Mac.
Important: There are different profiles for different versions of macOS. Ensure your MDM solution is configured to apply the correct profile to each host.

Creating an MDM profile with necessary properties

When creating your own profile, you must specify MDM properties to approve the needed macOS extensions and to approve full disk access.
Tip: When upgrading Mac hosts to macOS Sequoia 15, we recommend creating a second MDM profile for Sequoia hosts with the required system extension payload, rather than updating an existing profile. This will ensure the sensor remains running while the new settings are applied.

Payload: SystemExtensions

| Property | Value |
| --- | --- |
| AllowedSystemExtensions | Dict: {Key: X9E956P446Value: com.crowdstrike.falcon.Agent} |
| AllowUserOverrides<br><br>Important: If any SystemExtensions payload has a value of false for an AllowUserOverrides property, manual end user approval of non-specified system extensions will not be permitted. | true |

| Property | Value |
| --- | --- |
| NonRemovableFromUISystemExtensions<br>Note: This property is for Sequoia and later. | Dict: {Key: X9E956P446, Value: com.crowdstrike.falcon.Agent} |

Payload: com.apple.servicemanagement

Note: This payload is for Sonoma and later.

| Property | Value |
| --- | --- |
| Rules | Array [<br>{Key:RuleType,Value:BundleIdentifier, Key:RuleValue,Value:com.crowdstrike.falcon.UserAgent},<br>{Key:RuleType,Value:TeamIdentifier, Key:RuleValue,Value:X9E956P446}<br>] |

Payload: WebContentFilter

| Property | Value |
| --- | --- |
| FilterDataProviderBundleIdentifier | com.crowdstrike.falcon.Agent |
| FilterDataProviderDesignatedRequirement | identifier "com.crowdstrike.falcon.Agent" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] and certificate leaf[field.1.2.840.113635.100.6.1.13] and certificate leaf[subject.OU] = "X9E956P446" |
| FilterGrade | inspector |
| FilterPackets | false |
| FilterSockets | true |
| FilterType | Plugin |
| Organization | CrowdStrike Inc. |
| PluginBundleID | com.crowdstrike.falcon.App |

Approving Full Disk Access using MDM

Approving Full Disk Access for the Falcon sensor is a requirement, the Falcon sensor enters Reduced Functionality Mode (RFM) if this is not enabled. See Reduced functionality mode: Mac hosts.

To approve Full Disk Access, use the Privacy Preferences Policy Control payload with a SystemPolicyAllFiles property and specify this information in XML format:

```
<dict>
 <key>SystemPolicyAllFiles</key>
 <array>
  <dict>
   <key>Allowed</key>
   <true/>
   <key>CodeRequirement</key>
   <string>identifier "com.crowdstrike.falcon.Agent" and anchor apple generic and certificate
1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /*
exists */ and certificate leaf[subject.OU] = X9E956P446</string>
   <key>Comment</key>
   <string></string>
   <key>Identifier</key>
   <string>com.crowdstrike.falcon.Agent</string>
   <key>IdentifierType</key>
   <string>bundleID</string>
   <key>StaticCode</key>
   <false/>
  </dict>
  <dict>
   <key>Allowed</key>
   <true/>
   <key>CodeRequirement</key>
   <string>identifier "com.crowdstrike.falcon.App" and anchor apple generic and certificate
1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /*
exists */ and certificate leaf[subject.OU] = X9E956P446</string>
   <key>Comment</key>
   <string></string>
   <key>Identifier</key>
   <string>com.crowdstrike.falcon.App</string>
   <key>IdentifierType</key>
   <string>bundleID</string>
   <key>StaticCode</key>
   <false/>
  </dict>
 </array>
</dict>
```

## Networking requirements

### Internet access

Starting with Falcon sensor for Mac version 7.36, the sensor can discover a CID's cloud, or you can specify the cloud as shown in Recommended installation method: Using an MDM to sync profiles. For optimal discovery, allowlist all the IP addresses for the US-1, US-2, EU-1, US-GOV-1, and US-GOV-2 clouds.

Allow TLS traffic

After agent installation, an agent opens a permanent TLS connection over port 443. The connection is kept open until the endpoint is turned off or the network connection is terminated.

Depending on your network environment, you might need to allow TLS traffic on port 443 between your network and our cloud's network addresses.

If your network only allows traffic by destination IP address instead of FQDN, allow TLS traffic on port 443 over the static IP addresses. For more info, see Cloud IP Addresses and FQDNs.

Cloud domains for US-1

```
ts01-b.cloudsink.net
lfodown01-b.cloudsink.net
lfoup01-b.cloudsink.net
https://falcon.crowdstrike.com
https://assets.falcon.crowdstrike.com
https://assets-public.falcon.crowdstrike.com
https://api.crowdstrike.com
https://firehose.crowdstrike.com
```

CrowdStrike cloud US-2 domains

```
ts01-gyr-maverick.cloudsink.net
lfodown01-gyr-maverick.cloudsink.net
lfoup01-gyr-maverick.cloudsink.net
https://falcon.us-2.crowdstrike.com
https://assets.falcon.us-2.crowdstrike.com
https://assets-public.falcon.us-2.crowdstrike.com
https://api.us-2.crowdstrike.com
https://firehose.us-2.crowdstrike.com
```

CrowdStrike cloud EU-1 domains

```
ts01-lanner-lion.cloudsink.net
lfodown01-lanner-lion.cloudsink.net
lfoup01-lanner-lion.cloudsink.net
https://falcon.eu-1.crowdstrike.com
https://assets.falcon.eu-1.crowdstrike.com
https://assets-public.falcon.eu-1.crowdstrike.com
https://api.eu-1.crowdstrike.com
https://firehose.eu-1.crowdstrike.com
```

CrowdStrike cloud US-GOV-1 domains

```
ts01-laggar-gcw.cloudsink.net
sensorproxy-laggar-g-524628337.us-gov-west-1.elb.amazonaws.com
lfodown01-laggar-gcw.cloudsink.net
lfoup01-laggar-gcw.cloudsink.net
ELB-Laggar-P-LFO-DOWNLOAD-1265997121.us-gov-west-1.elb.amazonaws.com
https://falcon.laggar.gcw.crowdstrike.com
laggar-falconui01-g-245478519.us-gov-west-1.elb.amazonaws.com
https://api.laggar.gcw.crowdstrike.com
https://firehose.laggar.gcw.crowdstrike.com
falconhose-laggar01-g-720386815.us-gov-west-1.elb.amazonaws.com
```

CrowdStrike cloud US-GOV-2 domains

```
ts01-us-gov-2.cloudsink.crowdstrike.mil
lfodown01-us-gov-2.cloudsink.crowdstrike.mil
lfoup01-us-gov-2.cloudsink.crowdstrike.mil
https://falcon.us-gov-2.crowdstrike.mil
```

```
https://api.us-gov-2.crowdstrike.mil
https://firehose.us-gov-2.crowdstrike.mil
```

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.

Proxy support

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

### Supported sensor languages

For Falcon sensor text shown to users, such as sensor connection status, context menu, and notifications, the Falcon sensor provides localized text. To see localized text, set the language of the host's operating system to a supported language. For all other operating system languages, the Falcon sensor displays English text. Supported languages:

- English
- Chinese (Traditional)
- French
- German
- Italian
- Japanese
- Korean
- Portuguese
- Spanish

## Best practices for sensor deployment

The primary purpose of change control is to maintain stability in the production environment by thoroughly testing all changes in a pre-production (QA) setting.

To ensure successful testing, your pre-production test systems should accurately mirror their production counterparts.

Testing must verify application compatibility, performance, interoperability, and user permissions, among other factors.

In addition to typical user workstations, your test groups should include samples of your critical infrastructure, such as Domain Controllers, Exchange servers, critical database and application servers (including SQL and Web), encompassing both internal and customer-facing examples.

Most organizations already have a process for software distribution, which can be adapted as a working change control model. This model typically involves a time-phased, systematic deployment progression:

- Canary/QA Hosts: Initial deployment to a small group for early testing.
- Staging/Pre-Production Hosts: Deployment to a larger test group, which may be divided into sub-groups for staggered changes.
- Production Hosts: Final deployment to the live environment, which should also be broken into sub-groups for a phased rollout.

Whenever possible, deployment to production systems should occur during off-hours, strictly following the phased progression defined in your change control methodology.

## Installing the Falcon sensor for Mac

There are different 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 methods:
    - Use the standalone installer which streamlines your authorization and post-verification steps. See Falcon Sensor for Mac installer for more info.
    - For other supported Falcon sensor for Mac versions, see Alternative installation method: Installing without using an MDM to sync profiles for more info.

      Note: 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.

For information about other installation considerations, see Advanced installation options.

### Recommended installation method: Using an MDM to sync profiles

1. Use an MDM to deploy the correct profile to the hosts. This step can be performed any time prior to sensor deployment. For information on using our recommended profiles or creating your own, see Host authorizations.

   Note: Between deploying your MDM profile and installing the sensor, you may see a "not running" network filter. This is expected behavior and is resolved when you install the sensor.

2. Use the Google Chrome browser to download the sensor installer from Host setup and management > Deploy > Sensor downloads .

   You have these types of sensor installers to choose from:

   Important: The unified installer is available starting with Falcon sensor for Mac version 7.36 and is the only installer available. Any previously released, cloud-specific installers will remain available as long as the associated sensors are supported. We recommend using the unified installer whenever possible.

    - Unified installer. A single installer that works for these CrowdStrike clouds: US-1, US-2, EU-1, US-GOV-1, and US-GOV-2.
    - Cloud-specific installer. The installer works for only one of the CrowdStrike clouds: US-1, US-2, EU-1, US-GOV-1, or US-GOV-2.

3. Copy your customer ID checksum (CCID) from Host setup and management > Deploy > 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 installation tokens.
   - Optionally, set the cloud where the endpoint's CID resides.

     After installation, the sensor must connect to the CrowdStrike cloud where the endpoint's CID resides.

     With a cloud-specific installer, the sensor connects directly to the matching cloud.

     With the unified installer, you can let the sensor discover the CID's cloud automatically, or you can specify the cloud where the CID resides using the `license --cloud` option.

   Note: You must specify the CID immediately after the `license` subcommand.
   In this example, replace `0123456789ABCDEFGHIJKLMNOPQRSTUV` with your CID.

```
sudo /Applications/Falcon.app/Contents/Resources/falconctl license 0123456789ABCDEFGHIJKLMNOPQRSTUV \
[--cloud {us-1 | us-2 | eu-1 | us-gov-1 | us-gov-2}]
```

### 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. Use Google Chrome to download the sensor installer from Host setup and management > Deploy > Sensor downloads .

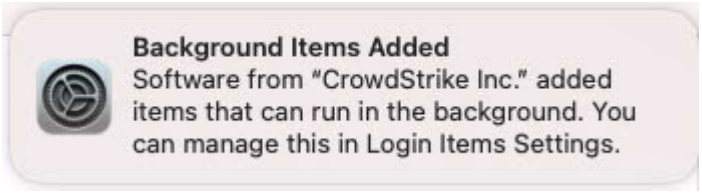
   You have these types of sensor installers to choose from:

   Important: The unified installer is available starting with Falcon sensor for Mac version 7.36 and is the only installer available. Any previously released, cloud-specific installers will remain available as long as the associated sensors are supported. We recommend using the unified installer whenever possible.

   - Unified installer. A single installer that works for these CrowdStrike clouds: US-1, US-2, EU-1, US-GOV-1, and US-GOV-2.
   - Cloud-specific installer. The installer works for only one of the CrowdStrike clouds: US-1, US-2, EU-1, US-GOV-1, or US-GOV-2.
2. Copy your customer ID checksum (CCID) from Host setup and management > Deploy > Sensor downloads .
3. Run the sensor installer on your device using one of these two methods:
   a. Double-click the `.pkg` file.
   b. 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 Sonoma 14 and later, the following dialog appears.




If you prevent this login item from running, the Falcon sensor still behaves normally. However, you don't get notifications about sensor activities.

Note: This dialog will also appear when you do updates.

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 installation tokens.
    - Optionally, set the cloud where the endpoint's CID resides.

      After installation, the sensor must connect to the CrowdStrike cloud where the endpoint's CID resides.

      With a cloud-specific installer, the sensor connects directly to the matching cloud.

      With the unified installer, you can let the sensor discover the CID's cloud automatically, or you can specify the cloud where the CID resides using the `license --cloud` option.

    Note: You must specify the CID immediately after the `license` subcommand.
    In this example, replace `0123456789ABCDEFGHIJKLMNOPQRSTUV` with your CID:

    ```
    sudo /Applications/Falcon.app/Contents/Resources/falconctl license 0123456789ABCDEFGHIJKLMNOPQRSTUV \
    [--cloud {us-1 | us-2 | eu-1 | us-gov-1 | us-gov-2}]
    ```

7. After providing your CID with the `license` command, you're asked to approve the system extension on each host:
    a. In the message, when asked to filter network content, click Allow.
    b. When the System Extension Blocked message appears, click Open Security Preferences.
    c. On the General tab, click Allow to allow the Falcon system extension. You might 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 required. You must grant Full Disk Access on each host for the sensor to work properly. Administrator account permission is required:

    Important: The Falcon sensor enters Reduced Functionality Mode (RFM) if this is not enabled. See Reduced functionality mode: Mac hosts.

    a. In System Preferences, click Security & Privacy.
    b. Go to the Privacy area or tab, depending on your macOS version.
    c. If privacy settings are locked, click the lock icon and specify the password.
    d. Select Full Disk Access.
    e. Enable FDA for these apps. If they are not in the list of apps, click the plus icon and find them in the list of applications:
        - Falcon
        - Falcon Sensor

f. Click the lock icon to re-lock privacy settings, if applicable.

g. For each host, either reload the sensor, reboot the host, or push an updated device control policy to the host.

   To reload the sensor, run these commands:

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

   For info about how to push an updated policy, see Assign a Device Control policy to host groups.

## Post-installation steps

### Verifying sensor installation

You can verify an installation by using the Falcon console or a terminal on the host.

Falcon console

After 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 Dashboards and reports > Reports > Sensor report .

Host

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.

### Enabling 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, see Managing sensor maintenance and uninstallation

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. Use Google Chrome to download the sensor installer from Host setup and management > Deploy > Sensor downloads .

   You have these types of sensor installers to choose from:

   Important: The unified installer is available starting with Falcon sensor for Mac version 7.36 and is the only installer available. Any previously released, cloud-specific installers will remain available as long as the associated sensors are supported. We recommend using the unified installer whenever possible.

- Unified installer. A single installer that works for these CrowdStrike clouds: US-1, US-2, EU-1, US-GOV-1, and US-GOV-2.
- Cloud-specific installer. The installer works for only one of the CrowdStrike clouds: US-1, US-2, EU-1, US-GOV-1, or US-GOV-2.

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 snippet 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: This section is about sensor grouping tags, which you can use with sensor images and templates. For more information about these tags and how they compare to Falcon grouping tags, see Group hosts using tags.

Assigning sensor grouping tags

Assign tags to a host using the `grouping-tags` command.

Tags are case-sensitive.

| Tags can include these characters | Tags can't include these characters |
|---|---|
| Letters (`a-z,A-Z`) | Spaces () |
| Numbers (`0-9`) | Commas (`,`) |

| Tags can include these characters | Tags can't include these characters |
|---|---|
| Hyphens (-) | |
| Underscores (_) | |
| Forward slashes (/) | |
| Period (.) | |
| At symbol (@) | |

To assign multiple tags, separate tags with commas. The combined length of 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:

- With Uninstall and maintenance protection enabled:

  ```
  sudo /Applications/Falcon.app/Contents/Resources/falconctl grouping-tags set
  Washington/DC_USA,Production --maintenance-token
  ```

  When prompted, enter your your maintenance token to continue.
- With Uninstall and maintenance protection disabled:

  ```
  sudo /Applications/Falcon.app/Contents/Resources/falconctl grouping-tags set
  Washington/DC_USA,Production
  ```

Tag changes take effect the next time the sensor restarts. To restart the sensor, run the following commands from a terminal:

- With Uninstall and maintenance protection enabled:

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

  When prompted, enter your your maintenance token to continue.
- With Uninstall and maintenance protection disabled:

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

Viewing a host's sensor grouping tags

Falcon console

Use Host Management to search for the host. The Grouping Tags information for the host includes Falcon grouping tags and sensor grouping tags.

Host

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

```
sudo /Applications/Falcon.app/Contents/Resources/falconctl grouping-tags get
```

Removing sensor grouping tags

To remove all tags from a host, run this command:

- With Uninstall and maintenance protection enabled:

  ```
  sudo /Applications/Falcon.app/Contents/Resources/falconctl grouping-tags clear --maintenance-token
  ```

  When prompted, enter your your maintenance token to continue.
- With Uninstall and maintenance protection disabled:

  ```
  sudo /Applications/Falcon.app/Contents/Resources/falconctl grouping-tags clear
  ```

Tag changes take effect the next time the sensor restarts. To restart the sensor, run the following commands from a terminal:

- With Uninstall and maintenance protection enabled:

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

  When prompted, enter your your maintenance token to continue.
- With Uninstall and maintenance protection disabled:

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

## Advanced installation options

### Installing to a CID that requires 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 through the API, enable the token requirement, and then provide the tokens to sensors at installation time. For more info, see Protecting your CID with installation tokens.

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.

Note: 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
      ```

      When prompted, enter your maintenance token to continue.
    - With Uninstall and maintenance protection disabled:

      ```
      sudo /Applications/Falcon.app/Contents/Resources/falconctl unload
      ```
4. Run this command to remove files used to associate the host's AID:

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

## Uninstall the Falcon sensor for Mac

Important: Uninstalling the sensor requires admin privileges.
The uninstallation process differs if certain sensor protection policies are enabled. For more info, see Managing sensor maintenance and uninstallation.

| Falcon configuration type | Uninstallation command |
|---|---|
| No additional options configured | On the host Mac, run this command from Terminal:<br>`sudo /Applications/Falcon.app/Contents/Resources/falconctl uninstall` |

| Falcon configuration type | Uninstallation command |
| --- | --- |
| Uninstall and maintenance protection is enabled | On the host Mac, run this command from Terminal:<br>`sudo /Applications/Falcon.app/Contents/Resources/falconctl uninstall --maintenance-token`<br>When prompted, enter the maintenance token. For more info, see Making changes to a single host. |
| Bulk maintenance mode is enabled for your hosts | On the host Mac, run this command from Terminal:<br>`sudo /Applications/Falcon.app/Contents/Resources/falconctl uninstall --maintenance-token`<br>When prompted, enter the maintenance token. For more info, see Making changes to multiple hosts. |

## Troubleshooting

### Verifying the Falcon system extension was installed

To verify the Falcon system extension is enabled and activated by the operating system, run this command at a terminal:

```
systemextensionsctl list
```

The output shows the com.crowdstrike.falcon.Agent system extension.

```
1 extension(s)
--- com.apple.system_extension.endpoint_security
enabled active teamID bundleID (version) name [state]
* * X9E956P446 com.crowdstrike.falcon.Agent (5.38/119.57) Agent [activated enabled]
```

If the system extension is not installed, use one of these methods to make sure the Falcon system extension is approved on each host:

- Download and use an MDM solution to deploy the profile we provide to each host, then reinstall the sensor. See Recommended installation method: Using an MDM to sync profiles.
- Reinstall the sensor using the steps to manually approve the Falcon system extension on each host. See Alternative installation method: Installing without using an MDM to sync profiles.

### Verifying that the sensor is running

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.

### Verifying the sensor is connected to the CrowdStrike cloud

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

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

If you're using an endpoint firewall on your host, it must be configured to allow access to the CrowdStrike domains. Customers have reported that these products require additional configuration when used with the Falcon sensor:

- Ad-Aware Pro Security
- Avast Internet Security
- AVG Internet Security
- Bullguard Internet Security
- Dr. Web Security Space
- MyInternetSecurity Preventon A/V + Firewall
- UnThreat Internet Security
- VIPRE Internet Security
- ZoneAlarm Internet Security Suite
- Chili internet Security
- ESET Node32 Smart Security
- BITDEFENDER Total Security
- Trustport Internet Security

### Providing troubleshooting info to Support

Providing `falconctl diagnose` output to our Support team can help troubleshoot sensor issues.

Run this command using `sudo` on the Mac host in a terminal:

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

While the diagnostic runs, a status bar appears in the terminal. The process can take 10 minutes.

When the diagnostic finishes, the terminal displays the path to the diagnostic file. Also, a Finder window appears and displays the `/private/tmp/` directory and the diagnostic file there. This file has a name similar to `falconctl_diagnose_4APo7TWJ.tgz`.

Attach this file to your Support case.

For additional troubleshooting information or to open a support case, visit the CrowdStrike Customer Center.

## Logs

Logs are stored using Apple's unified logging interface and are under their respective process IDs.

To view or stream the logs for the past twenty hours, run this command:

```
log show --predicate 'process == "com.crowdstrike.falcon.Agent"' --last 20h
```

For information about streaming, formatting, and searching the logs, see the `log` man page.

### Normal log contents

A normal startup log includes messages similar to these:

- The sensor is starting.
- The sensor is locating and initializing the config.
- The sensor is checking communications (whether to use proxy or not and on which host/port).
- The sensor is connecting and setting up SSL.
- The sensor connected and is sending its first message to CrowdStrike cloud.
- The sensor received a response from cloud. All startup tasks are complete.

## Reduced functionality mode: Mac hosts

Reduced functionality mode (RFM) is a mode for the Falcon sensor for Mac if Full Disk Access (FDA) is not enabled on the host.

A mac host's sensor that is in RFM still communicates with the cloud. However, when the host's file system is unavailable because FDA isn't enabled for the Falcon sensor, sensor functionality that interacts with the file system is reduced.

Note: Hosts on other platforms can also enter RFM, but RFM for the Falcon sensor behaves differently on each platform. See Reduced functionality mode: Linux hosts and Reduced functionality mode: Windows hosts.

### Checking if a sensor is in RFM

Use one of these methods to check if a Mac host's sensor is in RFM:

- In the Falcon console:
  - Executive summary dashboard: The dashboard at Dashboards and reports > Reports > Executive summary lists a count of sensors in RFM by operating system. You can click an RFM widget in the dashboard to open more details in Host management.
  - Host management: On Host setup and management > Manage endpoints > Host management , you can filter your list of hosts to show devices currently in RFM. You can also see the RFM status of a specific host from the host's summary panel. If a host is in RFM or has an unknown RFM status, a warning banner alerts you at the top of the panel.
  - Event search: In Investigate > Search > Advanced event search , search for `SensorStateBitMap` using this query:

    ```
    #event_simpleName=SensorHeartbeat event_platform=Mac ConfigIDBuild>=17506
    | bitfield:extractFlags(field="SensorStateBitMap", output=[[1, RFM]])
    | RFM=true
    | groupBy([aid], function=(selectFromMax(field="@timestamp", include=[@timestamp, ComputerName,
    aid, ConfigBuild])))
    | rename([[ComputerName, Hostname], [aid, "Sensor ID"], [ConfigBuild, "Agent Build"]])
    ```

- Using the API: RFM status information is also available using the host management API. See Host and Host Group Management APIs.

### Resolving RFM for Mac hosts

To restore a Mac host's sensor to full functionality, you must enable Full Disk Access using one of these methods:

- Using an MDM: If you manage hosts using an MDM, you must enable FDA in the applied profiles. See Approving Full Disk Access using MDM.
- Manually in the host's System Preferences: If you don't manage hosts using an MDM, you must manually enable FDA on the host in System Preferences. For more info, see the FDA enablement step of Alternative installation method: Installing without using an MDM to sync profiles.

Important: If you manage FDA using an MDM profile, the host's System Preferences might not accurately reflect the current setting.

After enabling FDA for the Falcon sensor, the host no longer shows a status of RFM in host management. The Zero Trust Assessment (ZTA) score automatically updates with macOS changes every 24 hours, or immediately if you restart the sensor. For more info about ZTA, see Zero Trust Assessment.

## Sensor safe mode: Mac hosts

Starting with Falcon sensor for Mac 7.26, the sensor provides safe mode to detect user mode service crash loops and take corrective action.

The Falcon Sensor for Mac detects sensor-related crash loops and switches to safe mode.

This mode provides no functional capabilities other than ensuring that the sensor gracefully comes back online and connects to the CrowdStrike cloud. The sensor can then receive remediation updates from the CrowdStrike cloud to return to a healthy state.

### Checking if a sensor is in safe mode

To check which hosts have sensors that are in safe mode, you have these options:

- Check the Host Management table

  Go to Host setup and management > Manage endpoints > Host management and check the table's Safe mode column. If the column is not present, add it by using Configure table columns .

  Possible values:

  - Yes
  - No
  - Unknown

    Indicates a supported platform with either a state that cannot be determined or a sensor with a version earlier than 7.26. Safe mode requires version 7.26 or later.

  - N/A

    Indicates an unsupported platform.

- Run a query

  You can check which hosts have sensors that are in safe mode by running a query. Go to Investigate > Search > Advanced event search , set the time interval to Last 5m, and run this query:

```
#event_simpleName=SensorHeartbeat event_platform=Mac ConfigIDBuild>=19707
| bitfield:extractFlags(field="SensorStateBitMap", output=[[3, Safemode]])
| Safemode=true
| groupBy([aid], function=(selectFromMax(field="@timestamp", include=[@timestamp, ComputerName, aid,
ConfigBuild])))
| rename([[ComputerName, Hostname], [aid, "Sensor ID"], [ConfigBuild, "Agent Build"]])
```

## Resolving safe mode for Mac hosts

A sensor in safe mode periodically attempts to return to a healthy state.

However, if you encounter a host in safe mode, visit the CrowdStrike Customer Center and open a support case.