cyberhaven

Jamf Installation Documentation

Installing the macOS Sensor

The macOS Endpoint Sensor can be deployed to your endpoint devices using any MDM.

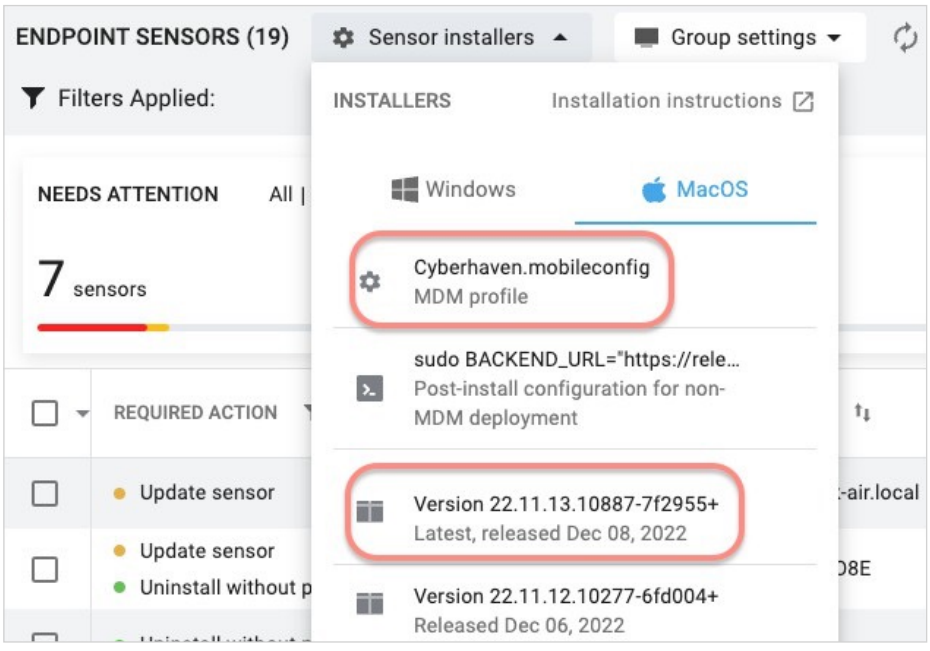
You can also manually install the Sensor on an individual device, but that is not recommended and is not supported for production use.

As part of your MDM configuration, you can also set up the Sensor as a Login item to prevent users from disabling Cyberhaven on their device. See Manage macOS Sensor as a Login Item using MDM.

Prerequisites

From the Cyberhaven Console, ensure that you have downloaded the following:

- macOS sensor installer
- macOS MDM configuration profile
- prior to Cyberhaven version 23.02 additional profiles may have been required; please see MDM profiles for an overview.



Tokens Request and Refresh

On the first startup following a fresh installation or upgrade of the macOS Sensor, the MDM profile must contain a valid installation token. This token is required for the Sensor to connect with the backend.

IMPORTANT

Install tokens expire every six months. As a best practice, we recommend updating your MDM profile with a new install token every four months. This proactive measure helps ensure continuous service and prevents disruptions when upgrading existing sensors or installing the Sensor on new macOS machines.

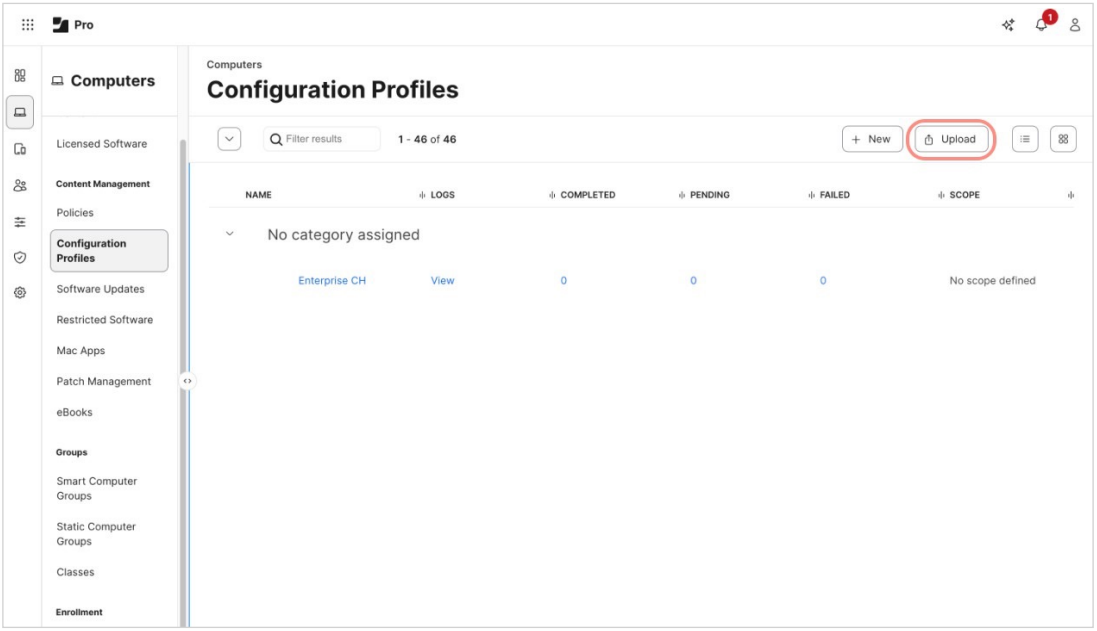
The Sensor reads the install token from the MDM Profile. It uses the token to obtain an AccessToken via the 'authorize' API. This AccessToken is then persisted to the Keychain-backed SecureStore.

The Sensor then refreshes the AccessToken on a regular interval (1 day by default, the same as Windows) using the new 'refresh-token' API.

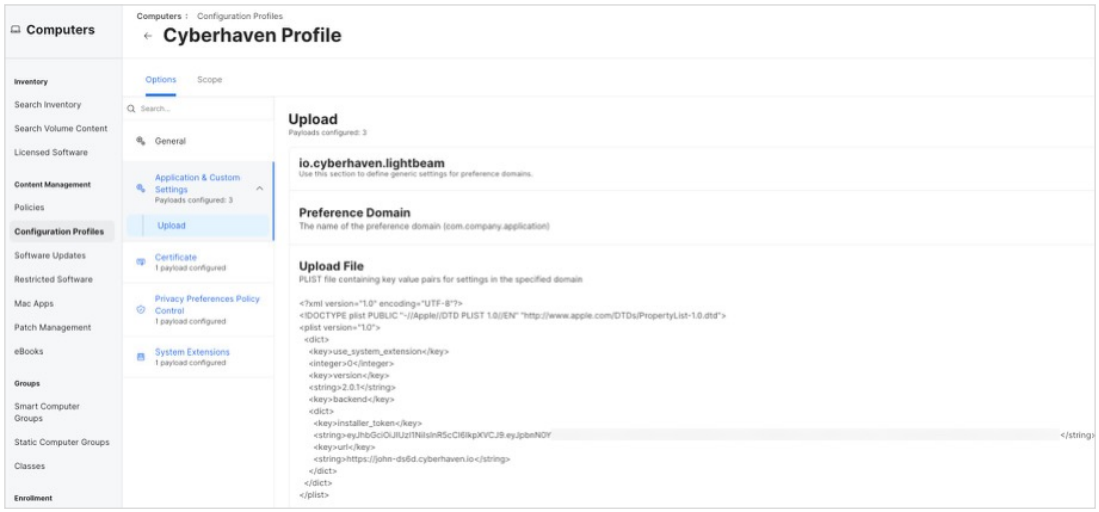
Install using Jamf

Updated on Dec 10, 2025

1. Upload the ready-made profile you downloaded from your Cyberhaven instance to create the privacy preferences policy control in Jamf.



2. Go to **Application & Custom Settings > Upload** and verify the uploaded package.



3. In the Scope tab, assign the profile to the computers and users of your choice. For instance, you can deploy to all computers and users.
4. Ensure that all privacy profiles have been pushed to the computers in scope.
5. After all computers in scope have had the Cyberhaven profile deployed (no pending or failed profile deployments), you can set up a policy to install the Cyberhaven package to the same scope (i.e., computers, users) as the Cyberhaven privacy profile. Note that users who receive the package before their privacy profiles were fully deployed will get popups to request security and privacy permissions.

Known Issue: VPN Configuration Prompt

Some MDM solutions may prompt for a VPN hostname when uploading the Cyberhaven MDM profile (version 2.0.8 or later), due to the inclusion of inline proxy support for Microsoft Teams traffic inspection. If prompted, enter 127.0.0.1 as the VPN hostname to proceed with the upload.