CrowdStrike Falcon Protection (macOS)

Description

Needing to deploy to CrowdStrike Falcon antivirus to your macOS fleet? FileWave has you covered.

CrowdStrike's flagship product is called Falcon, which is a cloud-native platform that combines next-generation antivirus, endpoint detection and response (EDR), threat intelligence, and proactive threat hunting. Falcon aims to provide real-time visibility into endpoint activity, rapid threat detection, and automated response to security incidents.

Ingredients

- FileWave Admin Central
- CrowdStrike Falcon Profile (Intel or Apple Silicon)
- CrowdStrike PKG installer
- CrowdStrike License code

Directions

Deploying the CrowdStrike Falcon to your devices

CrowdStrike deployment for macOS requires two Filesets: one TCC profile and the PKG installer. The TCC profile is dependent on which architecture your macOS fleet is, both are provided in this article for download. The PKG installer has two scripts that will execute with your CrowdStrike Falcon license and check for the TCC profile to be installed before CrowdStrike application.

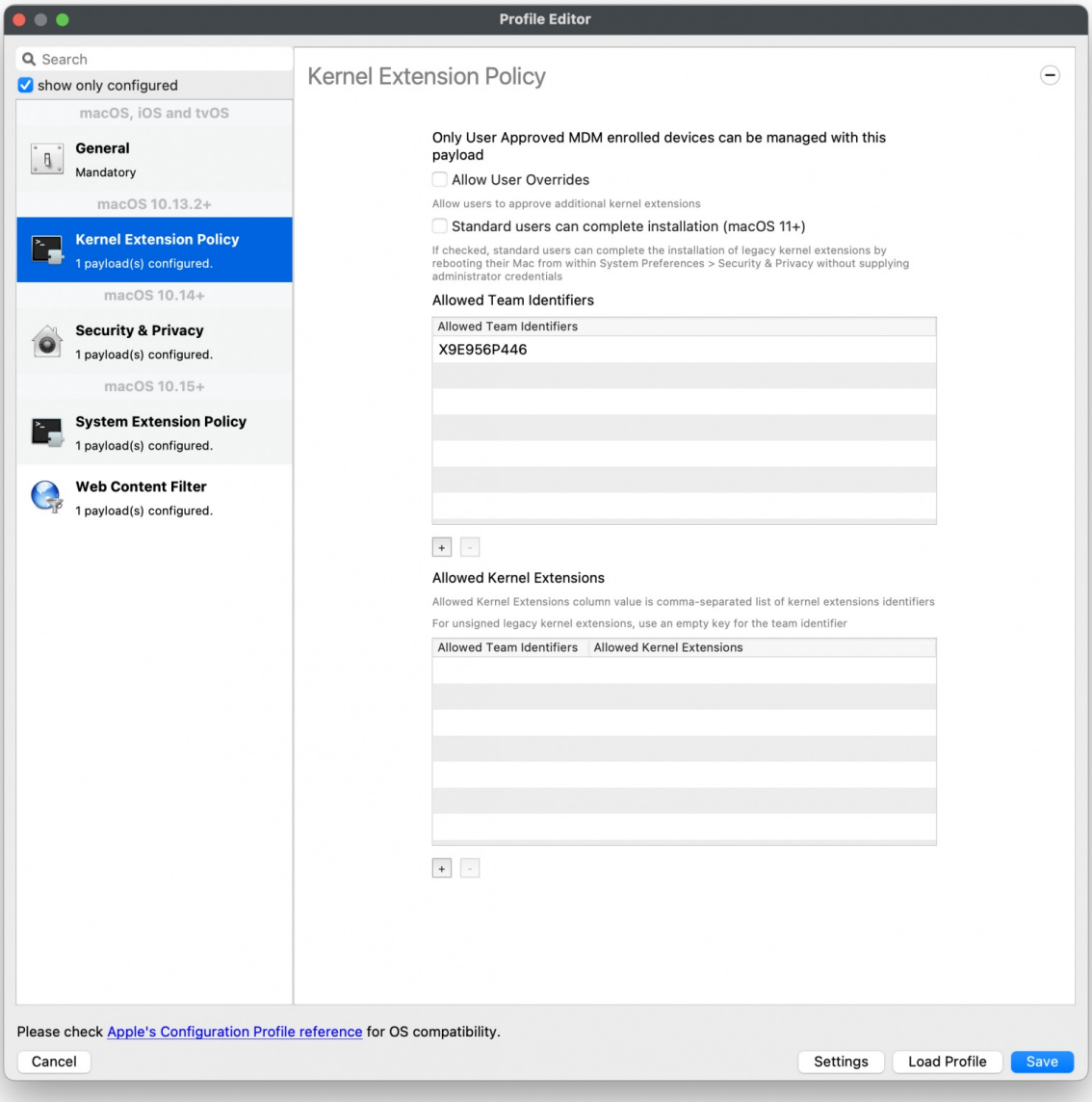
Download the TCC profile

> Note: Please download and verify the TCC profile for your macOS architecture. Below are screen shots of both Intel and Apple Silicon

Intel based macOS devices:

Falcon Profile for Intel.fileset.zip

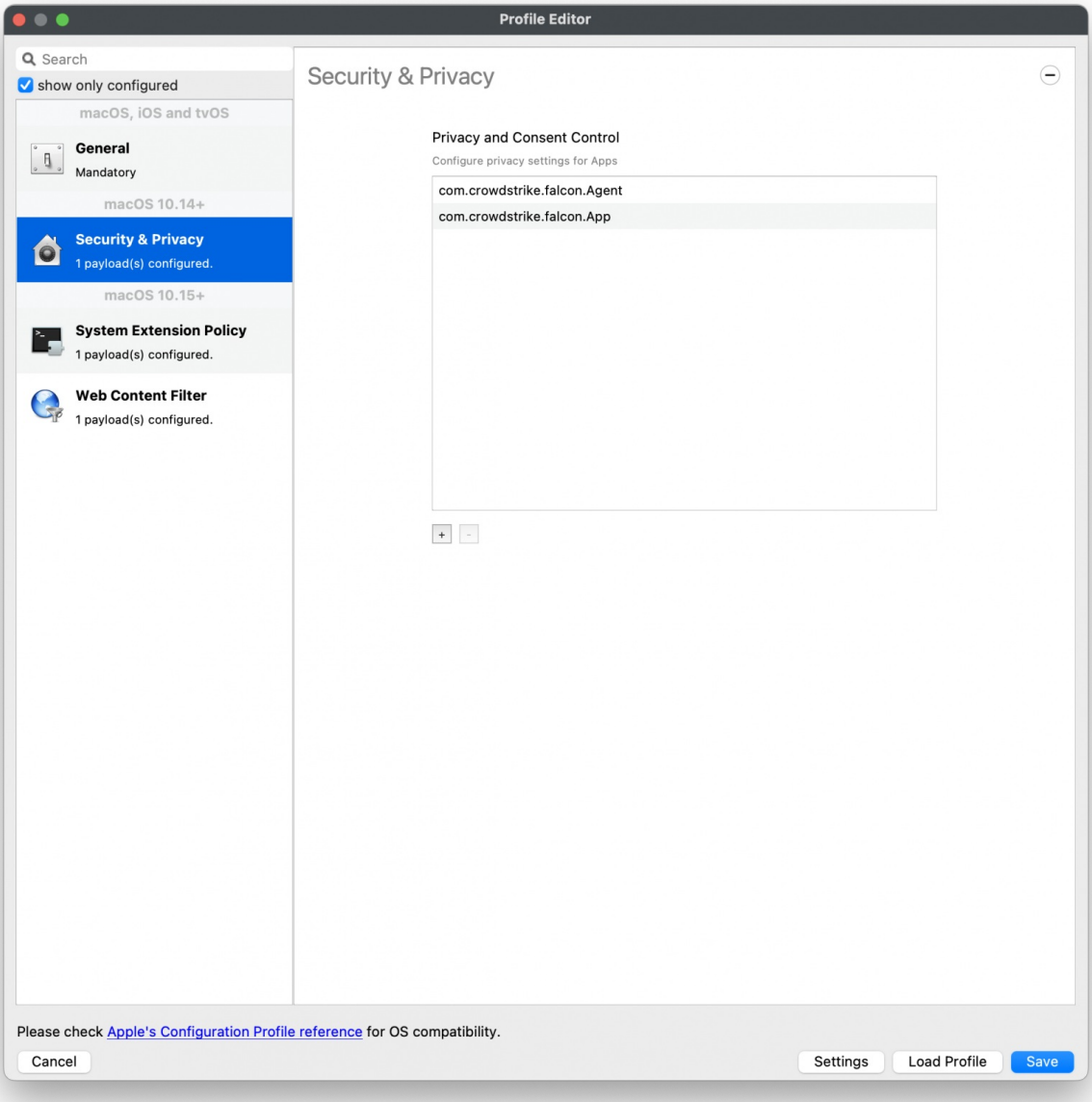
▼ Intel based TCC Profile



Apple Silicon based macOS devices:

Falcon profile for M1.fileset.zip

▼ Apple Silicon based TCC Profile

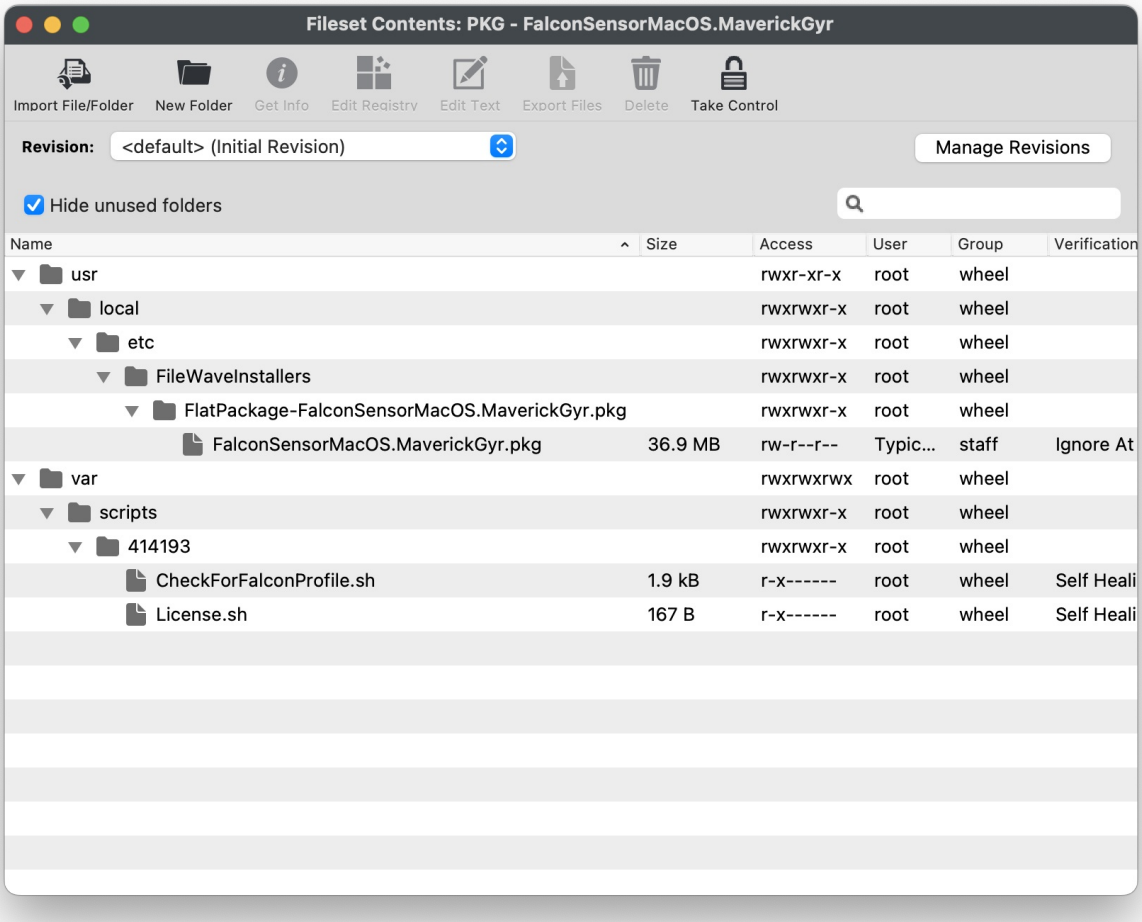


Download the PKG installer

The PKG installer will have three components in the Fileset. Note the PKG installer, along with the two scripts: a requirement and activation script.

> ⚠ The Fileset included with the PKG installer is version 6.58.17102.0 of CrowdStrike for macOS Big Sur and beyond (This version will not install on macOS Catalina).

PKG - FalconSensorMacOS.MaverickGyr.fileset.zip

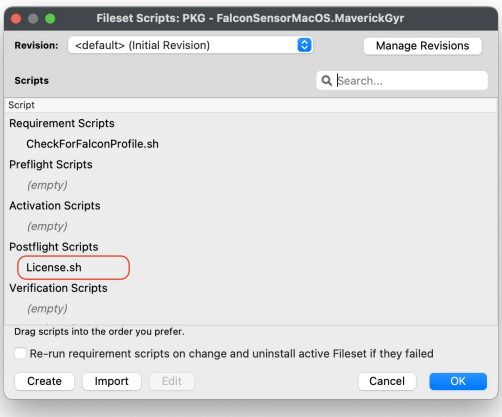


CrowdStrike License

Customizing the Fileset with your CrowdStrike license is required. The Fileset has a License.sh script to edit and enter in your license code.

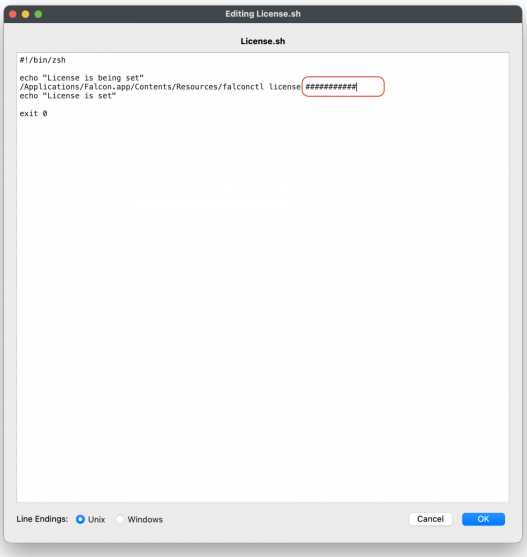
Editing the License.sh script

1. Highlight your CrowdStrike PKG installer Fileset
2. Select Scripts to open the Script window.
3. Highlight License.sh
4. Click Edit



Entering in your license code

1. Highlight the ####### string and enter in your CrowdStrike License code
2. Click OK to save
3. Click OK to save again to save your license code for the CrowdStrike Fileset



▼ License code script

```
#!/bin/zsh

echo "License is being set"
/Applications/Falcon.app/Contents/Resources/fa
lconctl license ##########
echo "License is set"

exit 0
```

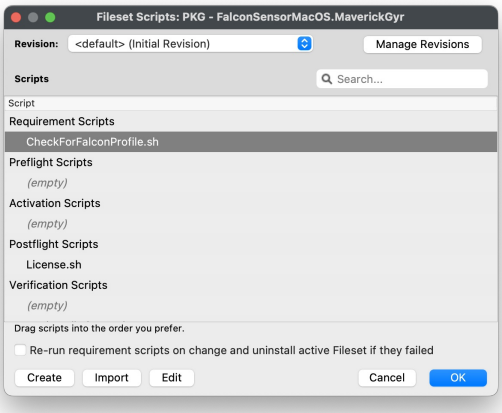
Check for Falcon Profile

The Payload Identifiers are already set and entered. The below are step-by-step instructions to add your own Payload Bundle Identifier if needed.

> ⚠ Note: The Requirement script verifies that the CrowdStrike Falcon Profile is installed successfully BEFORE running the installation of CrowdStrike.
>
> There are two entries for your profile identifiers: you may enter both the Intel and Apple Silicon as the script will check for either profile is installed successfully BEFORE running installation of CrowdStrike.

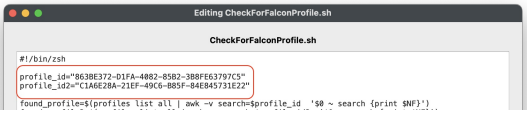
Editing the CheckForFalconProfile.sh

1. Highlight your CrowdStrike PKG installer Fileset
2. Select Scripts to open the Scripts window
3. Highlight the CheckForFalconProfile.sh script
4. Click Edit

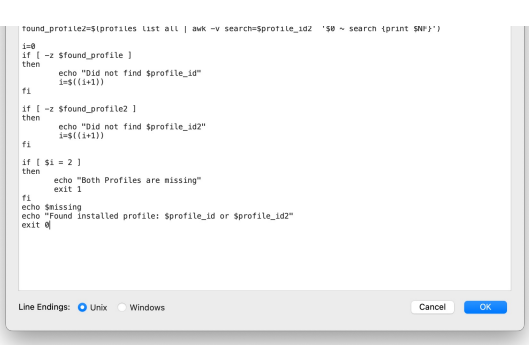


Entering in your Intel and/or Apple Silicon Profile Identifier

1. Highlight the string after profile_id="#####"

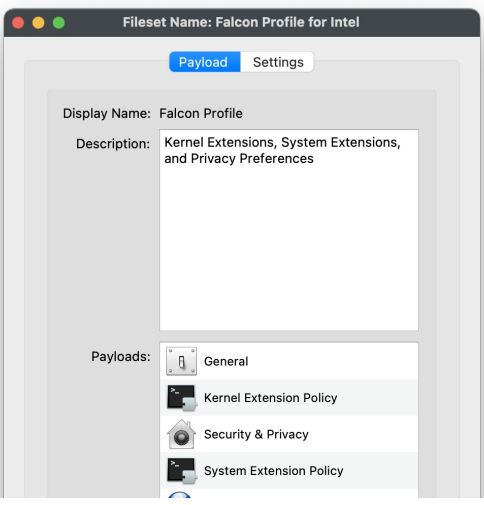


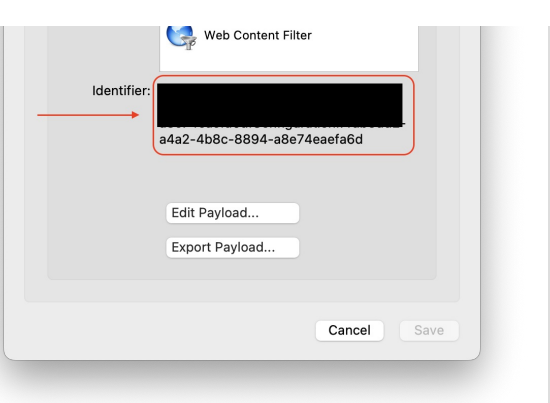
2. Replace the ######, with your TCC profile Identifier.
3. If not sure, open your Intel or Apple Silicon Profile and copy the Identifier.
4. Click OK to save
5. Click OK to save again to save your changes to the CrowdStrike Fileset



▼ Check for Falcon profile script

```
#!/bin/zsh

profile_id="863BE372-D1FA-4082-85B2-
3B8FE63797C5"
profile_id2="C1A6E28A-21EF-49C6-B85F-
84E845731E22"

found_profile=$(profiles list all | awk -v
search=$profile_id  '$0 ~ search {print $NF}')
found_profile2=$(profiles list all | awk -v
search=$profile_id2  '$0 ~ search {print
$NF}')

i=0
if [ -z $found_profile ]
then
        echo "Did not find $profile_id"
        i=$((i+1))
fi

if [ -z $found_profile2 ]
then
        echo "Did not find $profile_id2"
        i=$((i+1))
fi

if [ $i = 2 ]
then
       echo "Both Profiles are missing"
       exit 1
fi
echo $missing
echo "Found installed profile: $profile_id or
$profile_id2"
exit 0
```





Creating a Fileset Group

Keeping your Filesets organized is good practice, especially if there are multiple Filesets for software deployment. You may create a New Fileset Group, label it CrowdStrike Falcon (macOS 2023), and move all the Filesets you created into that Fileset Group. Then associate the Fileset Group labeled CrowdStrike Flacon (macOS 2023) to your devices versus individual Filesets.

Once all the Fileset and Profile have been created, you may associate the Fileset Group labeled CrowdStrike Falcon (macOS 2023) to a few devices as a test. This is to verify and confirm that the software is installed properly based on your license code configured.

Related Content

- CrowdStrike Falcon Protection (Windows EXE)

Revision #15
★Created 29 August 2023 15:05:11 by Andrew Kloosterhuis
✎Updated 12 September 2023 13:36:38 by Josh Levitsky