VMware Carbon Black Cloud sensor recipe (macOS)

Description

VMware Carbon Black is a powerful endpoint protection solution that plays a critical role in an organization's cybersecurity strategy. Deploying Carbon Black via the installer package through the admin console is a strategic approach that ensures consistent, efficient, and effective endpoint security. By mastering this deployment process, organizations can enhance their cybersecurity posture, mitigate threats proactively, and protect their digital assets in an increasingly dangerous digital landscape.

This guide will help you create a Fileset and deploy the application along with the required profiles.

Ingredients

- FileWave Central
- VMware Carbon Black Cloud dmg
- VMware CBC license code
- VMware CBC uninstaller code
- System Extension mobile configuration
- Network Extension Web Content Filter mobile configuration
- TCC Privacy Policy mobile configuration

Downloads

VMware CBCloud Profiles.zip

VMware Carbon Black Cloud.fileset.zip

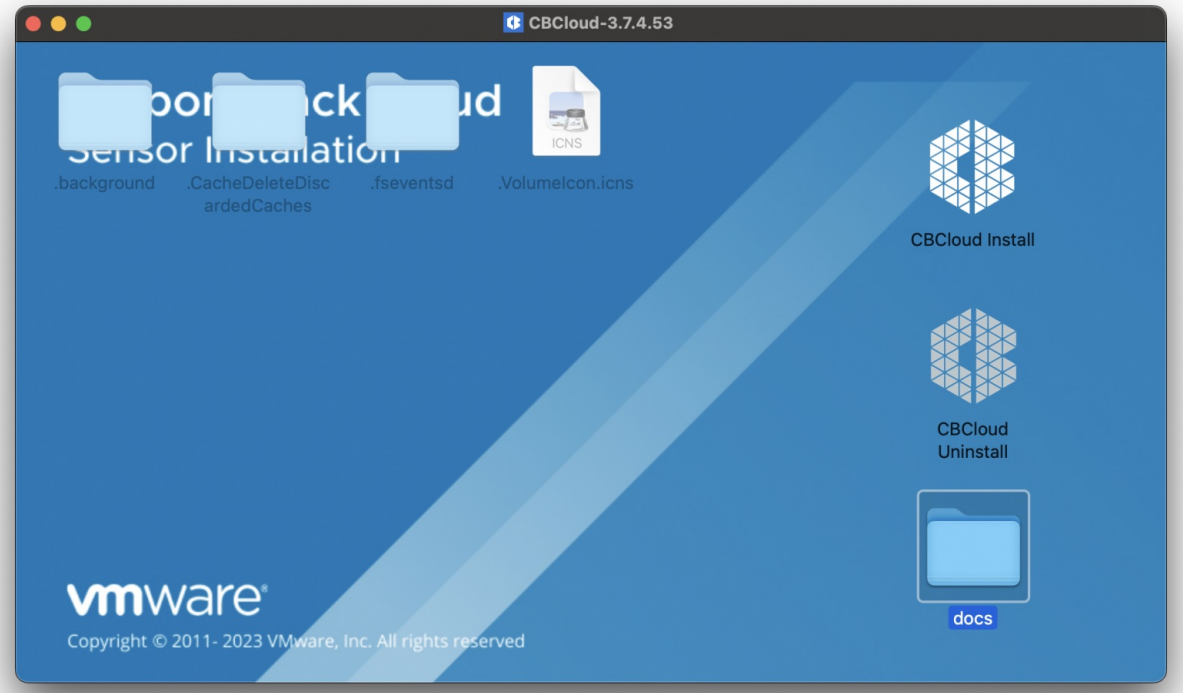
Directions

> ⚠ Please note this recipe includes Carbon Black Cloud sensor (CB Defense) version 3.7.4.53. This version is supported on MacOS 11.0 and newer.

Downloading and extracting the MDM profiles and installers

You will first want to grab and download your VMware installations and profiles. The .dmg will need to be mounted first and then extract the necessary components from this file.

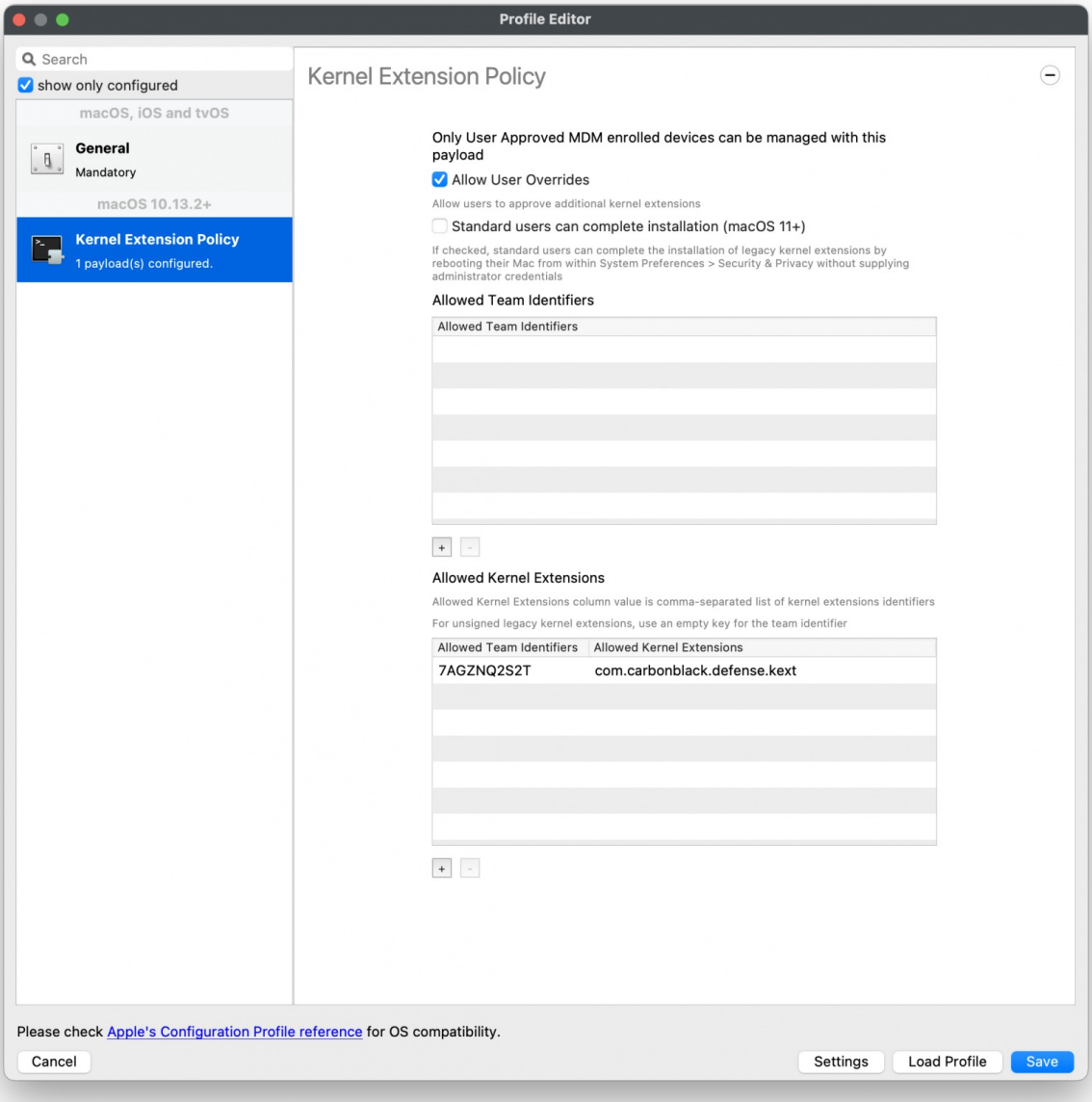
Once the .dmg has been mounted you will see the contents listed. Below is the CBCloud Install.pkg and doc folder containing the required MDM profiles.



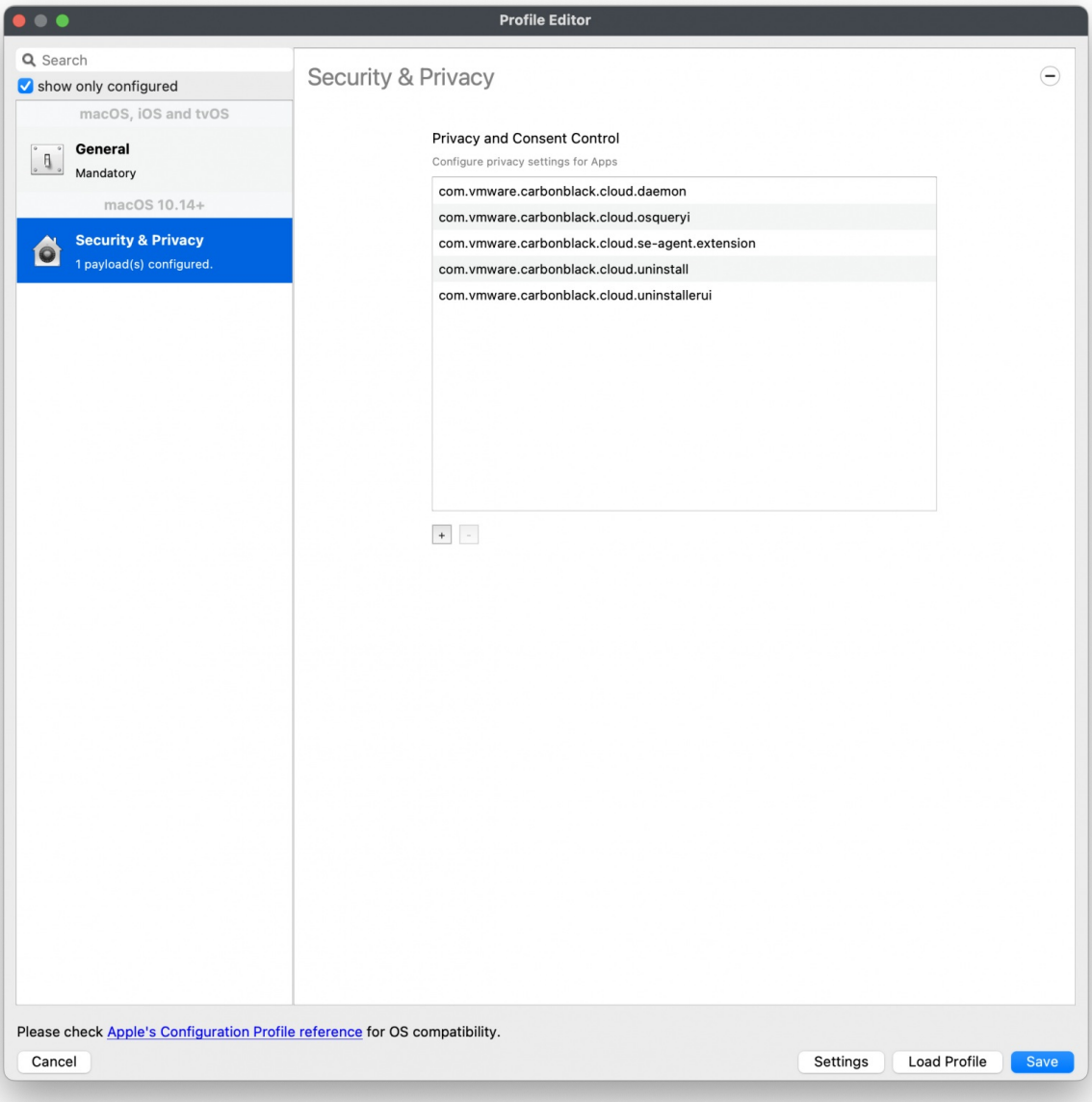
The required MDM profiles and unattended script for the Fileset deployed are found in the docs folder within the mounted .dmg.

Extract the MDM profiles. These MDM profiles will be uploaded into FileWave Central. Below are the configurations for the three MDM profiles:

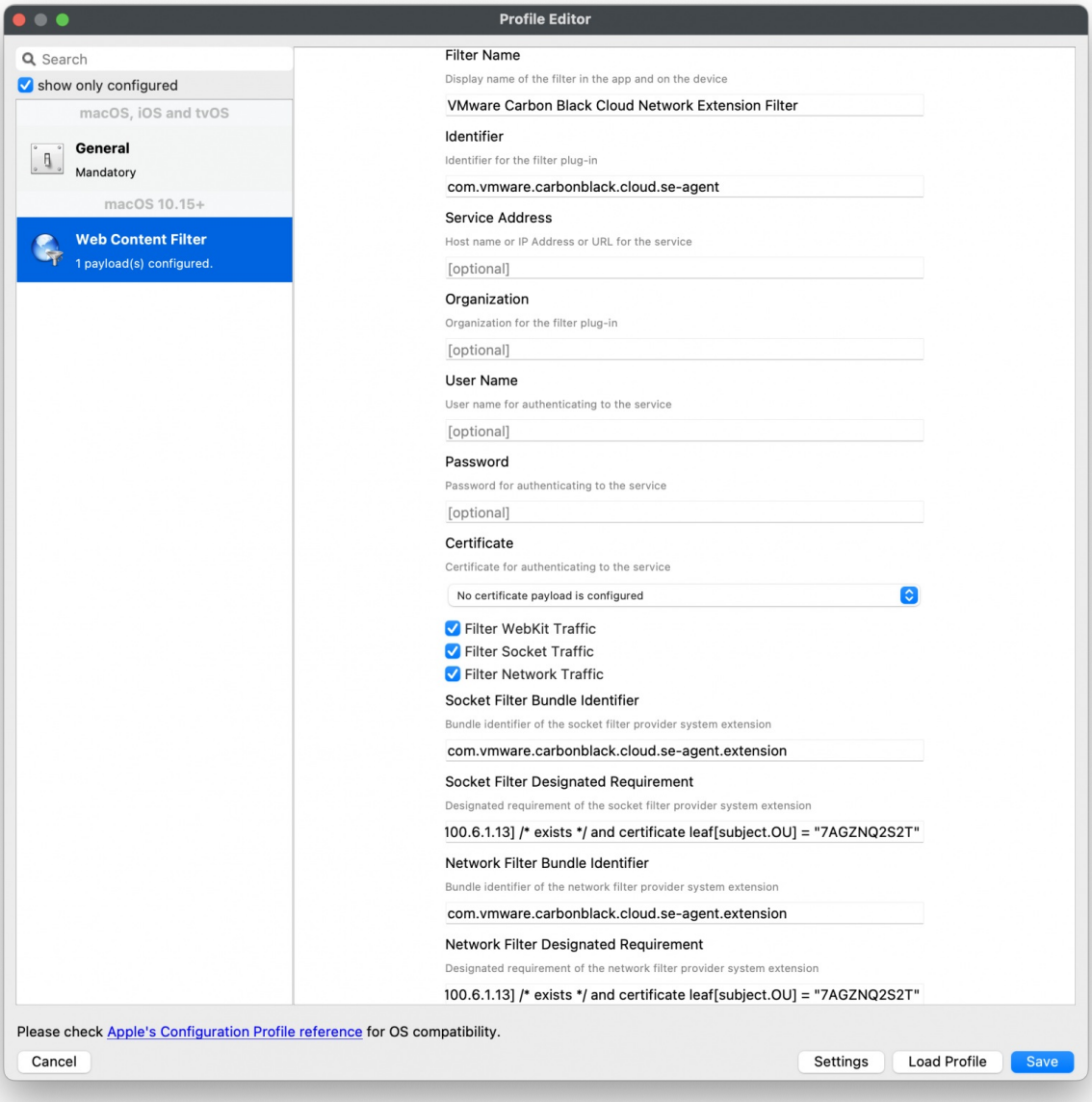
▼ Kernel Extension Policy



▼ Privacy and Consent Control (TCC) Policy



▼ Web Content Filter Policy



MDM Profiles Configurations

If you do not have the VMware Carbon Black Cloud .dmg, you may create the Profiles with the following.

> ⚠ VMware CCB macOS version 3.8+ introduces Approving the System Extension

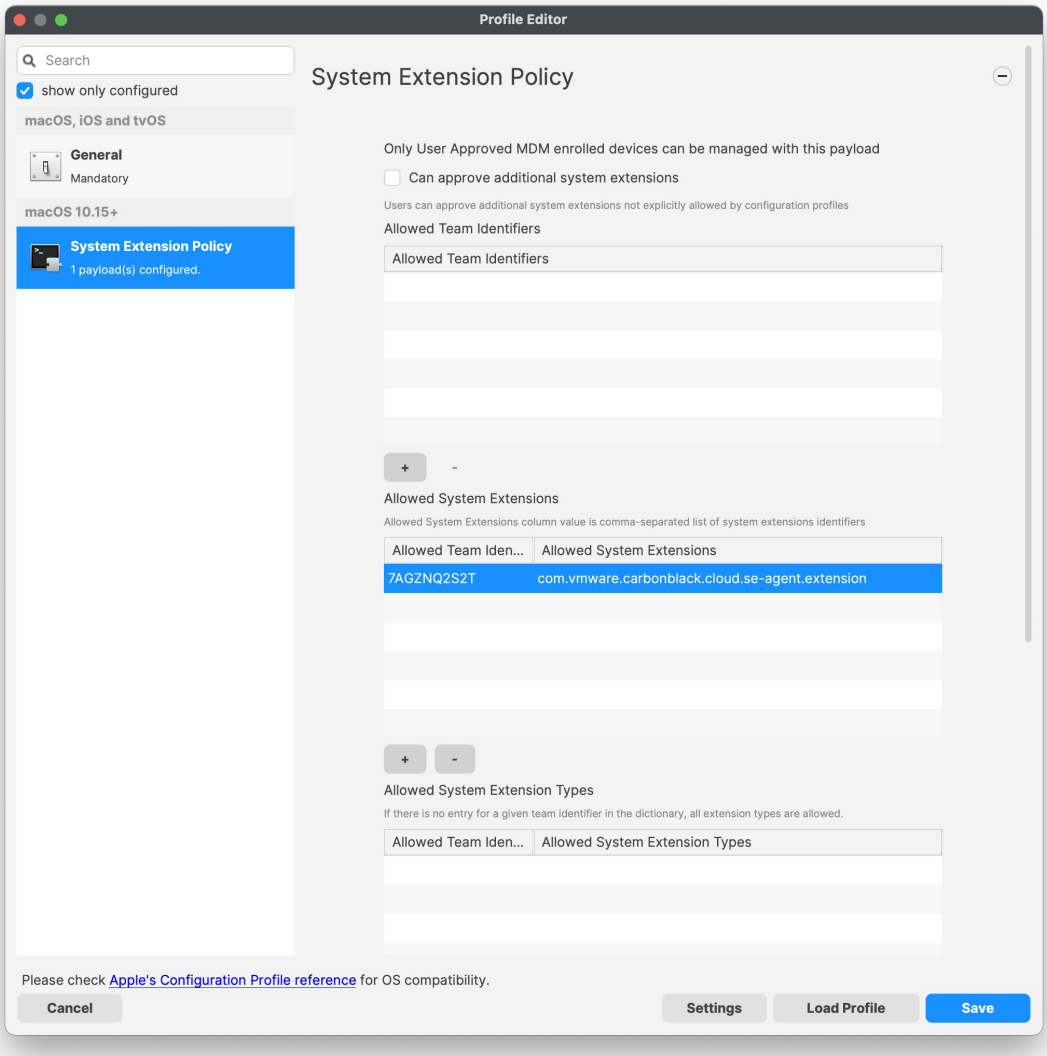
Approve System Extension

For the Allowed System Extension, please enter in the following:

▼ System Extension Policy

Specify the Apple Team ID and System Extension bundle Identifier in your Allowed System Extension configuration profile:

- System Extension Types: Allowed System Extensions
- Apple Team ID: 7AGZNQ2S2T
- System Extension Bundle ID: com.vmware.carbonblack.cloud.se-agent.extension



Kernel Extension Policy

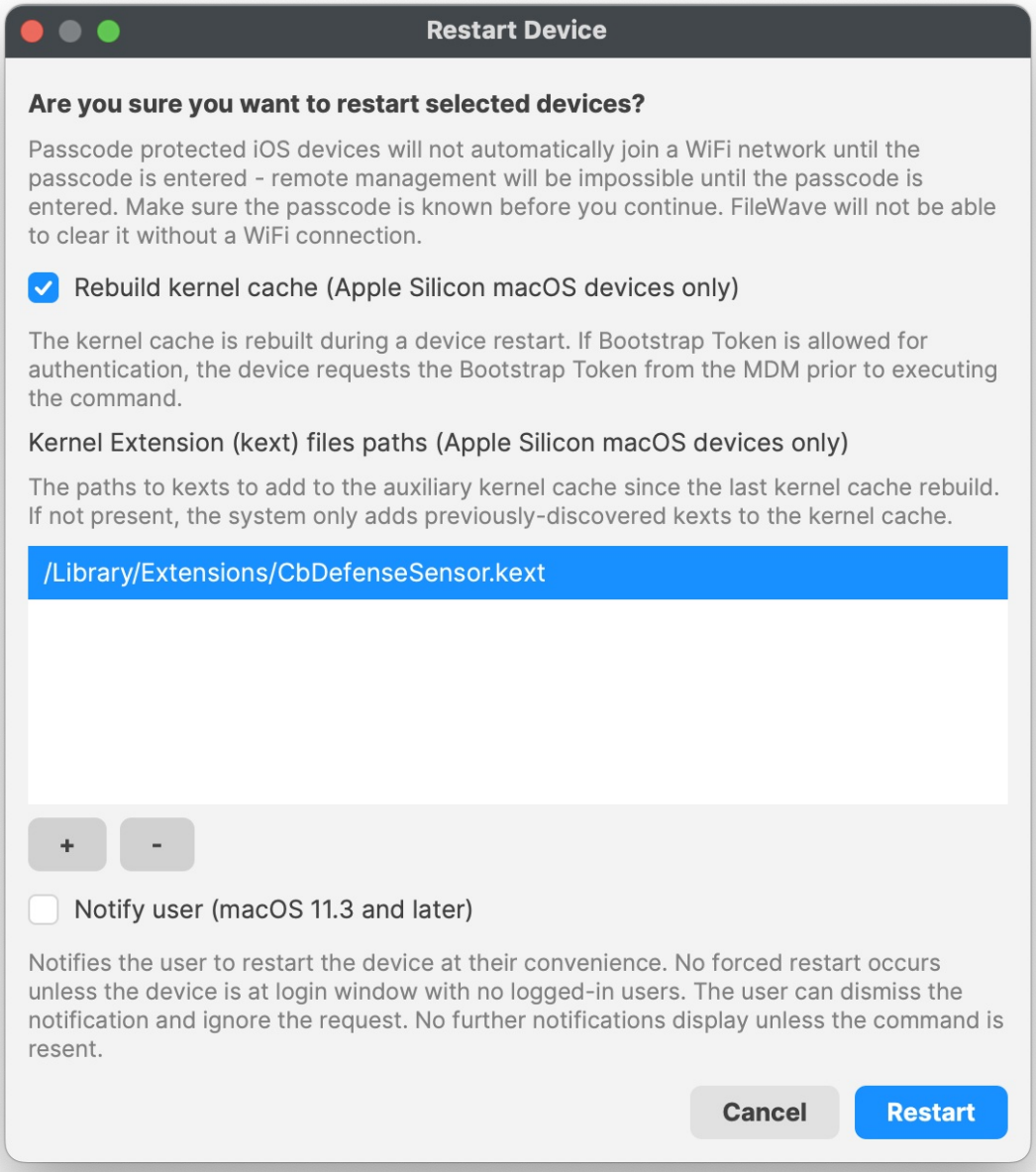
For the Kernel Approval profile, please enter in the TeamID and BundleID:

Apple Team ID: 7AGZNQ2S2T

KEXT Bundle ID: com.carbonblack.defense.kext

> Kernel Extension Policy: The recommended way to deliver this configuration is through the provided MDM-KEXT-reboot-command.xml. FileWave has the Rebuild Kernel Cache command by highlighting the MDM client, right-clicking Restart (Supported MDM devices), checking the box for Rebuild Kernel Cache, and entering in the Kernel file path:
>
> /Library/Extensions/CbDefenceSensor.kext

▼ Kernel Rebuild Cache



Privacy and Consent Control (TCC) Policy

The following will need to be entered for each of the BundleIDs along with Code Requirements and Services to set.

▼ TCC metadata

The fields should be completed exactly as follows. Please copy and paste for accuracy.
1]
Identifier: com.vmware.carbonblack.cloud.daemon

Identifier Type should be set to: Bundle ID

Code Requirement: identifier "com.vmware.carbonblack.cloud.daemon" 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] = "7AGZNQ2S2T"

App or Service should be set to: SystemPolicyAllFiles

Access should be set to: Allow

2]
Identifier: com.vmware.carbonblack.cloud.se-agent.extension

Identifier Type should be set to: Bundle ID

Code Requirement: identifier "com.vmware.carbonblack.cloud.se-agent.extension" 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] = "7AGZNQ2S2T

App or Service should be set to: SystemPolicyAllFiles

Access should be set to: Allow

3]
Identifier: com.vmware.carbonblack.cloud.osqueryi

Identifier Type should be set to: Bundle ID

Code Requirement: identifier "com.vmware.carbonblack.cloud.osqueryi" 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] = "7AGZNQ2S2T"

App or Service should be set to: SystemPolicyAllFiles

Access should be set to: Allow

4]
Identifier: com.vmware.carbonblack.cloud.uninstall

Identifier Type should be set to: Bundle ID

Code Requirement: identifier "com.vmware.carbonblack.cloud.uninstall" 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] = "7AGZNQ2S2T"

App or Service should be set to: SystemPolicyAllFiles

Access should be set to: Allow

5]
Identifier: com.vmware.carbonblack.cloud.uninstallerui

Identifier Type should be set to: Bundle ID

Code Requirement: identifier "com.vmware.carbonblack.cloud.uninstallerui" 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] = "7AGZNQ2S2T"

App or Service should be set to: SystemPolicyAllFiles

Access should be set to: Allow

Web Content Filter Policy

The following will need to be entered to create the web content filter manually.

▼ Web Content Filter Policy

The fields should be completed exactly as follows. Please copy and paste for accuracy.

In the General payload:

Payload Scope should be set to: System

In the Web Content Filter payload:

Filter Type: Plug-In

Plug-In Bundle ID: com.vmware.carbonblack.cloud.se-agent

Check Enable Socket Filtering

Filter Data Provider System Extension Bundle ID (macOS): com.vmware.carbonblack.cloud.se-agent.extension

Filter Data Provider Designated Requirement (macOS): identifier "com.vmware.carbonblack.cloud.se-agent.extension" 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] = "7AGZNQ2S2T"

Check Enable Packet Filtering (macOS)

Filter Packet Provider System Extension Bundle ID (macOS): com.vmware.carbonblack.cloud.se-agent.extension

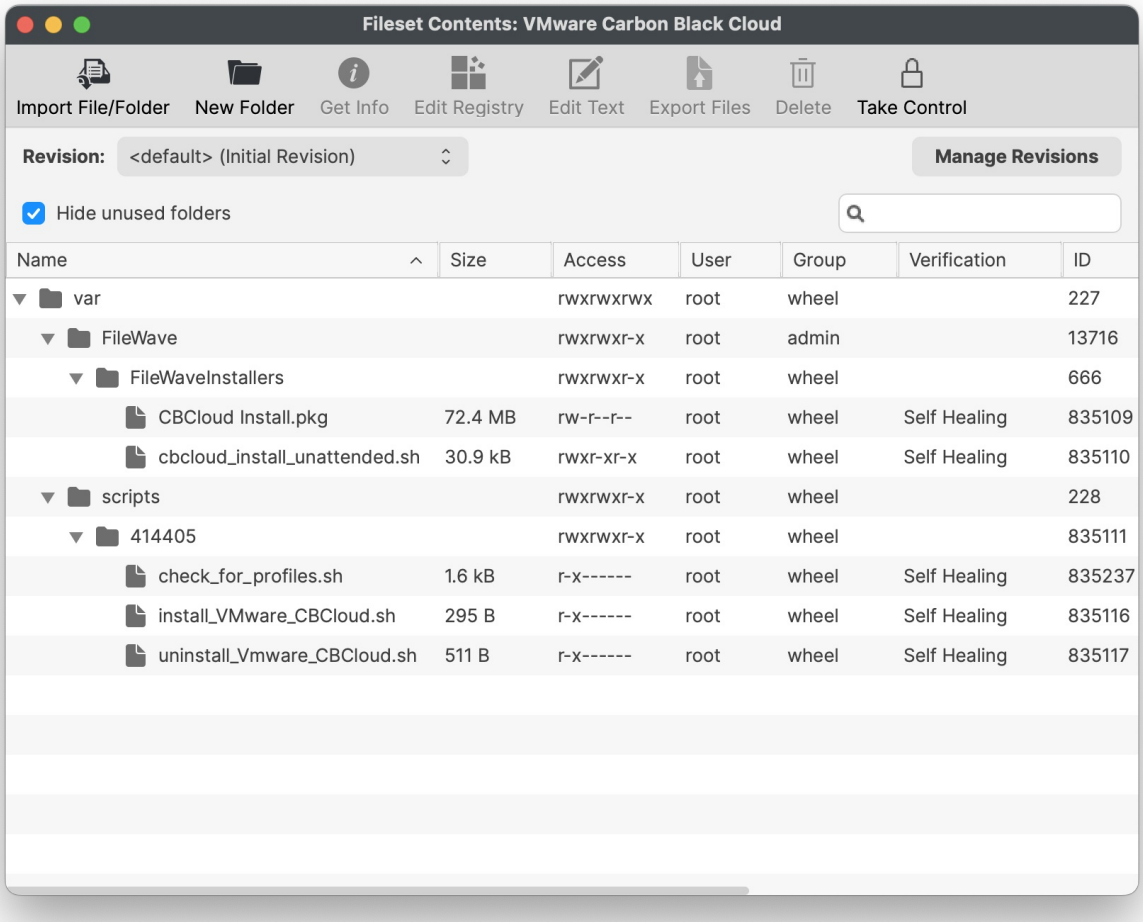
Filter Packet Provider Designated Requirement (macOS): identifier "com.vmware.carbonblack.cloud.se-agent.extension" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = "7AGZNQ2S2T"

Creating the VMware Carbon Black Cloud Fileset

You may download and upload the VMware Carbon Black Cloud Fileset into your FileWave Admin. You should see four items listed in the Fileset Contents:

1. CBCloud Install.pkg
2. check_for_profiles.sh script
3. cbcloud_install_unattended.sh script
4. install_VMware_CBCloud.sh script
5. uninstall_VMware_CBCloud.sh script

Verification Settings: VMware CBCloud client will get updates from the CBCloud server. If your organization allows, be sure to change the verification settings from 'Self-Healing' to 'Ignore at Verify' for the Fileset.

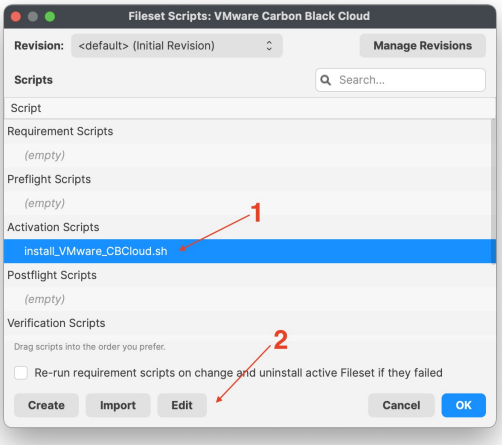


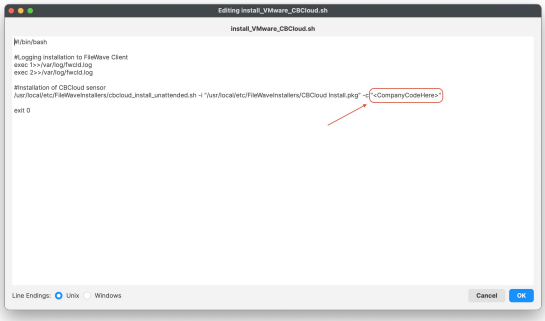
VMware CBCloud install script

You will need to modify and add your company code to the install_VMware_CBCloud.sh script.

1. Highlight the Fileset and click on Scripts (FW Central menu)
2. Highlight Activation Scripts, install_VMware_CBCloud.sh
3. Click on Edit to open the script

4. Enter your company code, i.e. #######
5. Click OK to save
6. Click OK to save your changes

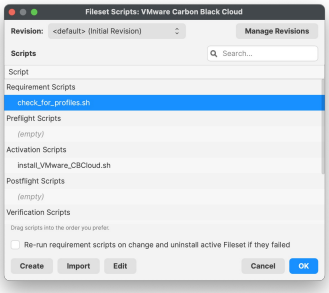


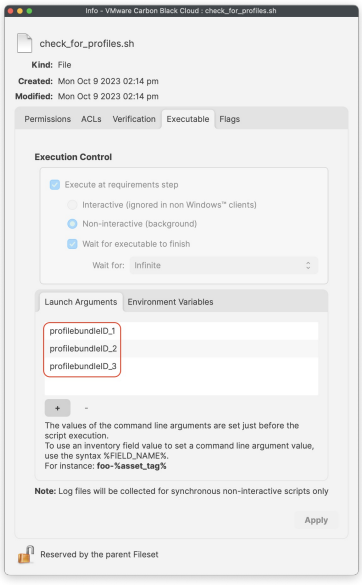


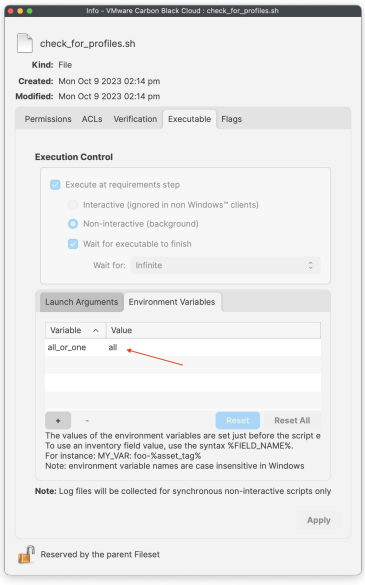
Check for Profiles requirement script

You will need to modify and add your profile bundle IDs to the requirement script.

1. Highlight the Fileset and on Scripts (FW Central menu)
2. Highlight Requirement Scripts, check_for_profiles.sh
3. Right-click and select properties
4. Select and click on the Launch Arguments tab
5. Enter in your three profile bundle IDs
6. Click 'Apply' to save your changes
7. Select and click on the Environment Variables tab
8. Confirm the all_or_one variables string is set to 'all'
9. Click 'Apply' to save your changes, if not saved
10. Close the script properties window
11. Click OK to save your changes to the requirement script







Vmware uninstall script

> ⚠ This is optional and not required!

If you have a company code to allow uninstallation of the VMware Carbon sensor, you may enter your code into the script under:

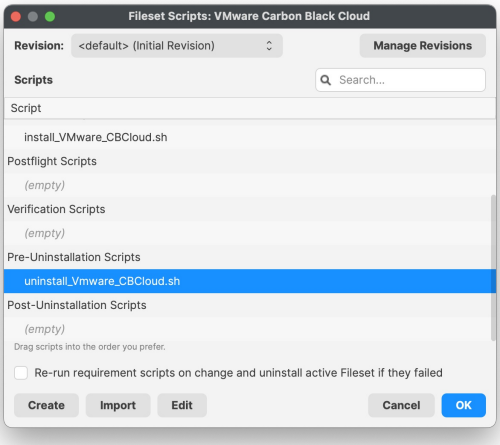
- Line 12 <CompanyCodeHere>; replace with your code and remove the <>

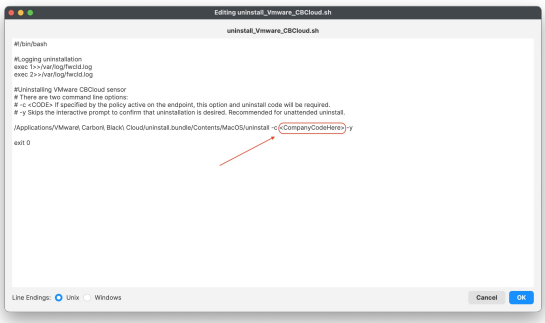
▼ uninstall_Vmware_CBCloud.sh

```
#!/bin/bash

#Logging uninstallation
exec 1>>/var/log/fwcld.log
exec 2>>/var/log/fwcld.log

#Uninstalling VMware CBCloud sensor
# There are two command line options:
# -c <CODE> If specified by the policy active on the endpoint, this option and uninstall code will be
required.
# -y Skips the interactive prompt to confirm that uninstallation is desired. Recommended for unattended
uninstall.

/Applications/VMware\ Carbon\ Black\ Cloud/uninstall.bundle/Contents/MacOS/uninstall -c <CompanyCodeHere> -y

exit 0
```

To make the changes in the Fileset:

1. Highlight the Fileset and click on Scripts (FW Central menu)
2. Highlight Pre-Uninstallation Scripts, uninstall_VMware_CBCloud.sh
3. Click on Edit to open the script
4. Enter in your company code, i.e. #######
5. Click OK to save
6. Click OK to save your changes





Fileset Group

Once the Fileset and Profiles have been created, the best practice is to create a Fileset group. Organizing and keeping multiple profiles and Filesets within the same group for the same application and its configurations is great management and organization.

> Profiles should be installed first. The VMware Carbon Black Cloud Fileset has a requirement script to ensure profiles are installed, before commencing with download and activation of the Fileset.

Remember to always test Fileset to a few devices before mass deployment.

Related Content

- VMware Carbon Black Cloud release notes

Revision #24
★Created 27 September 2023 18:53:45 by Andrew Kloosterhuis
✎Updated 12 March 2024 13:12:57 by Andrew Kloosterhuis