

AnyConnect Changes Related to macOS 11 (Big Sur)

Table of Contents

1. Introduction	2
2. About the AnyConnect System Extension	2
3. Approving the AnyConnect System Extension	4
3.1 Extension Approval by End User	4
3.2 Extension Approval using MDM	8
3.3 Confirming AnyConnect Extension Approval	8
3.4 AnyConnect Extension Deactivation	9
4. Last-resort Workaround: Failover to Kernel Extension	9
4.1 Kernel Extension Approval using MDM	9
4.2 Failover to Kernel Extension	10
5. Sample MDM Configuration Profile for AnyConnect System and Kernel Extension Approval	10

Table of Figures

Figure 1 - DNS proxy component	3
Figure 2 - App/Transparent proxy component	3
Figure 3 - Content filter component	4
Figure 4 - Extension blocked - OS prompt	5
Figure 5 - Extension blocked - AnyConnect prompt	5
Figure 6 - AnyConnect extension approval	6
Figure 7 - AnyConnect extension approval (multiple unapproved extensions)	7
Figure 8 - AnyConnect extension's content filter approval	7
Figure 9 - AnyConnect extension approval confirmation	8
Figure 10 - Extension deactivation prompt.....	9

1. Introduction

AnyConnect 4.9.03xxx leverages the System Extension framework available in macOS 11 (Big Sur). This differs from past AnyConnect versions, which rely on the now-deprecated Kernel Extension framework. This is the minimum version required to run AnyConnect on macOS 11.

This advisory describes changes introduced in the new AnyConnect version and the steps administrators can take to confirm AnyConnect is operating correctly on macOS 11. There are important changes in approving the AnyConnect system extension, as detailed in the next section.

The advisory also details the steps for failing over to the AnyConnect kernel extension, as last-resort workaround in case a critical system extension (or related OS framework) issue is encountered. The AnyConnect kernel extension is installed on macOS 11 solely for this purpose, it is no longer used by default.

2. About the AnyConnect System Extension

AnyConnect uses a network system extension on macOS 11, bundled into an application named Cisco AnyConnect Socket Filter. (This app controls the extension activation and deactivation and is installed under /Applications/Cisco .)

The AnyConnect extension has the following three components:

- DNS proxy
- App/Transparent proxy
- Content filter

These components are visible in the macOS System Preferences – Network UI window:

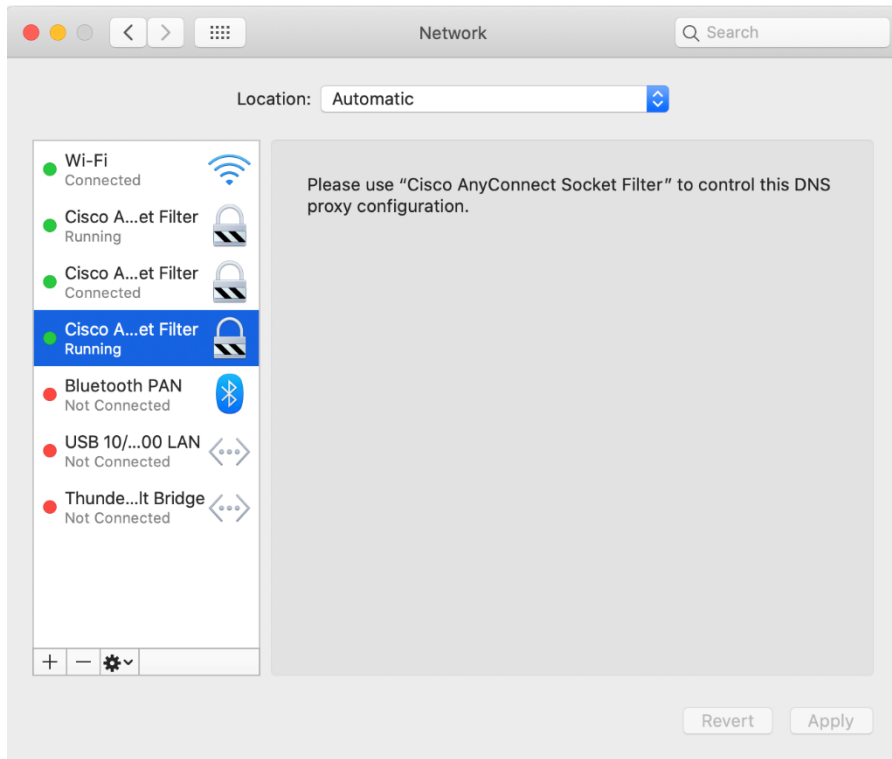


Figure 1 - DNS proxy component

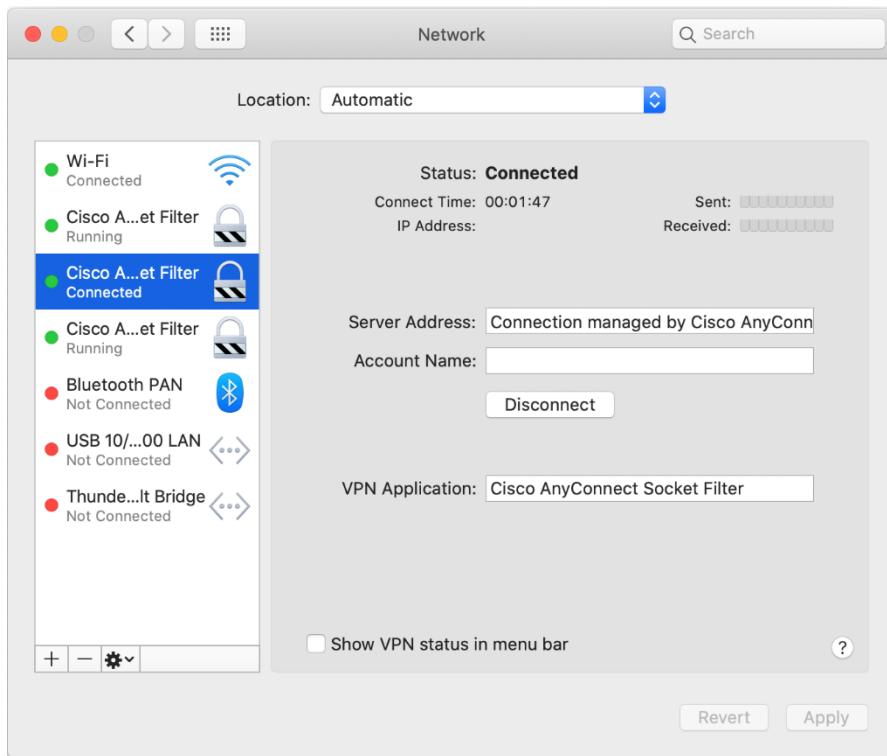


Figure 2 - App/Transparent proxy component

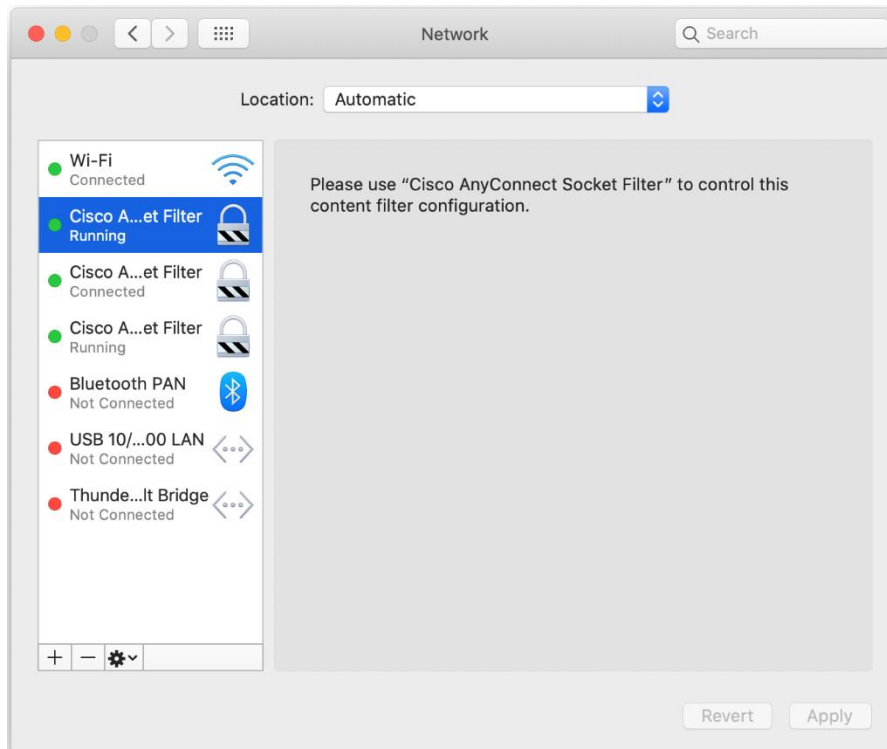


Figure 3 - Content filter component

AnyConnect requires its system extension and all its components to be active in order to operate properly, which implies that the mentioned components are all present and show up as green/running in the left pane of the macOS Network UI, as per above screenshots.

3. Approving the AnyConnect System Extension

macOS 11 requires end user or MDM approval before system extensions are allowed to run.

Two approvals are required for the AnyConnect system extension:

- Approve the system extension loading/activation.
- Approve the extension's content filter component activation.

3.1 Extension Approval by End User

The AnyConnect system extension and its content filter component can be approved by end user, by following either the OS prompting, or the more explicit AnyConnect Notification app's instructions.

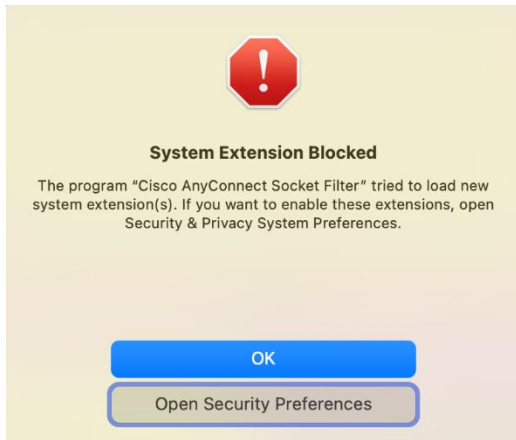


Figure 4 - Extension blocked - OS prompt

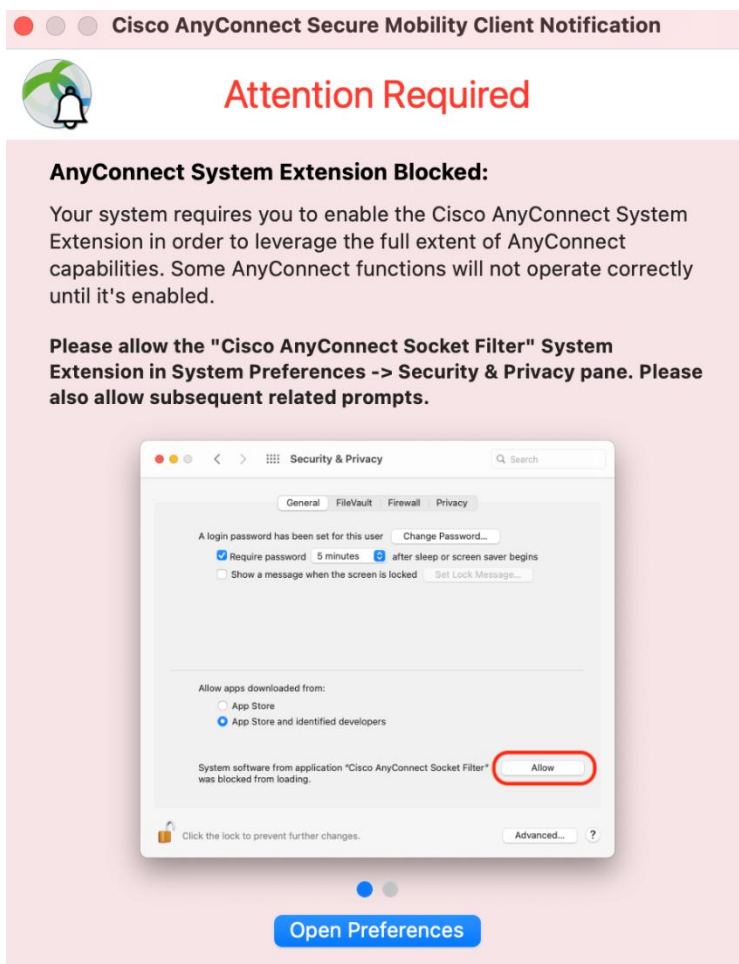


Figure 5 - Extension blocked - AnyConnect prompt

After opening the Security & Privacy Preferences window, click the bottom-left lock and provide the requested credentials, as prompted, to unlock it and allow changes.

The window's appearance depends on whether the AnyConnect extension is the only one requiring approval. If that's the case, simply click the Allow button.

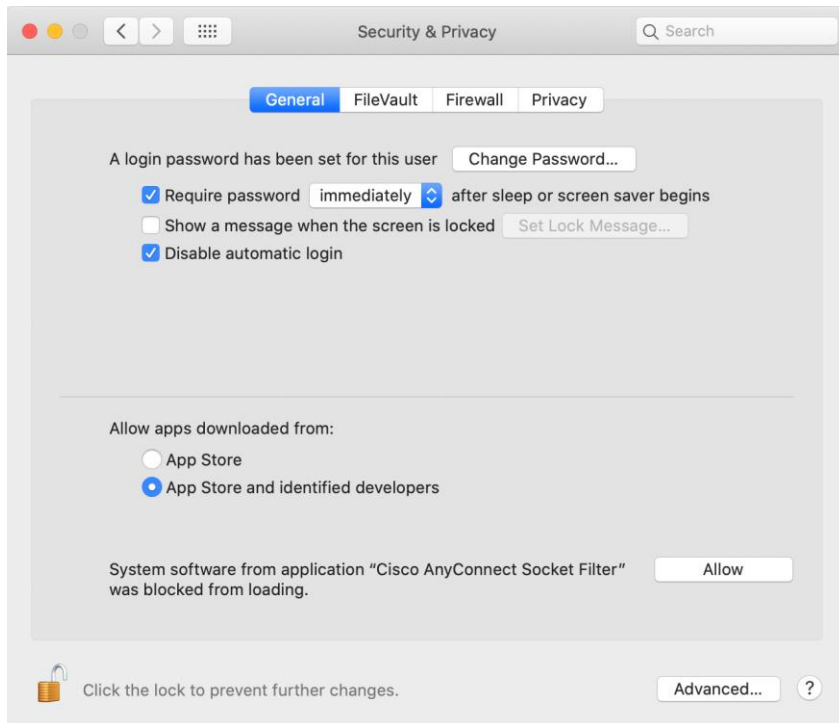


Figure 6 - AnyConnect extension approval

Otherwise click the Details... button, then select the "Cisco AnyConnect Socket Filter" check box and click OK.

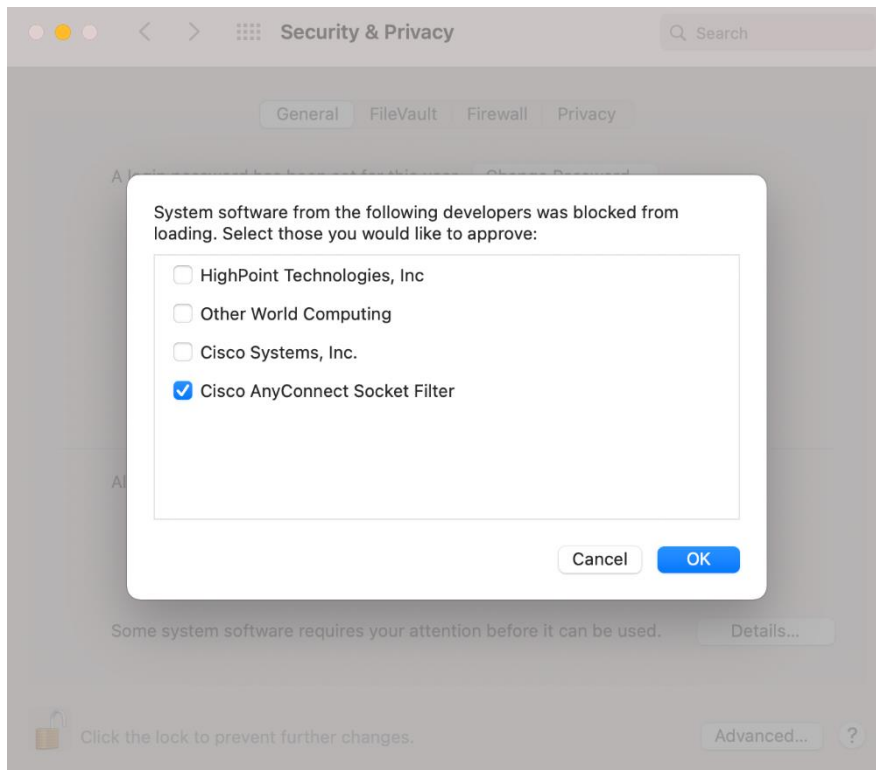


Figure 7 - AnyConnect extension approval (multiple unapproved extensions)

Shortly after approving the AnyConnect extension, the user is shown another popup, this time for approving the extension's content filter component.

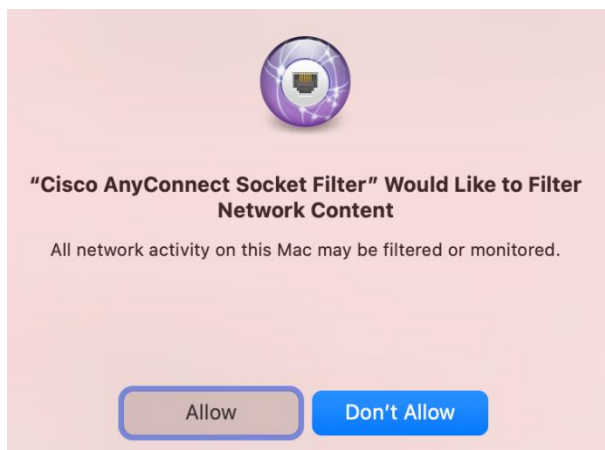


Figure 8 - AnyConnect extension's content filter approval

After the extension's content filter approval is complete, the extension and its components should be active, as confirmed by the AnyConnect Notification app:

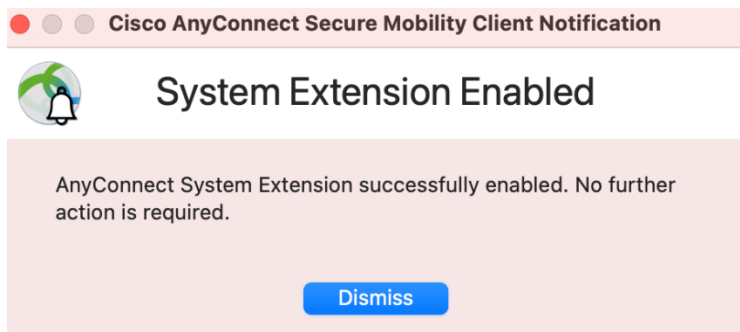


Figure 9 - AnyConnect extension approval confirmation

3.2 Extension Approval using MDM

The AnyConnect system extension can also be approved without end user interaction, using a management profile's [SystemExtensions](#) payload with the following settings:

Property	Value
Team Identifier	DE8Y96K9QP
Bundle Identifier	com.cisco.anyconnect.macos.acsockext
System Extension Type	NetworkExtension

A [WebContentFilter](#) payload with the following settings can be used to approve the extension's content filter component:

Property	Value
AutoFilterEnabled	false
FilterBrowsers	false
FilterSockets	true
FilterPackets	false
FilterGrade	firewall
FilterDataProviderBundleIdentifier	com.cisco.anyconnect.macos.acsockext
FilterDataProviderDesignatedRequirement	<code>anchor apple generic and identifier "com.cisco.anyconnect.macos.acsockext" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or 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] = DE8Y96K9QP)</code>
PluginBundleID	com.cisco.anyconnect.macos.acsock
VendorConfig	
UserDefinedName	Cisco AnyConnect Content Filter

3.3 Confirming AnyConnect Extension Approval

Run the command `systemextensionsctl list` to confirm that the AnyConnect system extension has been approved and activated.


```

% systemextensionsctl list
1 extension(s)
--- com.apple.system_extension.network_extension
enabled active teamID bundleID (version) name [state]
* * DE8Y96K9QP com.cisco.anyconnect.macos.acsocket
(4.9.03038/4.9.03038) Cisco AnyConnect Socket Filter Extension
[activated enabled]

```

Also inspect the System Preferences – Network UI to confirm that all three AnyConnect extension components are active, as per section [About the AnyConnect System Extension](#).

3.4 AnyConnect Extension Deactivation

During AnyConnect uninstallation, the user is prompted for admin credentials in order to approve the system extension deactivation:

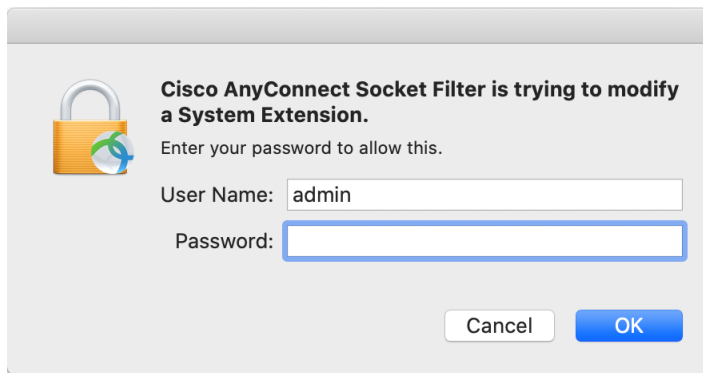


Figure 10 - Extension deactivation prompt

4. Last-resort Workaround: Failover to Kernel Extension

AnyConnect installs its kernel extension on macOS 11, too, as on previous OS versions. However, it is only installed as fallback in case of a critical system extension (or related OS framework) issue.

As a last-resort temporary workaround, Cisco TAC may recommend switching from the system extension to the legacy kernel extension, which offers equivalent functionality.

4.1 Kernel Extension Approval using MDM

Kernel extensions require approval via MDM in order to load on macOS 11, end user approval is no longer an option.

The AnyConnect kernel extension can be approved using a management profile's [SystemPolicyKernelExtensions](#) payload with the following settings:

Property	Value
Team Identifier	DE8Y96K9QP
Bundle Identifier	com.cisco.kext.acsock

4.2 Failover to Kernel Extension

Once the MDM configuration profile detailed in the previous section is installed, run the following command to instruct AnyConnect to deactivate the system extension and start using the kernel extension instead:

(The user should handle the system extension deactivation prompt as per section [AnyConnect Extension Deactivation.](#))

```
% sudo launchctl unload
/Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist &&
/Applications/Cisco/Cisco\ AnyConnect\ Socket\
Filter.app/Contents/MacOS/Cisco\ AnyConnect\ Socket\ Filter -deactivateExt
&& echo kext=1 | sudo tee /opt/cisco/anyconnect/acsock.cfg && sudo
launchctl load /Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist
```

A reboot should be performed if AnyConnect fails to load its kernel extension upon executing the above command, which can be verified by running the following command (should return one entry after successful kernel extension load):

```
% kextstat | grep com.cisco.kext.acsock
```

Once the system extension issue causing the failover to the kernel extension is confirmed resolved by Cisco TAC, run the following command to instruct AnyConnect to switch back to the system extension:

```
% sudo launchctl unload
/Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist && sudo
kextunload -b com.cisco.kext.acsock && sudo rm
/opt/cisco/anyconnect/acsock.cfg && sudo launchctl load
/Library/LaunchDaemons/com.cisco.anyconnect.vpnagentd.plist
```

Then install the AnyConnect or macOS version with the fix.

5. Sample MDM Configuration Profile for AnyConnect System and Kernel Extension Approval

The following MDM configuration profile can be used to allow loading of both AnyConnect system and kernel extensions, including the system extension's content filter component.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>PayloadContent</key>
    <array>
      <dict>
        <key>AllowUserOverrides</key>
        <true/>
        <key>AllowedKernelExtensions</key>
        <dict>
          <key>DE8Y96K9QP</key>
          <array>
            <string>com.cisco.kext.acsock</string>
```

```
        </array>
    </dict>
    <key>PayloadDescription</key>
    <string></string>
    <key>PayloadDisplayName</key>
    <string>AnyConnect Kernel Extension</string>
    <key>PayloadEnabled</key>
    <true/>
    <key>PayloadIdentifier</key>
    <string>37C29CF2-A783-411D-B2C7-100EDDFBE223</string>
    <key>PayloadOrganization</key>
    <string>Cisco Systems, Inc.</string>
    <key>PayloadType</key>
    <string>com.apple.syspolicy.kernel-extension-policy</string>
    <key>PayloadUUID</key>
    <string>37C29CF2-A783-411D-B2C7-100EDDFBE223</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
</dict>
<dict>
    <key>AllowUserOverrides</key>
    <true/>
    <key>AllowedSystemExtensions</key>
    <dict>
        <key>DE8Y96K9QP</key>
        <array>
            <string>com.cisco.anyconnect.macos.acsockext</string>
        </array>
    </dict>
    <key>PayloadDescription</key>
    <string></string>
    <key>PayloadDisplayName</key>
    <string>AnyConnect System Extension</string>
    <key>PayloadEnabled</key>
    <true/>
    <key>PayloadIdentifier</key>
    <string>A8364220-5D8D-40A9-Af66-1Fbfef94E116</string>
    <key>PayloadOrganization</key>
    <string>Cisco Systems, Inc.</string>
    <key>PayloadType</key>
    <string>com.apple.system-extension-policy</string>
    <key>PayloadUUID</key>
    <string>A8364220-5D8D-40A9-Af66-1Fbfef94E116</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
</dict>
<dict>
    <key>Enabled</key>
    <true/>
    <key>AutoFilterEnabled</key>
    <false/>
    <key>FilterBrowsers</key>
    <false/>
    <key>FilterSockets</key>
    <true/>
    <key>FilterPackets</key>
    <false/>

```

```
<key>FilterType</key>
<string>Plugin</string>
<key>FilterGrade</key>
<string>firewall</string>
<key>PayloadDescription</key>
<string></string>
<key>PayloadDisplayName</key>
<string>Cisco AnyConnect Content Filter</string>
<key>PayloadIdentifier</key>
<string>com.apple.webcontent-filter.339Ec532-9Ada-480A-Bf3D-
A535F0F0B665</string>
<key>PayloadType</key>
<string>com.apple.webcontent-filter</string>
<key>PayloadUUID</key>
<string>339Ec532-9Ada-480A-Bf3D-A535F0F0B665</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>FilterDataProviderBundleIdentifier</key>
<string>com.cisco.anyconnect.macos.acsockext</string>
<key>FilterDataProviderDesignatedRequirement</key>
<string>anchor apple generic and identifier
"com.cisco.anyconnect.macos.acsockext" and (certificate
leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or 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] = DE8Y96K9QP)</string>
<key>PluginBundleID</key>
<string>com.cisco.anyconnect.macos.acsock</string>
<key>UserDefinedName</key>
<string>Cisco AnyConnect Content Filter</string>
</dict>
</array>
<key>PayloadDescription</key>
<string></string>
<key>PayloadDisplayName</key>
<string>Approved AnyConnect System and Kernel Extensions</string>
<key>PayloadEnabled</key>
<true/>
<key>PayloadIdentifier</key>
<string>A401Bdc2-4Ab1-4406-A143-11F077Baf52B</string>
<key>PayloadOrganization</key>
<string>Cisco Systems, Inc.</string>
<key>PayloadRemovalDisallowed</key>
<true/>
<key>PayloadScope</key>
<string>System</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>A401Bdc2-4Ab1-4406-A143-11F077Baf52B</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```