



Appendix: AnyConnect Changes Related to macOS 11 (And Later)

You must be running AnyConnect 4.9.04xxx (or later) for macOS 11. It leverages the System Extension framework available in macOS, while it formerly used the now-deprecated Kernel Extension framework. Because of this change, administrators must approve the AnyConnect system extension and can confirm correct operation with these updates. Also, if a critical system extension (or related OS framework) issue is encountered, you can follow the steps for failing over to the AnyConnect kernel extension, as a last resort workaround, but it is installed solely for this purpose and is no longer used by default

- [About the AnyConnect System Extension, on page 1](#)
- [Approving the AnyConnect System Extension, on page 2](#)
- [Deactivate the AnyConnect System Extension, on page 3](#)
- [Failover to Kernel Extension, on page 4](#)
- [Sample MDM Configuration Profile for AnyConnect System and Kernel Extension Approval , on page 5](#)

About the AnyConnect System Extension

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

The AnyConnect extension has the following three components that are visible in the macOS System Preferences-Network UI window:

- DNS proxy
- App/transparent proxy
- Content filter

AnyConnect requires its system extension and all its components to be active for proper operation, which implies that the mentioned components are all present and show as green (running) in the left pane of the macOS Network UI.

Approving the AnyConnect System Extension

The AnyConnect system extension activation requires either approval by an end user with administrator rights or MDM approval:

- [Approve the System Extension Loading/Activation, on page 2](#)
- [Approve the System Extension Using MDM, on page 2](#)

Approve the System Extension Loading/Activation

Approve the AnyConnect system extension and its content filter component by following the OS prompts or the more explicit AnyConnect - Notification application's instructions.

Procedure

-
- Step 1** Click the **Open Preferences** button in the AnyConnect - Notification app, or the **Open Security Preferences** button, when you receive the "System Extension Blocked" message from macOS. You can also navigate to the System Preferences application and go to the Security&Privacy window.
- Step 2** Click the bottom-left lock and provide the requested credentials to unlock and allow changes.
- Step 3** Click **Allow** on the Security & Privacy window to accept the AnyConnect - Socket Filter extension.
-

When multiple system extensions require approval, the button is labeled Details... . In this case, click **Details...**, choose the **AnyConnect - Socket Filter** checkbox, click **OK**, and approve any subsequent prompts that require an Allow.

What to do next

You will receive a prompt to approve the extension's content filter component and a notification when it is.

Approve the System Extension Using MDM

Approve the AnyConnect system extension 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

Approve the extension's content filter component with the following WebContentFilter payload settings:

Property	Value
AutoFilterEnabled	false
FilterBrowsers	false
FilterSockets	true
FilterPackets	false
FilterGrade	firewall
FilterDataProviderBundleIdentifier	com.cisco.anyconnect.macos.acsockext
FilterDataProviderDesignatedRequirement	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)
PluginBundleID	com.cisco.anyconnect.macos.acsock
VendorConfig	
UserDefinedName	Cisco AnyConnect Content Filter

Confirm Activation of AnyConnect System Extension

To confirm that the AnyConnect system extension has been approved and activated, run the `systemextensionsctl list` command:

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

You can also check the System Preferences network UI to confirm that all three AnyConnect extension components are active.

Deactivate the AnyConnect System Extension

During AnyConnect uninstallation, the user is prompted for administrator credentials to approve the system extension deactivation. On macOS 12 and later, the AnyConnect system extension can be silently removed after deploying a management profile with the `RemovableSystemExtensions` property added to the `SystemExtensions` payload. This property must contain the bundle identifier of the AnyConnect system extension (`com.cisco.anyconnect.macos.acsockext`).



Note You should only use this management profile configuration when the administrator wants to automate the AnyConnect uninstallation, as it grants any user or process with root privileges the ability to remove the AnyConnect system extension, without prompting the user for a password.

Failover to Kernel Extension

AnyConnect still installs its kernel extension on macOS 11 (and later versions); however, you should use it only as a fallback in the event of a critical system extension (or related OS framework) issue or with instruction by Cisco Technical Assistance Center (TAC). Kernel extensions require approval via MDM before loading on macOS 11 (and later). End user approval is no longer an option.

Before you begin

Use these steps only as a last-resort workaround.

Procedure

Step 1 Approve the AnyConnect kernel extension using a management profile's *SystemPolicyKernelExtensions* payload with the following settings:

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

The MDM configuration profile is installed.

Step 2 Run the following command that causes AnyConnect to deactivate the system extensions and start using the kernel extension instead. You will be prompted for administrator credentials.

- If running version 4.10, enter **% 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**

Step 3 Run the following command to verify that the kernel extension was loaded: **% kextstat | grep com.cisco.kext.acsock**

If AnyConnect failed to load its kernel extension, perform a reboot.

Revert Back to System Extension

If Cisco TAC confirms a fix to the system extension issue (and eliminates the needs for the failover to kernel extension), run the following command, which instructs AnyConnect to switch back to the system extension. The command depends on the version of AnyConnect you are running.

If running a 4.10 version, run this:

```
% 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

% osascript -e 'quit app "Cisco Secure Client - AnyConnect VPN Service.app"' && open -W -a
"/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app" --args
uninstall && sudo /opt/cisco/secureclient/kdf/bin/acsocktool -kfr && open -a
"/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app"% sudo launchctl
unload /Library/LaunchDaemons/com.cisco.secureclient.vpnagentd.plist && sudo
/opt/cisco/secureclient/kdf/bin/acsocktool -kfr && sudo launchctl load
/Library/LaunchDaemons/com.cisco.secureclient.vpnagentd.plist
```

Sample MDM Configuration Profile for AnyConnect System and Kernel Extension Approval

Use the following MDM configuration profile to load both the AnyConnect system and the 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>

      </dict>

    </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>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>
```

