Appendix: Cisco Secure Client Changes Related to macOS 11 (And Later)

On macOS 11 and later, Cisco Secure Client leverages the macOS System Extension framework, while it formerly used the now-deprecated Kernel Extension Framework. An administrator must approve the Cisco Secure Client system extension as described in the sections below. Also, if a critical system extension (or related OS framework) issue is encountered, you can follow the steps for failing over to the Cisco Secure Client kernel extension, as a last resort workaround, but it is installed solely for this purpose and is no longer used by default.

- About the Cisco Secure Client System Extension, on page 1
- Approving the Cisco Secure Client System Extension, on page 2
- Managed Login Items, on page 3
- Deactivate the Cisco Secure Client System Extension, on page 4
- Failover to Kernel Extension, on page 4
- Sample MDM Configuration Profile for Cisco Secure Client System and Kernel Extension Approval , on page 5

About the Cisco Secure Client System Extension

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

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

- DNS proxy
- App/transparent proxy
- Content filter

Cisco Secure Client 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.

If a third-party product is employing a system extension with DNS proxy capabilities, either Cisco Secure Client or the third-party product (or both), may not function properly. macOS only supports one active DNS proxy extension at a time.

Approving the Cisco Secure Client System Extension

The Cisco Secure Client 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 Cisco Secure Client system extension and its content filter component by following the OS prompts or the more explicit Cisco Secure Client - Notification application's instructions.

Procedure

Step 1 When you receive the "System Extension Blocked" message from macOS, perform this operation:

- For macOS 15 (and later), click the **Open System Settings** button in the Cisco Secure Client - Notification app and then choose **Network Extensions** in System Settings > General > Login Items & Extensions section.
- For macOS 13 and 14, click the **Open Preferences** button in the Cisco Secure Client - Notification app, or the **Open Security Preferences** button. 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.

Step 3 For macOS 15, click to allow the Cisco Secure Client Socket Filter. For macOS 13 or 14, click **Allow** on the Security & Privacy window to accept the Cisco Secure Client - Socket Filter extension.

You will receive a "System Extension Enabled" message.

Approve the System Extension Using MDM

Approve the Cisco Secure Client 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 Cisco Secure Client System Extension

To confirm that the Cisco Secure Client 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
(5.0.00xxx/5.0..00xxx) Cisco Secure Client - Socket Filter Extension
[activated enabled]
```

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

Managed Login Items

For macOS 13 (and later) and Secure Client 5.1, the VPN and ZTA module requires user approval before they can function. To perform approval without user intervention, or prevent users from disabling the Login Items owned by the Secure Client, you must push an MDM profile with these attributes for Managed Login Items:

- Bundle Identifier Prefix: com.cisco.secureclient
- Team Identifier: DE8Y96K9QP

Refer to Web Deploy Upgrade on macOS 13 (or Later) Requires Admin Privileges or Apple Platform Deployment documentation for additional information.

Deactivate the Cisco Secure Client System Extension

During Cisco Secure Client uninstallation, the user is prompted for administrator credentials to approve the system extension deactivation. On macOS 12 and later, the Cisco Secure Client 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 Cisco Secure Client system extension (com.cisco.anyconnect.macos.acsockext).

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

Failover to Kernel Extension

Cisco Secure Client 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, and only if instructed by Cisco Technical Assistance Center (TAC), as kernel extenstions have been deprecated by Apple in macOS 10.15. 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 Cisco Secure Client 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 Cisco Secure Client to deactivate the system extensions and start using the kernel extension instead. You will be prompted for administrator credentials.

% sudo /opt/cisco/secureclient/kdf/bin/acsocktool -kf

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

If Cisco Secure Client 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 Cisco Secure Client to switch back to the system extension. The command depends on the version of Cisco Secure Client you are running.

If Cisco TAC confirms a fix to the system extension issue, install the recommended Cisco Secure Client or macOS version with the fix.

After applying the suggested fix (thus eliminating the need for the failover to the kernel extension), run the following command, which instructs Cisco Secure Client to switch back to the system extension:

```
sudo /opt/cisco/secureclient/kdf/bin/acsocktool -kfr
```

Sample MDM Configuration Profile for Cisco Secure Client System and Kernel Extension Approval

Use the following MDM configuration profile to load both the Cisco Secure Client 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>
            <key>PayloadDescription</key>
            <string></string>
            <key>PayloadDisplayName</key>
            <string>Cisco
Secure Client 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>Cisco
Secure Client 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
        Secure Client 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 Cisco
        Secure Client 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>
```