附录：与 macOS 11（及更高版本）相关的 Cisco Secure Client 更改

在 macOS 11 及更高版本上，Cisco Secure Client 利用 macOS 系统扩展框架，而以前使用的是现已过时的内核扩展框架。管理员必须批准 Cisco Secure Client 系统扩展，如以下部分所述。此外，如果遇到严重的系统扩展（或相关的操作系统框架）问题，作为最后的变通方法，您可以按照故障转移至 Cisco Secure Client 内核扩展的步骤进行操作，但这仅出于此目的而安装且不会再默认使用。

关于 Cisco Secure Client 系统扩展

Cisco Secure Client 在 macOS 11（及更高版本）上使用网络系统扩展，捆绑在名为 Cisco Secure Client - Socket Filter 的应用程序中。该应用程序会控制扩展的激活和停用，并安装在 /Applications/Cisco 下。

Cisco Secure Client 扩展包含以下三个组件，可在 macOS 系统首选项 - 网络用户界面窗口中显示：

- DNS 代理
- 应用程序/透明代理
- 内容过滤器

Cisco Secure Client 要求其系统扩展及其所有组件就能处于活动状态方可正常运行，这意味着上述组件全部安装到位，并在 macOS 网络用户界面的左窗格中显示为绿色（正在运行）。

批准 Cisco Secure Client 系统扩展

Cisco Secure Client 系统扩展激活需要由具有管理员权限的最终用户批准或 MDM 批准：

批准系统扩展加载/激活

按照操作系统提示或更明确的 Cisco Secure Client 通知应用程序的说明，批准 Cisco Secure Client 系统扩展及其内容过滤器组件。

步骤 1 当您从 macOS 收到“系统扩展已阻止”(System Extension Blocked) 消息时，点击 Cisco Secure Client - 通知应用程序中的**打开首选项 (Open Preferences)** 按钮或**打开安全首选项 (Open Security Preferences)** 按钮。您还可以导航到“系统首选项”(System Preferences) 应用程序并转到“安全和隐私”(Security&Privacy) 窗口。

步骤 2 点击左下角的锁，然后提供请求的凭证以解锁并允许更改。

步骤 3 点击安全和隐私窗口中的**允许 (Allow)**，接受思科 Cisco Secure Client - 套接字过滤器扩展。

当多个系统扩展需要审批时，按钮标记为“详细信息...”(Details...)。。在这种情况下，点击**详细信息...(Details...)**，选中**Cisco Secure Client - 套接字过滤器 (Cisco AnyConnect Socket Filter)** 复选框，点击**确定 (OK)**，然后批准需要“允许”(Allow) 的任何后续提示。

下一步做什么

您将收到批准扩展内容过滤器组件的提示，并在批准后收到通知。

使用 MDM 批准系统扩展

使用管理配置文件具有以下设置的 SystemExtensions 负载来批准 Cisco Secure Client 系统扩展而无需最终用户交互：

特性	值
团队标识符	DE8Y96K9QP
捆绑包标识符	com.cisco.anyconnect.macos.acsockext
系统扩展类型	NetworkExtension

使用以下 WebContentFilter 负载设置来批准扩展的内容过滤器组件：

特性	值
AutoFilterEnabled	false
FilterBrowsers	false
FilterSockets	true

特性	值
FilterPackets	false
FilterGrade	防火墙
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	思科 AnyConnect 内容过滤器

确认激活 Cisco Secure Client 系统扩展

要确认 Cisco Secure Client 系统扩展是否已获批准并激活，请运行 **systemextensionsctl list** 命令：

```
% 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]
```

您还可以检查系统首选项网络 UI 以确认所有三个 Cisco Secure Client 扩展组件是否均已激活。

停用 Cisco Secure Client 系统扩展

在 Cisco Secure Client 卸载期间，系统会提示用户输入管理员凭证，以便批准停用系统扩展。在 macOS 12 及更高版本上，在部署将 RemovableSystemExtensions 属性添加到 SystemExtensions 负载的管理配置文件后，可以以静默方式删除 Cisco Secure Client 系统扩展。此属性必须包含 Cisco Secure Client 系统扩展的捆绑包标识符 (com.cisco.anyconnect.macos.acsockext)。

注释 仅当管理员希望自动执行 Cisco Secure Client 卸载时，才应使用此管理配置文件配置，因为它授予任何具有 root 权限的用户或进程删除 Cisco Secure Client 系统扩展的能力，而不会提示用户输入密码。

故障转移到内核扩展

Cisco Secure Client 仍在 macOS 11（及更高版本）上安装其内核扩展；但是，只有在出现关键系统扩展（或相关操作系统框架）问题时，才可将其作为备用方案使用，而且只能在思科技术支持中心 (TAC) 的指导下使用，因为 Apple 已在 macOS 10.15 中弃用了内核扩展。在 macOS 11（及更高版本）上加载之前，内核扩展需要通过 MDM 审批。最终用户审批不再可供选择。

开始之前

仅将这些步骤用作最后的解决方法。

步骤 1 使用管理配置文件的 *SystemPolicyKernelExtensions* 负载通过以下设置来批准 Cisco Secure Client 内核扩展：

特性	值
团队标识符	DE8Y96K9QP
捆绑包标识符	com.cisco.kext.acsock

MDM 配置文件将进行安装。

步骤 2 运行以下会导致 Cisco Secure Client 停用系统扩展并开始使用内核扩展的命令。系统将提示您输入管理员凭证。

- 在 macOS 13 及更高版本上：

  % 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 -kf && open -a "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app"

- 在 macOS 12 及更早版本上：

  % sudo launchctl unload /Library/LaunchDaemons/com.cisco.secureclient.vpnagentd.plist && sudo /opt/cisco/secureclient/kdf/bin/acsocktool -kf && sudo launchctl load /Library/LaunchDaemons/com.cisco.secureclient.vpnagentd.plist

步骤 3 运行以下命令以验证是否已加载内核扩展：**% kextstat | grep com.cisco.kext.acsock**

如果 Cisco Secure Client 无法加载其内核扩展，请执行重新引导。

恢复到系统扩展

如果思科 TAC 确认修复了系统扩展问题（并消除了故障转移到内核扩展的需求），则可运行以下命令，指示 Cisco Secure Client 切换回系统扩展：命令取决于您所运行的 Cisco Secure Client 版本。

如果思科 TAC 确认修复了系统扩展问题，请安装建议的 Cisco Secure Client 或 macOS 版本的修复程序。

应用建议的修复后（从而消除故障转移到内核扩展的需要），运行以下命令，指示Cisco Secure Client切换回系统扩展。命令取决于您所运行的 macOS 版本。

在 macOS 13 及更高版本上：

```
% 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"
```

在 macOS 12 及更早版本上：

```
% 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
```

Cisco Secure Client 系统和内核扩展批准的示例 MDM 配置文件

使用以下 MDM 配置文件来加载 Cisco Secure Client 系统和内核扩展，包括系统扩展的内容过滤器组件。

```
<?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>
```

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。