

Disable the VPN Module in Secure Client

Contents

[Introduction](#)

[Requirement for VPN Module in Secure Client](#)

[Methods to Disable VPN Functionality](#)

[Disable VPN Module During Installation](#)

[Windows](#)

[macOS](#)

[Disable VPN Module Post Installation](#)

[Verification](#)

Introduction

This document describes how to disable the VPN module in Secure Client while ensuring DNS traffic interception continues to function.

Requirement for VPN Module in Secure Client

The VPN module is a required component of Secure Client, even if AnyConnect is not used for VPN access. Umbrella relies on shared Secure Client drivers to intercept and manage DNS traffic. Although installation of the VPN module is mandatory, you can fully disable VPN functionality.

Methods to Disable VPN Functionality

You can disable the VPN functionality in Secure Client by disabling it:

- During installation using install arguments (Windows) or modifying the installation package (OSX).
- After installation by deploying a configuration profile to the endpoint (which can be deployed programmatically).

Disable VPN Module During Installation

Windows

1. During installation, use the PRE_DEPLOY_DISABLE_VPN=1 MSI argument to disable VPN functionality.
2. For details, review [Customize Windows Installations of Cisco Secure Client](#).

macOS

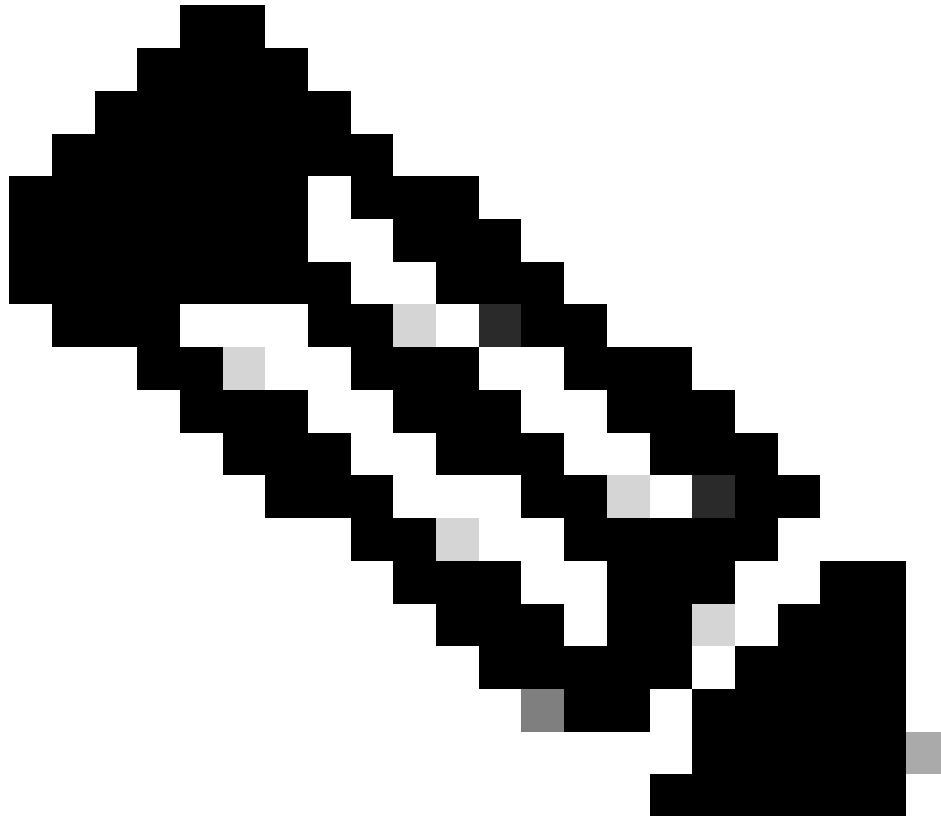
1. Customize the installation package (.DMG) with an ACTransforms.xml file which controls the enablement of the VPN functionality.
2. For more information, see [Customize MacOS installations of Cisco Secure Client](#).

Disable VPN Module Post Installation

1. Navigate to the profile directory on the endpoint:

- Windows:

C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile\



Note: The ProgramData folder is hidden by default in Windows. Type the path directly into Windows Explorer if needed.

-
- macOS:

/opt/cisco/secureclient/vpn/profile/

2. Create a new blank text document.

3. Copy the provided XML content into the document and save it as VPNDisable_ServiceProfile.xml in the **Profile** folder:

```
<?xml version="1.0" encoding="utf-8"?>
```

<!--

Cisco AnyConnect VPN Profile -

This profile is a sample intended to allow for the disabling of VPN service for those installations that do not require VPN support.

-->

```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/
```

```
<ClientInitialization>
```

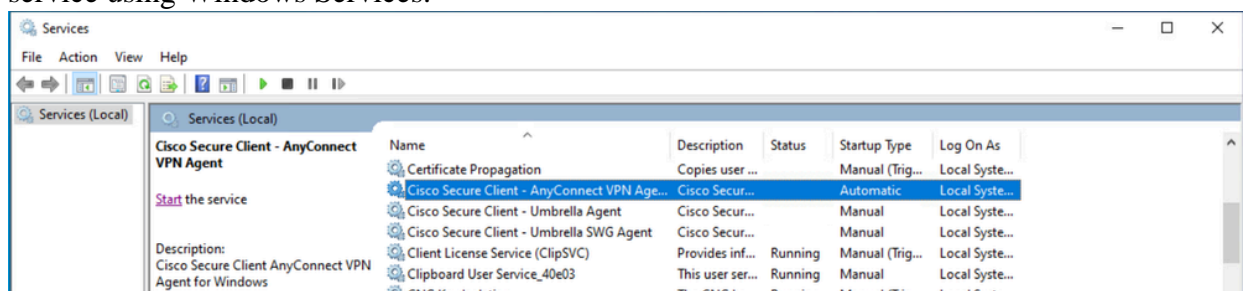
```
<ServiceDisable>true</ServiceDisable>
```

```
</ClientInitialization>
```

```
</AnyConnectProfile>
```

4. After saving the **VPNDisable_ServiceProfile.xml** file in the profile folder, restart the computer.

- On Windows, you can alternatively restart the **Cisco Secure Client – AnyConnect VPN Agent** service using Windows Services.



18212956792980

Verification

After restarting, launch the Secure Client graphical user interface (GUI) to verify that the VPN module is disabled.



18212229472020