User Guide

# AWS Client VPN

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS Client VPN: User Guide

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

# Table of Contents

**What is AWS Client VPN? ..... 1**
Components ..... 1
Additional resources ..... 1
**Getting started ..... 2**
Prerequisites ..... 2
Step 1: Get a VPN client application ..... 2
Step 2: Get the Client VPN endpoint configuration file ..... 3
Step 3: Connect to the VPN ..... 3
Self-service portal ..... 3
**Connect using an AWS provided client ..... 5**
Windows ..... 6
Requirements ..... 7
Connecting ..... 7
Release notes ..... 9
macOS ..... 15
Requirements ..... 16
Connecting ..... 16
Release notes ..... 17
Linux ..... 24
Requirements ..... 24
Installation ..... 24
Connecting ..... 26
Release notes ..... 28
**Connect using an OpenVPN client ..... 32**
Windows ..... 32
OpenVPN using a certificate from the Windows Certificate System Store ..... 32
OpenVPN GUI ..... 33
OpenVPN Connect Client ..... 35
Android and iOS ..... 35
macOS ..... 36
Tunnelblick ..... 36
OpenVPN Connect Client ..... 37
Linux ..... 38
OpenVPN - Network Manager ..... 38

OpenVPN ... 39
**Troubleshooting ... 40**
Client VPN endpoint troubleshooting for administrators ... 40
Send diagnostic logs to AWS Support in the AWS provided client ... 40
Sending diagnostic logs ... 16
Windows troubleshooting ... 41
AWS provided client ... 42
OpenVPN GUI ... 48
OpenVPN connect client ... 48
macOS troubleshooting ... 49
AWS provided client ... 50
Tunnelblick ... 52
OpenVPN ... 55
Linux troubleshooting ... 56
AWS provided client ... 42
OpenVPN (command line) ... 57
OpenVPN through Network Manager (GUI) ... 59
Common problems ... 59
TLS key negotiation failed ... 59
**Document history ... 61**

# What is AWS Client VPN?

AWS Client VPN is a managed client-based VPN service that enables you to securely access AWS resources and resources in your on-premises network.

This guide provides steps for establishing a VPN connection to a Client VPN endpoint using a client application on your device.

## Components

The following are the key components for using AWS Client VPN.

- **Client VPN endpoint** — Your Client VPN administrator creates and configures a Client VPN endpoint in AWS. Your administrator controls which networks and resources you can access when you establish a VPN connection.
- **VPN client application** — The software application that you use to connect to the Client VPN endpoint and establish a secure VPN connection.
- **Client VPN endpoint configuration file** — A configuration file that's provided to you by your Client VPN administrator. The file includes information about the Client VPN endpoint and the certificates required to establish a VPN connection. You load this file into your chosen VPN client application.

## Additional resources

If you're a Client VPN administrator, see the AWS Client VPN Administrator Guide for more information about creating and configuring a Client VPN endpoint.

# Getting started with Client VPN

Before you can establish a VPN session, your Client VPN administrator must create and configure a Client VPN endpoint. Your administrator controls which networks and resources you can access when you establish a VPN session. You then use a VPN client application to connect to a Client VPN endpoint and establish a secure VPN connection.

If you're an administrator who needs to create a Client VPN endpoint, see the AWS Client VPN Administrator Guide.

**Topics**


- Prerequisites
- Step 1: Get a VPN client application
- Step 2: Get the Client VPN endpoint configuration file
- Step 3: Connect to the VPN
- Use the self-service portal


## Prerequisites

To establish a VPN connection, you must have the following:

- Access to the internet
- A supported device
- For Client VPN endpoints that use SAML-based federated authentication (single sign-on), one of the following browsers:
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

## Step 1: Get a VPN client application

You can connect to a Client VPN endpoint and establish a VPN connection using the AWS provided client or another OpenVPN-based client application.

The AWS provided client is a supported on Windows, macOS, Ubuntu 18.04 LTS, and Ubuntu 20.04 LTS. You can download the client at AWS Client VPN download.

Alternatively, download and install an OpenVPN client application on the device from which you intend to establish the VPN connection.

## Step 2: Get the Client VPN endpoint configuration file

You must get the Client VPN endpoint configuration file from your administrator. The configuration file includes the information about the Client VPN endpoint and the certificates that are required to establish a VPN connection.

Alternatively, if your Client VPN administrator has configured a self-service portal for the Client VPN endpoint, you can download the latest version of the AWS provided client and the latest version of the Client VPN endpoint configuration file yourself. For more information, see Use the self-service portal.

## Step 3: Connect to the VPN

Import the Client VPN endpoint configuration file to the AWS provided client or to your OpenVPN client application and connect to the VPN. For steps to connect to a VPN, see the following topics:

- Connect using an AWS provided client
- Connect using an OpenVPN client

For Client VPN endpoints that use Active Directory authentication, you will be prompted to enter your user name and password. If multi-factor authentication (MFA) has been enabled for the directory, you will also be prompted to enter your MFA code.

For Client VPN endpoints that use SAML-based federated authentication (single sign-on), the AWS provided client opens a browser window on your computer. You'll be prompted to enter your corporate credentials before you can connect to the Client VPN endpoint.

## Use the self-service portal

Your Client VPN endpoint administrator can configure a self-service portal for the Client VPN endpoint. The self-service portal is a web page that enables you to download the latest version of

the AWS provided client and the latest version of the Client VPN endpoint configuration file. For more information about configuring the self-service portal, see Client VPN endpoints in the *AWS Client VPN Administrator Guide*.

Before you begin, you must have the ID of the Client VPN endpoint. Your Client VPN endpoint administrator can provide you with the ID, or can give you a self-service portal URL that includes the ID.

**To access the self-service portal**

1. Go to the self-service portal at https://self-service.clientvpn.amazonaws.com/, or use the URL that was provided to you by your administrator.
2. If required, enter the ID of the Client VPN endpoint, for example, `cvpn-endpoint-0123456abcd123456`. Choose **Next**.
3. Enter your user name and password and choose **Sign In**. This is the same user name and password that you use to connect to the Client VPN endpoint.
4. In the self-service portal, you can do the following:
   - Download the latest version of the client configuration file for the Client VPN endpoint.
   - Download the latest version of the AWS provided client for your platform.

# Connect using an AWS provided client

You can connect to a Client VPN endpoint using the AWS provided client. The AWS provided client is supported on Windows, macOS, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

**Clients**

- AWS Client VPN for Windows
- AWS Client VPN for macOS
- AWS Client VPN for Linux

**OpenVPN directives**

The AWS provided client supports the following OpenVPN directives:

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- ca
- cert
- cipher
- client
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- dhcp-option
- ifconfig-ipv6
- inactive
- keepalive

- key
- nobind
- persist-key
- persist-tun
- ping
- ping-restart
- proto
- pull
- pull-filter
- rcvbuf
- remote
- remote-cert-tls
- remote-random-hostname
- reneg-sec
- resolv-retry
- route
- route-ipv6
- server-poll-timeout
- static-challenge
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

# AWS Client VPN for Windows

The following procedure shows how to establish a VPN connection using the AWS provided client for Windows. You can download and install the client at AWS Client VPN download. The AWS provided client does not support automatic updates.

**Contents**


- Requirements
- Connecting
- Release notes


## Requirements

To use the AWS provided client for Windows, the following are required:

- Windows 10 64-bit operating system, x64 processor
- .NET Framework 4.7.2 or higher

The client reserves TCP port 8096 on your computer. For Client VPN endpoints that use SAML-based federated authentication (single sign-on), the client reserves TCP port 35001.

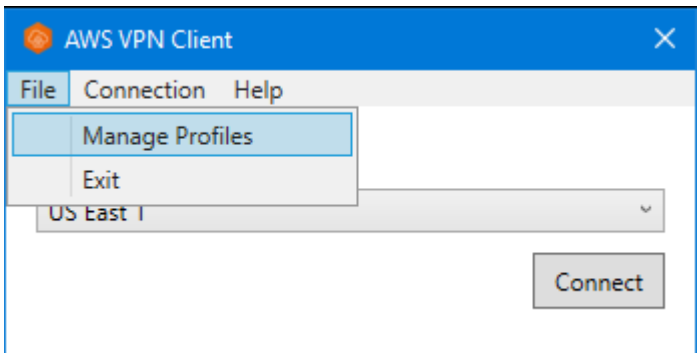
Before you begin, ensure that your Client VPN administrator has created a Client VPN endpoint and provided you with the Client VPN endpoint configuration file.

## Connecting

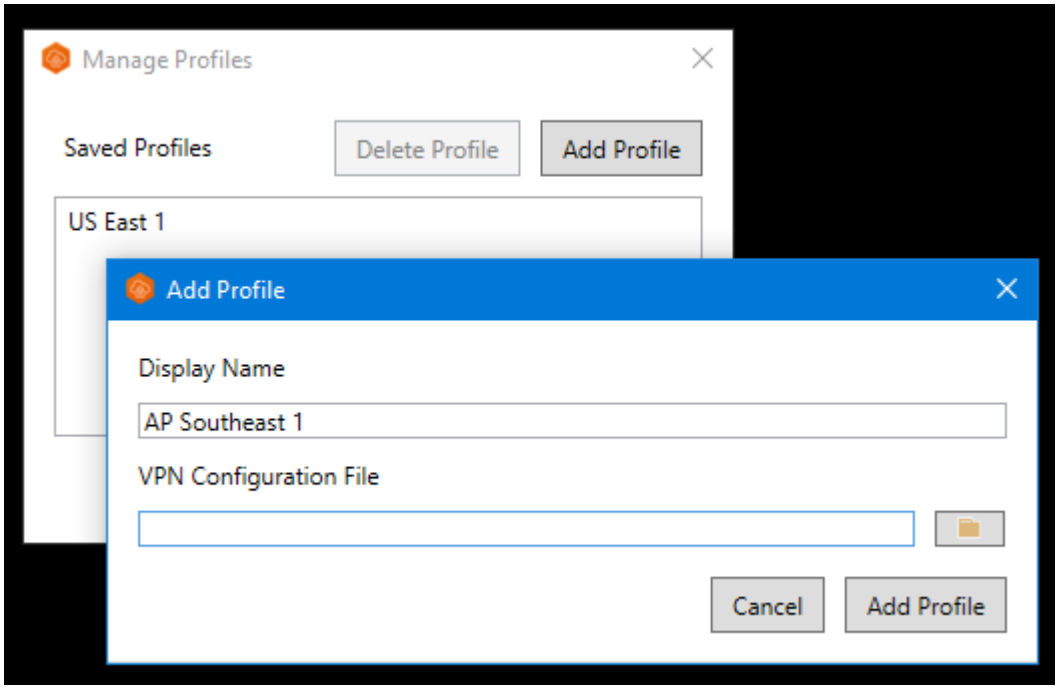
Before you begin, ensure that you've read the requirements. The AWS provided client is also referred to as *AWS VPN Client* in the following steps.

**To connect using the AWS provided client for Windows**

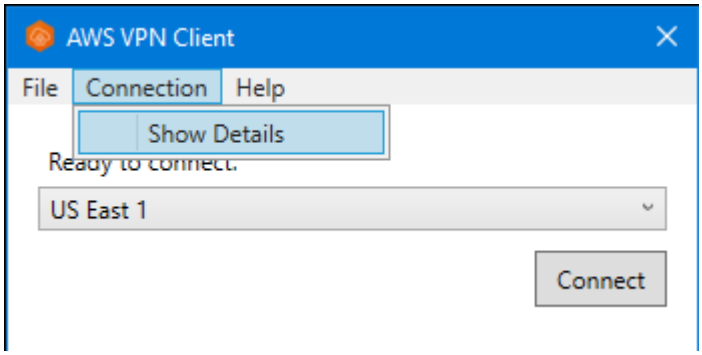
1. Open the **AWS VPN Client** app.
2. Choose **File**, **Manage Profiles**.



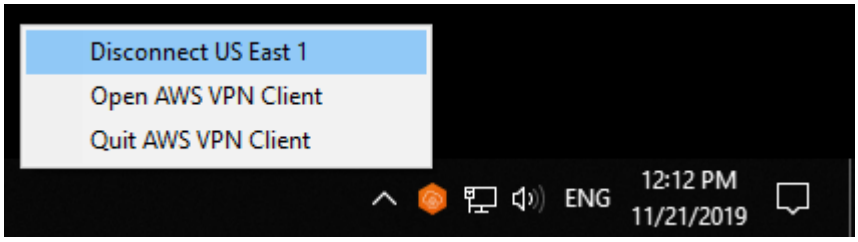

3. Choose **Add Profile**.




4. For **Display Name**, enter a name for the profile.
5. For **VPN Configuration File**, browse to and then select the configuration file that you received from your Client VPN administrator, and choose **Add Profile**.
6. In the **AWS VPN Client** window, ensure that your profile is selected, and then choose **Connect**. If the Client VPN endpoint has been configured to use credential-based authentication, you'll be prompted to enter a user name and password.
7. To view statistics for your connection, choose **Connection**, **Show Details**.




8. To disconnect, in the **AWS VPN Client** window, choose **Disconnect**. Alternatively, choose the client icon on the Windows taskbar, and then choose **Disconnect**.




## Release notes

The following table contains the release notes and download links for the current and previous versions of AWS Client VPN for Windows.

> **Note**
>
> We continue to provide usability and security fixes with every release. We strongly recommend that you use the latest version for every platform. Previous versions may be affected by usability and/or security issues, see release notes for details.

| Version | Changes | Date | Download link and SHA256 |
|---|---|---|---|
| 3.11.2 | • Resolved a SAML authentication issue with Chromium-based browsers since version 123. | April 11, 2024 | Download version 3.11.2<br><br>sha256: 8ba258dd1 5bea3e861 adad108f8 a6d6d4bcd 8fe42cb9e f8bbc294e 72f365c7cc |
| 3.11.1 | • Fixed a buffer overflow action that could potentially allow a local actor to execute arbitrary commands with elevated permissions. | February 16, 2024 | Download version 3.11.1 |

| Version | Changes | Date | Download link and SHA256 |
| --- | --- | --- | --- |
| | • Improved security posture. | | sha256: fb67b60aa 837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0 |
| 3.11.0 | • Fixed a connectivity issue caused by Windows VMs.<br>• Fixed connectivity issues for some LAN configurations.<br>• Improved accessibility. | December 6, 2023 | Download version 3.11.0<br><br>sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9 |
| 3.10.0 | • Fixed a connectivity issue when NAT64 is enabled in the client network.<br>• Fixed a connectivity issue when Hyper-V network adapters are installed on the client machine.<br>• Minor bug fixes and enhancements. | August 24, 2023 | Download version 3.10.0<br><br>sha256: d46721aad 40ccb816f 163e406c3 66ff03b11 20abbb43a 20607e06d 3b1fa8667f |

| Version | Changes | Date | Download link and SHA256 |
| --- | --- | --- | --- |
| 3.9.0 | • Improved security posture. | August 3, 2023 | Download version 3.9.0<br><br>sha256: de9a3800e a23491555 40bd32bba e472404c6 36d8d8267 a0e1fb217 3a8aae21ed |
| 3.8.0 | • Improved security posture. | July 15, 2023 | No longer supported |
| 3.7.0 | • Rolled back changes from 3.6.0. | July 15, 2023 | No longer supported |
| 3.6.0 | • Improved security posture. | July 14, 2023 | No longer supported |
| 3.5.0 | Minor bug fixes and enhancements. | April 3, 2023 | No longer supported |
| 3.4.0 | Rolled back the changes from version 3.3.0. | March 28, 2023 | No longer supported |
| 3.3.0 | Minor bug fixes and enhancements. | March 17, 2023 | No longer supported |

| Version | Changes | Date | Download link and SHA256 |
| --- | --- | --- | --- |
| 3.2.0 | • Added support for "verify-x509-name" OpenVPN flag.<br>• Automatically detect when updated versions of the client are available.<br>• Added the ability to automatically install new client versions when available. | January 23, 2023 | No longer supported |
| 3.1.0 | Improved security posture. | May 23, 2022 | No longer supported |
| 3.0.0 | • Added Windows 11 support.<br>• Fixed TAP Windows driver naming causing other driver names to be affected.<br>• Fixed the banner message not being displayed when using federated authentication.<br>• Fixed banner text display for longer text.<br>• Enhanced security posture. | March 3, 2022 | No longer supported |
| 2.0.0 | • Added support for banner text after new connection is established.<br>• Removed ability to use pull-filter in relation to echo. i.e. pull-filter * echo<br>• Minor bug fixes and enhancements. | January 20, 2022 | No longer supported |
| 1.3.7 | • Fixed federated authentication connection attempt in some cases.<br>• Minor bug fixes and enhancements. | November 8, 2021 | No longer supported |

| Version | Changes | Date | Download link and SHA256 |
| --- | --- | --- | --- |
| 1.3.6 | • Added support for OpenVPN flags: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout.<br>• Minor bug fixes and enhancements. | September 20, 2021 | No longer supported |
| 1.3.5 | Patch to delete large windows log files. | August 16, 2021 | No longer supported |
| 1.3.4 | • Added support for OpenVPN flag: dhcp-option.<br>• Minor bug fixes and enhancements. | August 4, 2021 | No longer supported |
| 1.3.3 | • Added support for OpenVPN flags: inactive, pull-filter, route.<br>• Fixed an issue that caused app crashes on disconnect or exit.<br>• Fixed an issue with Active Directory usernames with backslash.<br>• Fixed app crash when manipulating profile list outside of app.<br>• Minor bug fixes and enhancements. | July 1, 2021 | No longer supported |
| 1.3.2 | • Add IPv6 leak prevention, when it is configured.<br>• Fixed a potential crash when you use the **Show Details** option under **Connection**. | May 12, 2021 | No longer supported |

| Version | Changes | Date | Download link and SHA256 |
|---|---|---|---|
| 1.3.1 | • Added support for multiple client certificates with same subject. Expired certificates will be ignored.<br>• Fixed local log retention to reduce disk usage.<br>• Added support for 'route-ipv6' OpenVPN directive.<br>• Minor bug fixes and enhancements. | April 5, 2021 | No longer supported |
| 1.3.0 | Added support features such as error reporting, sending diagnostic logs, and analytics. | March 8, 2021 | No longer supported |
| 1.2.7 | • Added support for the cryptoapicert OpenVPN directive.<br>• Fixed stale routes between connectio ns.<br>• Minor bug fixes and enhancements. | February 25, 2021 | No longer supported |
| 1.2.6 | Minor bug fixes and enhancements. | October 26, 2020 | No longer supported |
| 1.2.5 | • Added support for comments in the OpenVPN configuration.<br>• Added an error message for TLS handshake errors. | October 8, 2020 | No longer supported |
| 1.2.4 | Minor bug fixes and enhancements. | September 1, 2020 | No longer supported |
| 1.2.3 | Roll back changes in version 1.2.2. | August 20, 2020 | No longer supported |

| Version | Changes | Date | Download link and SHA256 |
|---|---|---|---|
| 1.2.1 | Minor bug fixes and enhancements. | July 1, 2020 | No longer supported |
| 1.2.0 | • Added support for SAML 2.0-based federated authentication.<br>• Deprecated support for the Windows 7 platform. | May 19, 2020 | No longer supported |
| 1.1.1 | Minor bug fixes and enhancements. | April 21, 2020 | No longer supported |
| 1.1.0 | • Added support for OpenVPN static challenge echo functionality to hide or show the text displayed in the user interface.<br>• Minor bug fixes and enhancements. | March 9, 2020 | No longer supported |
| 1.0.0 | The initial release. | February 4, 2020 | No longer supported |

# AWS Client VPN for macOS

The following procedure shows how to establish a VPN connection using the AWS provided client for macOS. You can download and install the client at AWS Client VPN download. The AWS provided client does not support automatic updates.

**Contents**


- Requirements
- Connecting
- Release notes

## Requirements

To use the AWS provided client for macOS, the following is required:

- macOS Monterey (12.0), Ventura (13.0), or Sonoma (14.0).
- x86_64 processor compatible.
- The client reserves TCP port 8096 on your computer.
- For Client VPN endpoints that use SAML-based federated authentication (single sign-on), the client reserves TCP port 35001.

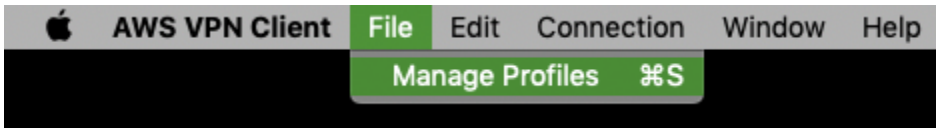
## Connecting

Before you begin, ensure that your Client VPN administrator has created a Client VPN endpoint and provided you with the Client VPN endpoint configuration file.

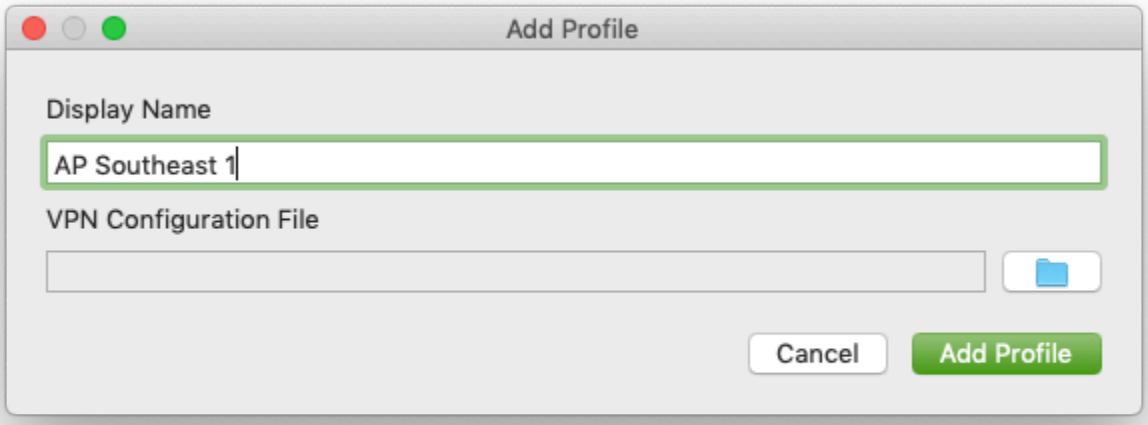
Also, ensure that you've read the requirements. The AWS provided client is also referred to as the *AWS VPN Client* in the following steps.

**To connect using the AWS provided client for macOS**

1. Open the **AWS VPN Client** app.
2. Choose **File**, **Manage Profiles**.

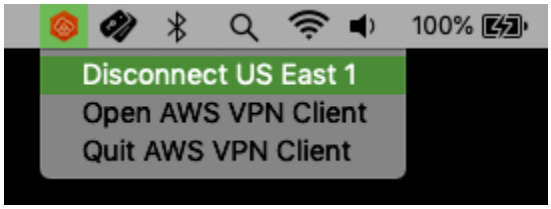



3. Choose **Add Profile**.
4. For **Display Name**, enter a name for the profile.




5. For **VPN Configuration File**, browse to the configuration file that you received from your Client VPN administrator. Choose **Open**.
6. Choose **Add Profile**.
7. In the **AWS VPN Client** window, ensure that your profile is selected and then choose **Connect**. If the Client VPN endpoint has been configured to use credential-based authentication, you'll be prompted to enter a user name and password.
8. To view statistics for your connection, choose **Connection**, **Show Details**.

9. To disconnect, in the **AWS VPN Client** window, choose **Disconnect**. Alternatively, choose the client icon on the menu bar, and then choose **Disconnect *<your-profile-name>***.




## Release notes

The following table contains the release notes and download links for the current and previous versions of AWS Client VPN for macOS.

**Note**

We continue to provide usability and security fixes with every release. We strongly recommend that you use the latest version for every platform. Previous versions may be affected by usability and/or security issues, see release notes for details.

| Version | Changes | Date | Download link |
| --- | --- | --- | --- |
| 3.9.2 | • Resolved a SAML authentication issue with Chromium-based browsers since version 123.<br>• Added support for macOS Sonoma. Deprecate support for macOS Big Sur.<br>• Improved security posture. | April 11, 2024 | Download version 3.9.2<br><br>sha256: 374467d991e8953b5032e5b985cda80a0ea27fb5d5f23cf16c556a1568b0d480 |
| 3.9.1 | • Fixed a buffer overflow action that could potentially allow a local actor to execute arbitrary commands with elevated permissions.<br>• Fixed application update download progress bar.<br>• Improved security posture. | February 16, 2024 | Download version 3.9.1<br><br>sha256: 9bba4b27a635e75038703e2cf4cd814aa75306179fac8e500e2c7af4e899e971 |
| 3.9.0 | • Fixed connectivity issues for some LAN configurations.<br>• Improved accessibility. | December 6, 2023 | Download version 3.9.0<br><br>sha256: f0f6a5579fe9431577 |

| Version | Changes | Date | Download link |
| --- | --- | --- | --- |
| | | | 452e8aac0 7241c36cb 34c2b3f02 8dfdd07f4 1d00ff80d8 |
| 3.8.0 | • Fixed a connectivity issue when NAT64 is enabled in the client network.<br>• Minor bug fixes and enhancements. | August 24, 2023 | Download version 3.8.0<br><br>sha256: d5a229b12 efa2e8862 7127a6dc2 7f5c6a1bc 9c426a8c4 66131ecbd bd6bbb4461 |
| 3.7.0 | • Improved security posture. | August 3, 2023 | Download version 3.7.0<br><br>sha256: 4a34b25b4 8233b02d6 107638a38 68f7e419a 84d20bb49 89f7b394a ae9a9de00a |
| 3.6.0 | • Improved security posture. | July 15, 2023 | No longer supported |
| 3.5.0 | • Rolled back changes from 3.4.0. | July 15, 2023 | No longer supported |

| Version | Changes | Date | Download link |
| --- | --- | --- | --- |
| 3.4.0 | • Improved security posture. | July 14, 2023 | No longer supported |
| 3.3.0 | • Added support for macOS Ventura (13.0).<br>• Minor bug fixes and enhancements. | April 27, 2023 | No longer supported |
| 3.2.0 | • Added support for "verify-x509-name" OpenVPN flag.<br>• Automatically detect when updated versions of the client are available.<br>• Added the ability to automatically install new client versions when available. | January 23, 2023 | No longer supported |
| 3.1.0 | • Added support for macOS Monterey.<br>• Fixed issue for drive type detection.<br>• Improved security posture. | May 23, 2022 | No longer supported |
| 3.0.0 | • Fixed the banner message not being displayed when using federated authentication.<br>• Fixed banner text display for longer text.<br>• Enhanced security posture. | March 3, 2022 | No longer supported. |
| 2.0.0 | • Added support for banner text after new connection is established.<br>• Removed ability to use pull-filter in relation to echo. i.e. pull-filter * echo<br>• Minor bug fixes and enhancements. | January 20, 2022 | No longer supported. |

| Version | Changes | Date | Download link |
| --- | --- | --- | --- |
| 1.4.0 | • Added DNS server monitoring during connection. Settings will be re-configured if they do not match VPN settings.<br>• Fixed federated authentication connection attempt in some cases.<br>• Minor bug fixes and enhancements. | November 9, 2021 | No longer supported. |
| 1.3.5 | • Added support for OpenVPN flags: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout.<br>• Minor bug fixes and enhancements. | September 20, 2021 | No longer supported. |
| 1.3.4 | • Added support for OpenVPN flag: dhcp-option.<br>• Minor bug fixes and enhancements. | August 4, 2021 | No longer supported. |
| 1.3.3 | • Added support for OpenVPN flags: inactive, pull-filter, route.<br>• Fixed an issue with configuration filenames with spaces or Unicode.<br>• Fixed an issue that caused app crashes on disconnect or exit.<br>• Fixed an issue with Active Directory usernames with backslash.<br>• Fixed app crash when manipulating profile list outside of app.<br>• Minor bug fixes and enhancements. | July 1, 2021 | No longer supported. |

| Version | Changes | Date | Download link |
| --- | --- | --- | --- |
| 1.3.2 | • Add IPv6 leak prevention, when it is configured.<br>• Fixed a potential crash when you use the **Show Details** option under **Connection**.<br>• Add daemon log rotation. | May 12, 2021 | No longer supported. |
| 1.3.1 | • Added support for macOS Big Sur (10.16).<br>• Fixed issue that removed DNS settings configured by other applications.<br>• Fixed issue when using a non-valid certificate for mutual authentication causing connectivity issues.<br>• Added support for 'route-ipv6' OpenVPN directive.<br>• Minor bug fixes and enhancements. | April 5, 2021 | No longer supported. |
| 1.3.0 | Added support features such as error reporting, sending diagnostic logs, and analytics. | March 8, 2021 | No longer supported. |
| 1.2.5 | Minor bug fixes and enhancements. | February 25, 2021 | No longer supported. |
| 1.2.4 | Minor bug fixes and enhancements. | October 26, 2020 | No longer supported. |
| 1.2.3 | • Added support for comments in the OpenVPN configuration.<br>• Added an error message for TLS handshake errors.<br>• Fixed an uninstall bug that was affecting some users. | October 8, 2020 | No longer supported. |

| Version | Changes | Date | Download link |
| --- | --- | --- | --- |
| 1.2.2 | Minor bug fixes and enhancements. | August 12, 2020 | No longer supported. |
| 1.2.1 | • Added support for uninstalling application.<br>• Minor bug fixes and enhancements. | July 1, 2020 | No longer supported. |
| 1.2.0 | • Added support for SAML 2.0-based federated authentication.<br>• Added support for macOS Catalina (10.15). | May 19, 2020 | No longer supported. |
| 1.1.2 | Minor bug fixes and enhancements. | April 21, 2020 | No longer supported. |
| 1.1.1 | • Fixed issue where DNS was not resolving.<br>• Fixed an app crash issue caused by longer connections.<br>• Fixed an MFA issue. | April 2, 2020 | No longer supported. |
| 1.1.0 | • Added support for macOS DNS configuration.<br>• Added support for OpenVPN static challenge echo functionality to hide or show the text displayed in the user interface.<br>• Minor bug fixes and enhancements. | March 9, 2020 | No longer supported. |
| 1.0.0 | The initial release. | February 4, 2020 | No longer supported. |

# AWS Client VPN for Linux

The following procedures show how to install the AWS provided client for Linux, and to establish a VPN connection using the AWS provided client. The AWS provided client for Linux does not support automatic updates.

**Contents**


- Requirements
- Installation
- Connecting
- Release notes


## Requirements

To use the AWS provided client for Linux, the following is required:

- Ubuntu 18.04 LTS or Ubuntu 20.04 LTS (AMD64 only)

The client reserves TCP port 8096 on your computer. For Client VPN endpoints that use SAML-based federated authentication (single sign-on) the client reserves TCP port 35001.

Before you begin, ensure that your Client VPN administrator has created a Client VPN endpoint and provided you with the Client VPN endpoint configuration file.

## Installation

There are multiple methods that can be used to install the AWS provided client for Linux. Use one of the methods provided in the following options. Before you begin, ensure that you've read the requirements.

**Option 1 -- Install via package repository**

1. Add the AWS VPN Client public key to your Ubuntu OS.

```
wget -qO- https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-
repo/awsvpnclient_public_key.asc | sudo tee /etc/apt/trusted.gpg.d/
awsvpnclient_public_key.asc
```

2. Use the applicable command to add the repository to your Ubuntu OS, depending on your Ubuntu version:

   Ubuntu 18.04

   ```
   echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
    ubuntu-18.04 main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
   ```

   Ubuntu 20.04

   ```
   echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
    ubuntu-20.04 main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
   ```

3. Use the following command to update the repositories on your system.

   ```
   sudo apt-get update
   ```

4. Use the following command to install the AWS provided client for Linux.

   ```
   sudo apt-get install awsvpnclient
   ```

**Option 2 -- Install using the .deb package file**

1. Download the .deb file from AWS Client VPN download or by using the following command.

   ```
   curl https://d20adtppz83p9s.cloudfront.net/GTK/latest/awsvpnclient_amd64.deb -o
    awsvpnclient_amd64.deb
   ```

2. Install the AWS provided client for Linux using the dpkg utility.

   ```
   sudo dpkg -i awsvpnclient_amd64.deb
   ```

**Option 3 -- Install the .deb package using Ubuntu Software Center**

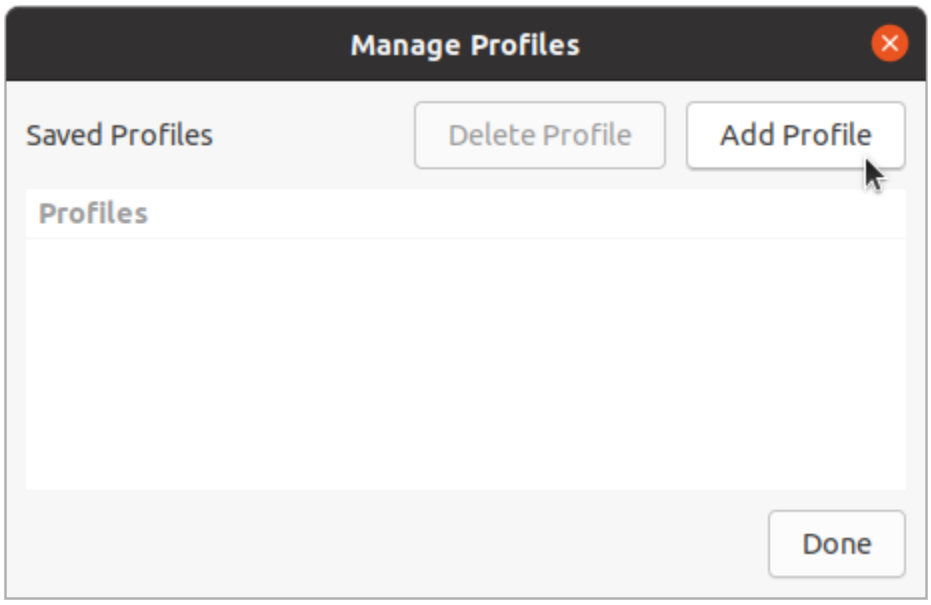
1. Download the .deb package file from AWS Client VPN download .
2. After downloading the .deb package file, use the Ubuntu Software Center to install the package. Follow the steps for installing from a standalone .deb package using Ubuntu Software Center, as described on the Ubuntu Wiki.

# Connecting

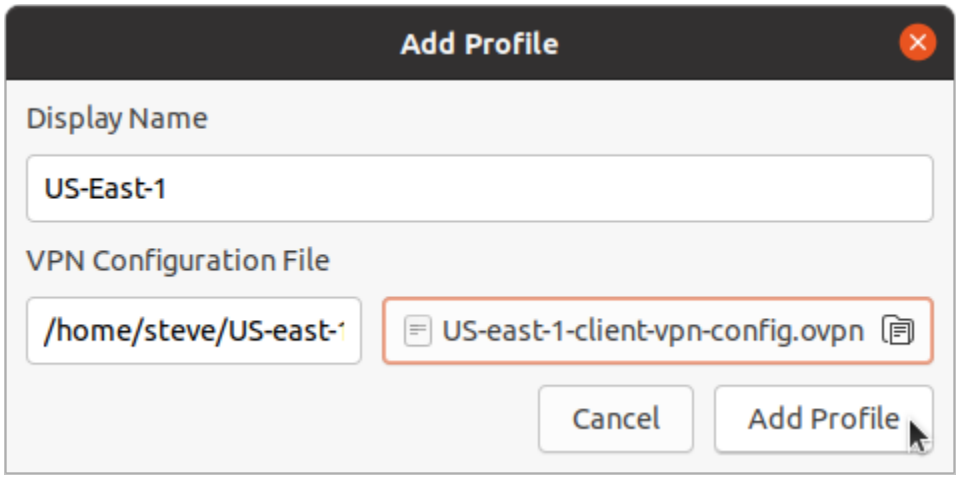
The AWS provided client is also referred to as the *AWS VPN Client* in the following steps.

**To connect using the AWS provided client for Linux**

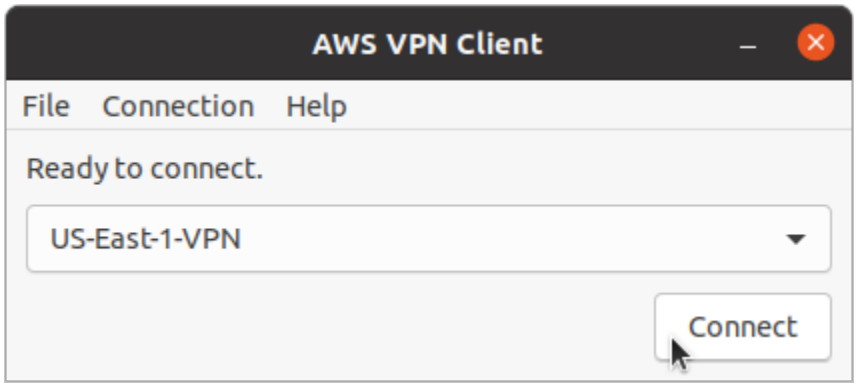
1. Open the **AWS VPN Client** app.
2. Choose **File**, **Manage Profiles**.
3. Choose **Add Profile**.



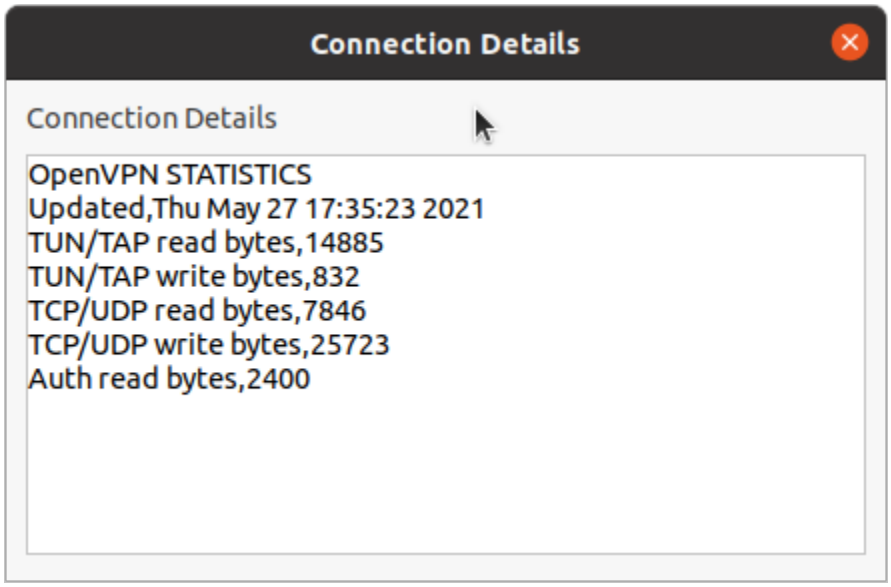

4. For **Display Name**, enter a name for the profile.
5. For **VPN Configuration File**, browse to the configuration file that you received from your Client VPN administrator. Choose **Open**.
6. Choose **Add Profile**.



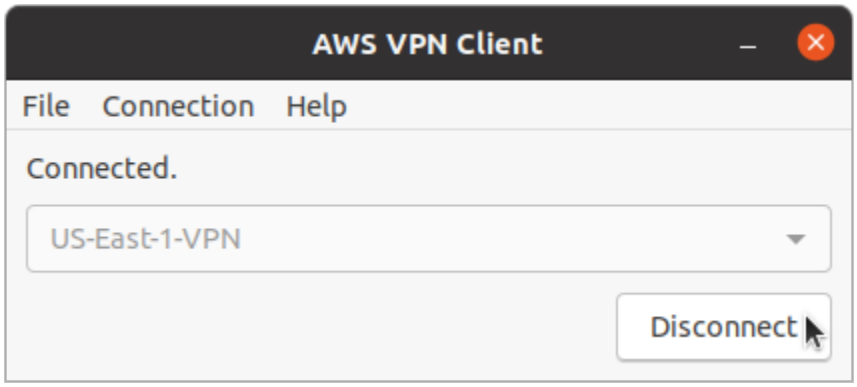
7. In the **AWS VPN Client** window, ensure that your profile is selected, and then choose **Connect**. If the Client VPN endpoint has been configured to use credential-based authentication, you'll be prompted to enter a user name and password.




8. To view statistics for your connection, choose **Connection**, **Show Details**.




9. To disconnect, in the **AWS VPN Client** window, choose **Disconnect**.



# Release notes

The following table contains the release notes and download links for the current and previous versions of AWS Client VPN for Linux.

> **Note**
>
> We continue to provide usability and security fixes with every release. We strongly recommend that you use the latest version for every platform. Previous versions may be affected by usability and/or security issues, see release notes for details.

| Version | Changes | Date | Download link |
|---|---|---|---|
| 3.12.2 | • Resolved a SAML authentication issue with Chromium-based browsers since version 123. | April 11, 2024 | Download version 3.12.2<br><br>sha256: f7178c337 97740bd59 6a14cbe7b 6f5f58fb7 9d17af79f 88bd88013 53a7571a7d |
| 3.12.1 | • Fixed a buffer overflow action that could potentially allow a local actor to execute arbitrary commands with elevated permissions.<br>• Improved security posture. | February 16, 2024 | Download version 3.12.1<br><br>sha256: 547c4ffd3 e35c54db8 e0b792aed 9de1510f6 f31a6009e 55b8af4f0 c2f5cf31d0 |

| Version | Changes | Date | Download link |
| --- | --- | --- | --- |
| 3.12.0 | • Fixed connectivity issues for some LAN configurations. | December 19, 2023 | Download version 3.12.0<br><br>sha256: 9b7398730 9f1dca196 0a322c5dd 86eec1568 ed270bfd2 5f78cc430 e3b5f85cc1 |
| 3.11.0 | • Rollback for "Fixed connectivity issues for some LAN configurations".<br>• Improved accessibility. | December 6, 2023 | Download version 3.11.0<br><br>sha256: 86c0fa1bf 1c9719408 2835a739e c7f1c87e5 40194955f 414a35c67 9b94538970 |
| 3.10.0 | • Fixed connectivity issues for some LAN configurations.<br>• Improved accessibility. | December 6, 2023 | Download version 3.10.0<br><br>sha256: e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51 |

| Version | Changes | Date | Download link |
| --- | --- | --- | --- |
| 3.9.0 | • Fixed a connectivity issue when NAT64 is enabled in the client network.<br>• Minor bug fixes and enhancements. | August 24, 2023 | Download version 3.9.0<br><br>sha256: 6cde9cfff82754119e6a68464d4bb350da3cb3e1ebf9140dacf24e4fd2197454 |
| 3.8.0 | • Improved security posture. | August 3, 2023 | Download version 3.8.0<br><br>sha256: 5fe479236cc0a1940ba37fe168e551096f8dae4c68d45560a164e41edea3e5bd |
| 3.7.0 | • Improved security posture. | July 15, 2023 | No longer supported |
| 3.6.0 | • Rolled back changes from 3.5.0. | July 15, 2023 | No longer supported |
| 3.5.0 | • Improved security posture. | July 14, 2023 | No longer supported |
| 3.4.0 | • Added support for "verify-x509-name" OpenVPN flag. | February 14, 2023 | No longer supported |

| Version | Changes | Date | Download link |
| --- | --- | --- | --- |
| 3.1.0 | • Fixed issue for drive type detection.<br>• Improved security posture. | May 23, 2022 | No longer supported |
| 3.0.0 | • Fixed the banner message not being displayed when using federated authentication.<br>• Fixed banner text display for longer text and specific character sequences.<br>• Enhanced security posture. | March 3, 2022 | No longer supported. |
| 2.0.0 | • Added support for banner text after new connection is established.<br>• Removed ability to use pull-filter in relation to echo. i.e. pull-filter * echo<br>• Minor bug fixes and enhancements. | January 20, 2022 | No longer supported. |
| 1.0.3 | • Fixed federated authentication connection attempt in some cases.<br>• Minor bug fixes and enhancements. | November 8, 2021 | No longer supported. |
| 1.0.2 | • Added support for OpenVPN flags: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout.<br>• Minor bug fixes and enhancements. | September 28, 2021 | No longer supported. |
| 1.0.1 | • Enabled option to quit from Ubuntu application bar.<br>• Added support for OpenVPN flags: inactive, pull-filter, route.<br>• Minor bug fixes and enhancements. | August 4, 2021 | No longer supported. |
| 1.0.0 | The initial release. | June 11, 2021 | No longer supported. |

# Connect using an OpenVPN client

You can connect to a Client VPN endpoint using common Open VPN client applications.

> **Note**
>
> For SAML-based federated authentication, you must use the AWS provided client to connect to a Client VPN endpoint. For more information, see Connect using an AWS provided client or contact your VPN administrator.

**Client applications**

- Connect using a Windows client application
- Connect using an Android or iOS VPN client application
- Connect using a macOS client application
- Connect using an OpenVPN client application

# Connect using a Windows client application

The following procedures show how to establish a VPN connection using Windows-based VPN clients.

Before you begin, ensure that your Client VPN administrator has created a Client VPN endpoint and provided you with the Client VPN endpoint configuration file.

For troubleshooting information, see Windows troubleshooting.

## OpenVPN using a certificate from the Windows Certificate System Store

You can configure the OpenVPN client to use a certificate and private key from the Windows Certificate System Store. This option is useful when you use a smart card as part of your Client VPN connection. For information about the OpenVPN client cryptoapicert option, see Reference Manual for OpenVPN on the OpenVPN website.

> **Note**
>
> The certificate must be stored on the local computer.

**To use the cryptoapicert option with OpenVPN**

1. Create a .pfx file that contains the client certificate and the private key.
2. Import the .pfx file to your personal certificate store, on your local computer. For more information, see How to: View certificates with the MMC snap-in on the Microsoft website.
3. Verify that your account has permissions to read the local computer certificate. You can use the Microsoft Management Console to modify the permissions. For more information, see Rights to see the local computer certificates store on the Microsoft Technet website.
4. Update the OpenVPN configuration file and specify the certificate by using either the certificate subject, or the certificate thumbprint.

   The following is an example of specifying the certificate by using a subject.

   ```
   cryptoapicert “SUBJ:Jane Doe”
   ```

   The following is an example of specifying the certificate by using a thumbprint. You can find the thumbprint by using the Microsoft Management Console. For more information, see How to: Retrieve the Thumbprint of a Certificate on the Microsoft Technet website.

   ```
   cryptoapicert “THUMB:a5 42 00 42 01"
   ```

After you complete the configuration, you use OpenVPN to establish a connection.

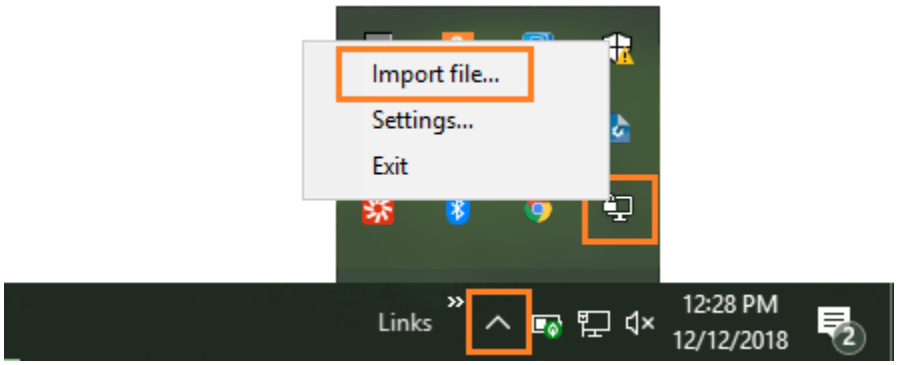
## OpenVPN GUI

The following procedure shows how to establish a VPN connection using the OpenVPN GUI client application on a Windows computer.

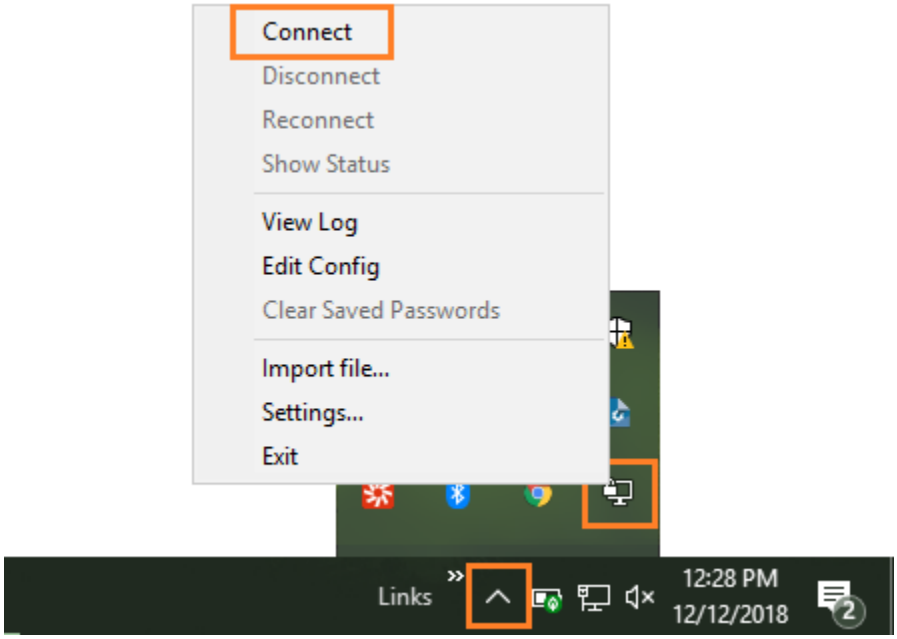
> **Note**
>
> For information about the OpenVPN client application, see Community Downloads on the OpenVPN website.

**To establish a VPN connection**

1. Start the OpenVPN client application.
2. On the Windows taskbar, choose **Show/Hide icons**, right-click **OpenVPN GUI**, and choose **Import file**.




3. In the Open dialog box, select the configuration file that you received from your Client VPN administrator and choose **Open**.
4. On the Windows taskbar, choose **Show/Hide icons**, right-click **OpenVPN GUI**, and choose **Connect**.



## OpenVPN Connect Client

The following procedure shows how to establish a VPN connection using the OpenVPN Connect Client application on a Windows computer.

> **Note**
>
> For more information, see Connecting to Access Server with Windows on the OpenVPN website.

**To establish a VPN connection**

1. Start the OpenVPN Connect Client application.
2. On the Windows taskbar, choose **Show/Hide icons**, right-click **OpenVPN**, and choose **Import profile**.
3. Choose **Import from File** and select the configuration file that you received from your Client VPN administrator.
4. To begin the connection, choose the connection profile.

# Connect using an Android or iOS VPN client application

The following information shows how to establish a VPN connection using the OpenVPN client application on an Android or iOS mobile device. The steps for Android and iOS are the same.

> **Note**
>
> For more information about the OpenVPN client application for Android, see the FAQ regarding OpenVPN Connect Android on the OpenVPN website.

Before you begin, ensure that your Client VPN administrator has created a Client VPN endpoint and provided you with the Client VPN endpoint configuration file.

To establish the connection, start the OpenVPN client application, and then import the file that you received from your Client VPN administrator.

# Connect using a macOS client application

The following procedures show how to establish a VPN connection using macOS-based VPN clients.

Before you begin, ensure that your Client VPN administrator has created a Client VPN endpoint and provided you with the Client VPN endpoint configuration file.

For troubleshooting information, see macOS troubleshooting.

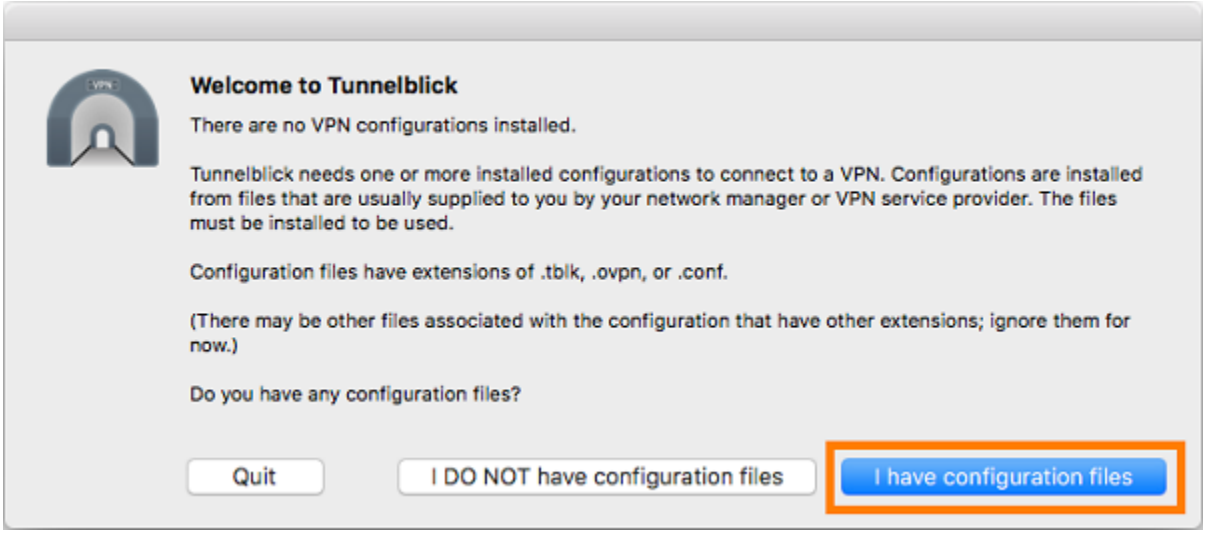
## Tunnelblick

The following procedure shows how to establish a VPN connection using the Tunnelblick client application on a macOS computer.

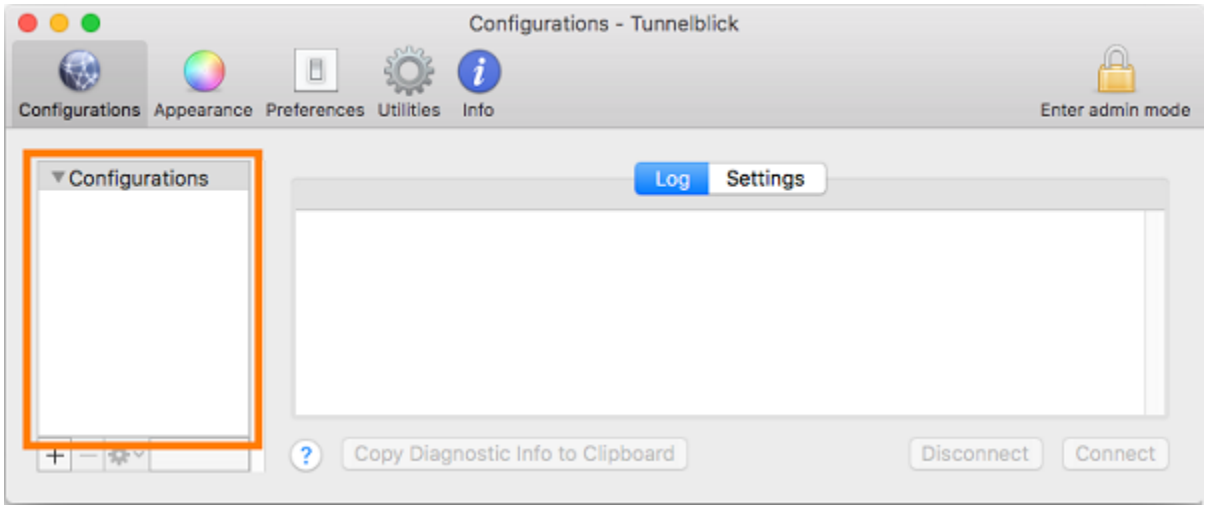
> **Note**
>
> For more information about the Tunnelblick client application for macOS, see the Tunnelblick documentation on the Tunnelblick website.

### To establish a VPN connection

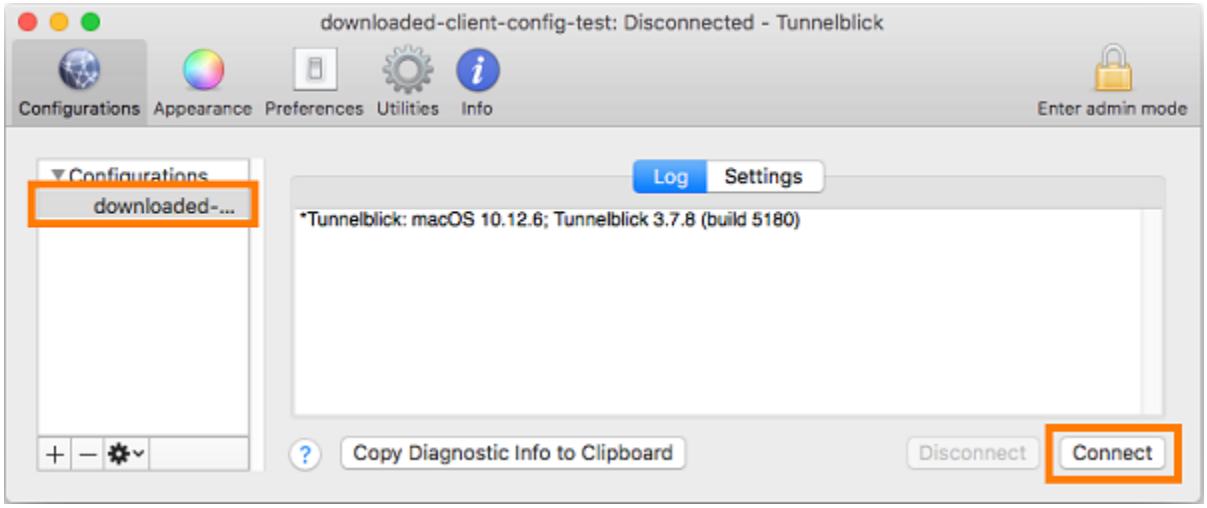
1. Start the Tunnelblick client application and choose **I have configuration files**.




2. Drag and drop the configuration file that you received from your VPN administrator in the **Configurations** panel.




3. Select the configuration file in the **Configurations** panel and choose **Connect**.




## OpenVPN Connect Client

The following procedure shows how to establish a VPN connection using the OpenVPN Connect Client application on a macOS computer.

> **Note**
>
> For more information, see Connecting to Access Server with macOS on the OpenVPN website.

**To establish a VPN connection**

1. Start the OpenVPN application, and choose **Import**, **From local file...**.
2. Navigate to the configuration file that you received from your VPN administrator, and choose **Open**.

# Connect using an OpenVPN client application

The following procedures show how to establish a VPN connection using OpenVPN-based VPN clients.

Before you begin, ensure that your Client VPN administrator has created a Client VPN endpoint and provided you with the Client VPN endpoint configuration file.

For troubleshooting information, see Linux troubleshooting.

> **Important**
>
> If the Client VPN endpoint has been configured to use SAML-based federated authentication, you cannot use the OpenVPN-based VPN client to connect to a Client VPN endpoint.

## OpenVPN - Network Manager

The following procedure shows how to establish a VPN connection using the OpenVPN application through the Network Manager GUI on an Ubuntu computer.

**To establish a VPN connection**

1. Install the network manager module using the following command.

```
sudo apt-get install --reinstall network-manager network-manager-gnome network-manager-openvpn network-manager-openvpn-gnome
```

2. Go to **Settings**, **Network**.
3. Choose the plus symbol (**+**) next to **VPN**, and then choose **Import from file...**.
4. Navigate to the configuration file that you received from your VPN administrator and choose **Open**.

5. In the **Add VPN** window, choose **Add**.
6. Start the connection by enabling the toggle next to the VPN profile that you added.

## OpenVPN

The following procedure shows how to establish a VPN connection using the OpenVPN application on an Ubuntu computer.

**To establish a VPN connection**

1. Install OpenVPN using the following command.

```
sudo apt-get install openvpn
```

2. Start the connection by loading the configuration file that you received from your VPN administrator.

```
sudo openvpn --config /path/to/config/file
```

# Troubleshooting your Client VPN connection

Use the following topics to troubleshoot problems that you might have when using a client application to connect to a Client VPN endpoint.

**Topics**


- Client VPN endpoint troubleshooting for administrators
- Send diagnostic logs to AWS Support in the AWS provided client
- Windows troubleshooting
- macOS troubleshooting
- Linux troubleshooting
- Common problems


## Client VPN endpoint troubleshooting for administrators

Some of the steps in this guide can be performed by you. Other steps must be performed by your Client VPN administrator on the Client VPN endpoint itself. The following sections let you know when you need to contact your administrator.

For additional information about troubleshooting Client VPN endpoint issues, see Troubleshooting Client VPN in the *AWS Client VPN Administrator Guide*.

## Send diagnostic logs to AWS Support in the AWS provided client

If you have problems with the AWS provided client and you need to contact AWS Support to help troubleshoot, the client has an option to send the diagnostic logs to AWS Support. The option is available on the Windows, macOS and Linux client applications.

Before you send the files, you must agree to allow AWS Support to access your diagnostic logs. After you agree, we provide you with a reference number that you can give to AWS Support so that they can immediately access the files.

### Sending diagnostic logs

The AWS provided client is also referred to as the *AWS VPN Client* in the following steps.

**To send diagnostic logs using the AWS provided client for Windows**

1. Open the **AWS VPN Client** app.
2. Choose **Help**, **Send Diagnostic Logs**.
3. In the **Send Diagnostic Logs** window, choose **Yes**.
4. In the **Send Diagnostic Logs** window, perform one of the following operations:

   - To copy the reference number to the clipboard, choose **Yes**, and then choose **OK**.
   - To manually track the reference number, choose **No**.

   When you contact AWS Support, you will need to provide them with the reference number.

**To send diagnostic logs using the AWS provided client for macOS**

1. Open the **AWS VPN Client** app.
2. Choose **Help**, **Send Diagnostic Logs**.
3. In the **Send Diagnostic Logs** window, choose **Yes**.
4. Note the reference number from the confirmation window, and then choose **OK**.

   When you contact AWS Support, you will need to provide them with the reference number.

**To send diagnostic logs using the AWS provided client for Ubuntu**

1. Open the **AWS VPN Client** app.
2. Choose **Help**, **Send Diagnostic Logs**.
3. In the **Send Diagnostic Logs** window, choose **Send**.
4. Note the reference number from the confirmation window. You are given a choice to copy the information to your clipboard if you wish.

   When you contact AWS Support, you will need to provide them with the reference number.

# Windows troubleshooting

The following sections contain information about problems that you might have when using Windows-based clients to connect to a Client VPN endpoint.

**Topics**


- AWS provided client
- OpenVPN GUI
- OpenVPN connect client


# AWS provided client

## AWS provided client

The AWS provided client creates event logs and stores them in the following location on your computer.

```
C:\Users\User\AppData\Roaming\AWSVPNClient\logs
```

The following types of logs are available:

- **Application logs**: Contain information about the application. These logs are prefixed with 'aws_vpn_client_'.
- **OpenVPN logs**: Contain information about OpenVPN processes. These logs are prefixed with 'ovpn_aws_vpn_client_'.

The AWS provided client uses the Windows service to perform root operations. Windows service logs are stored in the following location on your computer.

```
C:\Program Files\Amazon\AWS VPN Client\WinServiceLogs\username
```

**Topics**


- Client cannot connect
- Client cannot connect with "no TAP-Windows adapters" log message
- Client is stuck in a reconnecting state
- VPN connection process quits unexpectedly
- Application fails to launch
- Client cannot create profile
- Client crash occurs on Dell PCs using Windows 10 or 11
- VPN disconnects with a pop up message

### Client cannot connect

#### Problem

The AWS provided client cannot connect to the Client VPN endpoint.

#### Cause

The cause of this problem might be one of the following:

- Another OpenVPN process is already running on your computer, which prevents the client from connecting.
- Your configuration (.ovpn) file is not valid.

#### Solution

Check to see if there are other OpenVPN applications running on your computer. If there are, stop or quit these processes and try connecting to the Client VPN endpoint again. Check the OpenVPN logs for errors, and ask your Client VPN administrator to verify the following information:

- That the configuration file contains the correct client key and certificate. For more information, see Export Client Configuration in the *AWS Client VPN Administrator Guide*.
- That the CRL is still valid. For more information, see Clients Unable to Connect to a Client VPN Endpoint in the *AWS Client VPN Administrator Guide*.

### Client cannot connect with "no TAP-Windows adapters" log message

#### Problem

The AWS provided client cannot connect to the Client VPN endpoint *and* the following error message appears in the application logs: "There are no TAP-Windows adapters on this system. You should be able to create a TAP-Windows adapter by going to Start -> All Programs -> TAP-Windows -> Utilities -> Add a new TAP-Windows virtual ethernet adapter".

#### Solution

You can remediate this problem by taking one or more of the following actions:

- Restart the TAP-Windows adapter.
- Reinstall the TAP-Windows driver.

- Create a new TAP-Windows adapter.

### Client is stuck in a reconnecting state

#### Problem

The AWS provided client is trying to connect to the Client VPN endpoint, but is stuck in a reconnecting state.

#### Cause

The cause of this problem might be one of the following:

- Your computer is not connected to the internet.
- The DNS hostname does not resolve to an IP address.
- An OpenVPN process is indefinitely trying to connect to the endpoint.

#### Solution

Verify that your computer is connected to the internet. Ask your Client VPN administrator to verify that the `remote` directive in the configuration file resolves to a valid IP address. You can also disconnect the VPN session by choosing **Disconnect** in the AWS VPN Client window, and try connecting again.

### VPN connection process quits unexpectedly

#### Problem

While connecting to a Client VPN endpoint, the client quits unexpectedly.

#### Cause

TAP-Windows is not installed on your computer. This software is required to run the client.

#### Solution

Rerun the AWS provided client installer to install all of the required dependencies.

### Application fails to launch

#### Problem

On Windows 7, the AWS provided client does not launch when you try to open it.

**Cause**

.NET Framework 4.7.2 or higher is not installed on your computer. This is required to run the client.

**Solution**

Rerun the AWS provided client installer to install all of the required dependencies.

**Client cannot create profile**

**Problem**

You get the following error when you try to create a profile using the AWS provided client.

```
The config should have either cert and key or auth-user-pass specified.
```

**Cause**

If the Client VPN endpoint uses mutual authentication, the configuration (.ovpn) file does not contain the client certificate and key.

**Solution**

Ensure that your Client VPN administrator adds the client certificate and key to the configuration file. For more information, see Export Client Configuration in the *AWS Client VPN Administrator Guide*.

**Client crash occurs on Dell PCs using Windows 10 or 11**

**Problem**

On certain Dell PCs (desktop and laptop) that are running Windows 10 or 11, a crash can occur when you're browsing your file system to import a VPN configuration file. If this issue occurs, you'll see messages like the following in the logs of the AWS provided client:

```
System.AccessViolationException: Attempted to read or write protected memory. This is
 often an indication that other memory is corrupt.
   at System.Data.SQLite.UnsafeNativeMethods.sqlite3_open_interop(Byte[] utf8Filename,
 Int32 flags, IntPtr& db)
```

```
   at System.Data.SQLite.SQLite3.Open(String strFilename, SQLiteConnectionFlags
connectionFlags, SQLiteOpenFlagsEnum openFlags, Int32 maxPoolSize, Boolean usePool)
   at System.Data.SQLite.SQLiteConnection.Open()
   at
STCommonShellIntegration.DataShellManagement.CreateNewConnection(SQLiteConnection&
newConnection)
   at STCommonShellIntegration.DataShellManagement.InitConfiguration(Dictionary`2
targetSettings)
   at DBROverlayIcon.DBRBackupOverlayIcon.initComponent()
```

**Cause**

The Dell Backup and Recovery system in Windows 10 and 11 might cause conflicts with the AWS provided client, particularly with the following three DLLs:

- DBRShellExtension.dll
- DBROverlayIconBackuped.dll
- DBROverlayIconNotBackuped.dll

**Solution**

To avoid this problem, first make sure that your client is up to date with the latest version of the AWS provided client. Go to AWS Client VPN download and if a newer version is available, upgrade to the latest version.

**In addition, do one of the following:**

- If you are using the Dell Backup and Recovery application, make sure that it's up to date. A Dell forum post states that this issue is resolved in newer versions of the application.
- If you're not using the Dell Backup and Recovery application, some action will still need to be taken if you are experiencing this problem. If you do not wish to upgrade the application, as an alternative, you can delete or rename the DLL files. However, note that this will prevent the Dell Backup and Recovery application from functioning completely.

**Delete or rename the DLL files**

1. Go to Windows Explorer and browse to the location where Dell Backup and Recovery is installed. It typically is installed in the following location, but you might need to search to find it.

```
C:\Program Files (x86)\Dell Backup and Recovery\Components\Shell
```

2. Manually delete the following DLL files from the installation directory, or rename them. Either action will prevent them from being loaded.

   - DBRShellExtension.dll
   - DBROverlayIconBackuped.dll
   - DBROverlayIconNotBackuped.dll

   You can rename the files by adding ".bak" to the end of the file name, for example, **DBROverlayIconBackuped.dll.bak**.

### VPN disconnects with a pop up message

#### Problem

The VPN disconnects with a pop up message that says: "The VPN connection is being terminated because the address space of the local network your device is connected to has changed. Please establish a new VPN connection."

#### Cause

TAP-Windows adapter does not contain the required description.

#### Solution

If the `Description` field does not match below, first remove the TAP-Windows adapter, then rerun the AWS provided client installer to install all of the required dependencies.

```
C:\Users\jdoe> ipconfig /all

Ethernet adapter Ethernet 2:

Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
Description . . . . . . . . . . . : AWS VPN Client TAP-Windows Adapter V9
Physical Address. . . . . . . . . : 00-FF-50-ED-5A-DE
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

## OpenVPN GUI

The following troubleshooting information was tested on versions 11.10.0.0 and 11.11.0.0 of the OpenVPN GUI software on Windows 10 Home (64-bit) and Windows Server 2016 (64-bit).

The configuration file is stored in the following location on your computer.

```
C:\Users\User\OpenVPN\config
```

The connection logs are stored in the following location on your computer.

```
C:\Users\User\OpenVPN\log
```

## OpenVPN connect client

The following troubleshooting information was tested on versions 2.6.0.100 and 2.7.1.101 of the OpenVPN Connect Client software on Windows 10 Home (64-bit) and Windows Server 2016 (64-bit).

The configuration file is stored in the following location on your computer.

```
C:\Users\User\AppData\Roaming\OpenVPN Connect\profile
```

The connection logs are stored in the following location on your computer.

```
C:\Users\User\AppData\Roaming\OpenVPN Connect\logs
```

### Unable to resolve DNS

#### Problem

The connection fails with the following error.

```
Transport Error: DNS resolve error on 'cvpn-endpoint-xyz123.prod.clientvpn.us-
east-1.amazonaws.com (http://cvpn-endpoint-xyz123.prod.clientvpn.us-
east-1.amazonaws.com/)' for UDP session: No such host is known.
```

#### Cause

The DNS name cannot be resolved. The client must prepend a random string to the DNS name to prevent DNS caching; however, some clients do not do this.

**Solution**

See the solution for Unable to Resolve Client VPN Endpoint DNS Name in the *AWS Client VPN Administrator Guide*.

### Missing PKI alias

**Problem**

A connection to a Client VPN endpoint that does not use mutual authentication fails with the following error.

```
FATAL:CLIENT_EXCEPTION: connect error: Missing External PKI alias
```

**Cause**

The OpenVPN Connect Client software has a known issue where it attempts to authenticate using mutual authentication. If the configuration file does not contain a client key and certificate, authentication fails.

**Solution**

Specify a random client key and certificate in the Client VPN configuration file and import the new configuration into the OpenVPN Connect Client software. Alternatively, use a different client, such as the OpenVPN GUI client (v11.12.0.0) or the Viscosity client (v.1.7.14).

## macOS troubleshooting

The following sections contain information about logging and problems that you might have when using macOS clients. Please ensure that you are running the latest version of these clients.

**Topics**

- AWS provided client
- Tunnelblick
- OpenVPN

# AWS provided client

The AWS provided client creates event logs and stores them in the following location on your computer.

```
/Users/username/.config/AWSVPNClient/logs
```

The following types of logs are available:

- **Application logs**: Contain information about the application. These logs are prefixed with 'aws_vpn_client_'.
- **OpenVPN logs**: Contain information about OpenVPN processes. These logs are prefixed with 'ovpn_aws_vpn_client_'.

The AWS provided client uses the client daemon to perform root operations. The daemon logs are stored in the following locations on your computer.

```
/tmp/AcvcHelperErrLog.txt
/tmp/AcvcHelperOutLog.txt
```

The AWS provided client stores the configuration files in the following location on your computer.

```
/Users/username/.config/AWSVPNClient/OpenVpnConfigs
```

**Topics**


- Client cannot connect
- Client is stuck in a reconnecting state
- Client cannot create profile


## Client cannot connect

### Problem

The AWS provided client cannot connect to the Client VPN endpoint.

### Cause

The cause of this problem might be one of the following:

- Another OpenVPN process is already running on your computer, which prevents the client from connecting.
- Your configuration (.ovpn) file is not valid.

#### Solution

Check to see if there are other OpenVPN applications running on your computer. If there are, stop or quit these processes and try connecting to the Client VPN endpoint again. Check the OpenVPN logs for errors, and ask your Client VPN administrator to verify the following information:

- That the configuration file contains the correct client key and certificate. For more information, see Export Client Configuration in the *AWS Client VPN Administrator Guide*.
- That the CRL is still valid. For more information, see Clients Unable to Connect to a Client VPN Endpoint in the *AWS Client VPN Administrator Guide*.

### Client is stuck in a reconnecting state

#### Problem

The AWS provided client is trying to connect to the Client VPN endpoint, but is stuck in a reconnecting state.

#### Cause

The cause of this problem might be one of the following:

- Your computer is not connected to the internet.
- The DNS hostname does not resolve to an IP address.
- An OpenVPN process is indefinitely trying to connect to the endpoint.

#### Solution

Verify that your computer is connected to the internet. Ask your Client VPN administrator to verify that the `remote` directive in the configuration file resolves to a valid IP address. You can also disconnect the VPN session by choosing **Disconnect** in the AWS VPN Client window, and try connecting again.

### Client cannot create profile

#### Problem

You get the following error when you try to create a profile using the AWS provided client.

```
The config should have either cert and key or auth-user-pass specified.
```

#### Cause

If the Client VPN endpoint uses mutual authentication, the configuration (.ovpn) file does not contain the client certificate and key.

#### Solution

Ensure that your Client VPN administrator adds the client certificate and key to the configuration file. For more information, see Export Client Configuration in the *AWS Client VPN Administrator Guide*.

## Tunnelblick

The following troubleshooting information was tested on version 3.7.8 (build 5180) of the Tunnelblick software on macOS High Sierra 10.13.6.

The configuration file for private configurations is stored in the following location on your computer.

```
/Users/username/Library/Application Support/Tunnelblick/Configurations
```

The configuration file for shared configurations is stored in the following location on your computer.

```
/Library/Application Support/Tunnelblick/Shared
```

The connection logs are stored in the following location on your computer.

```
/Library/Application Support/Tunnelblick/Logs
```

To increase the log verbosity, open the Tunnelblick application, choose **Settings**, and adjust the value for **VPN log level**.

## Cipher algorithm 'AES-256-GCM' not found

### Problem

The connection fails and returns the following error in the logs.

```
2019-04-11 09:37:14 Cipher algorithm 'AES-256-GCM' not found
2019-04-11 09:37:14 Exiting due to fatal error
```

### Cause

The application is using an OpenVPN version that doesn't support cipher algorithm AES-256-GCM.

### Solution

Choose a compatible OpenVPN version by doing the following:

1. Open the Tunnelblick application.
2. Choose **Settings**.
3. For **OpenVPN version**, choose **2.4.6 - OpenSSL version is v1.0.2q**.

## Connection stops responding and resets

### Problem

The connection fails and returns the following error in the logs.

```
MANAGEMENT: >STATE:1559117927,WAIT,,,,,,
MANAGEMENT: >STATE:1559117928,AUTH,,,,,,
TLS: Initial packet from [AF_INET]3.217.107.5:443, sid=df19e70f a992cda3
VERIFY OK: depth=1, CN=server-certificate
VERIFY KU OK
Validating certificate extended key usage
Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
 Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=server-cvpn
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
```

### Cause

The client certificate has been revoked. The connection stops responding after trying to authenticate and is eventually reset from the server side.

**Solution**

Request a new configuration file from your Client VPN administrator.

## Extended key usage (EKU)

**Problem**

The connection fails and returns the following error in the logs.

```
TLS: Initial packet from [AF_INET]50.19.205.135:443, sid=29f2c917 4856ad34
VERIFY OK: depth=2, O=Digital Signature Trust Co., CN=DST Root CA X3
VERIFY OK: depth=1, C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
VERIFY KU OK
Validating certificate extended key usage
 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
 Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=cvpn-lab.myrandomnotes.com (http://cvpn-lab.myrandomnotes.com/)
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
MANAGEMENT: >STATE:1559138717,RECONNECTING,connection-reset,,,,,
```

**Cause**

The server authentication succeeded. However, the client authentication fails because the client certificate has the extended key usage (EKU) field enabled for server authentication.

**Solution**

Verify that you are using correct client certificate and key. If necessary, verify with your Client VPN administrator. This error might occur if you're using the server certificate and not the client certificate to connect to the Client VPN endpoint.

## Expired certificate

**Problem**

The server authentication succeeds but the client authentication fails with the following error.

```
WARNING: “Connection reset, restarting [0] , SIGUSR1[soft,connection-reset] received,
 process restarting”
```

**Cause**

The client certificate validity has expired.

**Solution**

Request a new client certificate from your Client VPN administrator.

# OpenVPN

The following troubleshooting information was tested on version 2.7.1.100 of the OpenVPN Connect Client software on macOS High Sierra 10.13.6.

The configuration file is stored in the following location on your computer.

```
/Library/Application Support/OpenVPN/profile
```

The connection logs are stored in the following location on your computer.

```
Library/Application Support/OpenVPN/log/connection_name.log
```

## Cannot resolve DNS

**Problem**

The connection fails with the following error.

```
Mon Jul 15 13:07:17 2019 Transport Error: DNS resolve error on 'cvpn-
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com' for UDP session: Host not found
 (authoritative)
Mon Jul 15 13:07:17 2019 Client terminated, restarting in 2000 ms...
Mon Jul 15 13:07:18 2019 CONNECTION_TIMEOUT [FATAL-ERR]
Mon Jul 15 13:07:18 2019 DISCONNECTED
Mon Jul 15 13:07:18 2019 >FATAL:CONNECTION_TIMEOUT
```

**Cause**

OpenVPN Connect is unable to resolve the Client VPN DNS name.

**Solution**

See the solution for Unable to Resolve Client VPN Endpoint DNS Name in the *AWS Client VPN Administrator Guide*.

# Linux troubleshooting

The following sections contain information about logging, and about problems that you might have when using Linux-based clients. Please ensure that you are running the latest version of these clients.

**Topics**

- AWS provided client
- OpenVPN (command line)
- OpenVPN through Network Manager (GUI)

## AWS provided client

The AWS provided client stores log files and configuration files in the following location on your system:

```
/home/username/.config/AWSVPNClient/
```

The AWS provided client daemon process stores log files in the following location on your system:

```
/var/log/aws-vpn-client/username/
```

**Problem**

Under some circumstances after a VPN connection is established, DNS queries will still go to the default system nameserver, instead of the nameservers that are configured for the ClientVPN endpoint.

**Cause**

The client interacts with **systemd-resolved**, a service available on Linux systems, which serves as a central piece of DNS management. It is used to configure DNS servers that are pushed from the

ClientVPN endpoint. The problem occurs because **systemd-resolved** doesn't set the highest priority to DNS servers that are provided by the ClientVPN endpoint. Instead, it appends the servers to the existing list of DNS servers that are configured on the local system. As a result, the original DNS servers might still have the highest priority, and therefore be used to resolve DNS queries.

**Solution**

1. Add the following directive on the first line of the OpenVPN config file, to make sure that all DNS queries are sent to the VPN tunnel.

   ```
   dhcp-option DOMAIN-ROUTE .
   ```

2. Use the stub resolver provided by **systemd-resolved**. To do this, symlink `/etc/resolv.conf` to `/run/systemd/resolve/stub-resolv.conf` by running the following command on the system.

   ```
   sudo ln -sf /run/systemd/resolve/stub-resolv.conf /etc/resolv.conf
   ```

3. (Optional) If you do not want **systemd-resolved** to proxy DNS queries, and instead would like the queries to be sent to the real DNS nameservers directly, symlink `/etc/resolv.conf` to `/run/systemd/resolve/resolv.conf` instead.

   ```
   sudo ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf
   ```

   You might want to do this procedure in order to bypass the **systemd-resolved** configuration, for example for DNS answer caching, per-interface DNS configuration, DNSSec enforcement, and so on. This option is especially useful when you have a need to override a public DNS record with a private record when connected to VPN. For example, you might have a private DNS resolver in your private VPC with a record for www.example.com, which resolves to a private IP. This option could be used to override the public record of www.example.com, which resolves to a public IP.

## OpenVPN (command line)

**Problem**

The connection does not function correctly because DNS resolution is not working.

**Cause**

The DNS server is not configured on the Client VPN endpoint, or it is not being honored by the client software.

**Solution**

Use the following steps to check that the DNS server is configured and working correctly.

1. Ensure that a DNS server entry is present in the logs. In the following example, the DNS server `192.168.0.2` (configured in the Client VPN endpoint) is returned in the last line.

   ```
   Mon Apr 15 21:26:55 2019 us=274574 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
   WRRMon Apr 15 21:26:55 2019 us=276082 PUSH: Received control message:
    'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 192.168.0.2,route-
   gateway 10.0.0.97,topology subnet,ping 1,ping-restart 20,auth-token,ifconfig
    10.0.0.98 255.255.255.224,peer-id 0
   ```

   If there is no DNS server specified, ask your Client VPN administrator to modify the Client VPN endpoint and ensure that a DNS server (for example, the VPC DNS server) has been specified for the Client VPN endpoint. For more information, see Client VPN Endpoints in the *AWS Client VPN Administrator Guide*.
2. Ensure that the `resolvconf` package is installed by running the following command.

   ```
   sudo apt list resolvconf
   ```

   The output should return the following.

   ```
   Listing... Done
   resolvconf/bionic-updates,now 1.79ubuntu10.18.04.3 all [installed]
   ```

   If it's not installed, install it using the following command.

   ```
   sudo apt install resolvconf
   ```
3. Open the Client VPN configuration file (the .ovpn file) in a text editor and add the following lines.

   ```
   script-security 2
   up /etc/openvpn/update-resolv-conf
   down /etc/openvpn/update-resolv-conf
   ```

Check the logs to verify that the `resolvconf` script has been invoked. The logs should contain a line similar to the following.

```
Mon Apr 15 21:33:52 2019 us=795388 /etc/openvpn/update-resolv-conf tun0 1500 1552
 10.0.0.98 255.255.255.224 init
dhcp-option DNS 192.168.0.2
```

## OpenVPN through Network Manager (GUI)

### Problem

When using the Network Manager OpenVPN client, the connection fails with the following error.

```
Apr 15 17:11:07  OpenVPN 2.4.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
 [PKCS11] [MH/PKTINFO] [AEAD] built on Sep  5 2018
Apr 15 17:11:07  library versions: OpenSSL 1.1.0g  2 Nov 2017, LZO 2.08
Apr 15 17:11:07  RESOLVE: Cannot resolve host address: cvpn-
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com:443 (Name or service not known)
Apr 15 17:11:07  RESOLVE: Cannot resolve host
Apr 15 17:11:07  Could not determine IPv4/IPv6 protocol
```

### Cause

The `remote-random-hostname` flag is not honored, and the client cannot connect using the `network-manager-gnome` package.

### Solution

See the solution for Unable to Resolve Client VPN Endpoint DNS Name in the *AWS Client VPN Administrator Guide*.

# Common problems

The following are common problems that you might have when using a client to connect to a Client VPN endpoint.

## TLS key negotiation failed

### Problem

The TLS negotiation fails with the following error.

```
TLS key negotiation failed to occur within 60 seconds (check your network connectivity)
TLS Error: TLS handshake failed
```

### Cause

The cause of this problem might be one of the following:

- Firewall rules are blocking UDP or TCP traffic.
- You're using the incorrect client key and certificate in your configuration (.ovpn) file.
- The client certificate revocation list (CRL) has expired.

### Solution

Check to see if the firewall rules on your computer are blocking inbound or outbound TCP or UDP traffic on ports 443 or 1194. Ask your Client VPN administrator to verify the following information:

- That the firewall rules for the Client VPN endpoint do not block TCP or UDP traffic on ports 443 or 1194.
- That the configuration file contains the correct client key and certificate. For more information, see Export Client Configuration in the *AWS Client VPN Administrator Guide*.
- That the CRL is still valid. For more information, see Clients Unable to Connect to a Client VPN Endpoint in the *AWS Client VPN Administrator Guide*.

# Document history

The following table describes the AWS Client VPN User Guide updates.

| Change | Description | Date |
| --- | --- | --- |
| AWS provided client (3.9.2) for macOS released | See release notes for details. | April 11, 2024 |
| AWS provided client (3.12.2) for Ubuntu released | See release notes for details. | April 11, 2024 |
| AWS provided client (3.11.2) for Windows released | See release notes for details. | April 11, 2024 |
| AWS provided client (3.9.1) for macOS released | See release notes for details. | February 16, 2024 |
| AWS provided client (3.12.1) for Ubuntu released | See release notes for details. | February 16, 2024 |
| AWS provided client (3.11.1) for Windows released | See release notes for details. | February 16, 2024 |
| AWS provided client (3.12.0) for Ubuntu released | See release notes for details. | December 19, 2023 |
| AWS provided client (3.9.0) for macOS released | See release notes for details. | December 6, 2023 |
| AWS provided client (3.11.0) for Windows released | See release notes for details. | December 6, 2023 |
| AWS provided client (3.11.0) for Ubuntu released | See release notes for details. | December 6, 2023 |
| AWS provided client (3.10.0) for Ubuntu released | See release notes for details. | December 6, 2023 |

| | | |
|---|---|---|
| AWS provided client (3.9.0) for Ubuntu released | See release notes for details. | August 24, 2023 |
| AWS provided client (3.8.0) for macOS released | See release notes for details. | August 24, 2023 |
| AWS provided client (3.10.0) for Windows released | See release notes for details. | August 24, 2023 |
| AWS provided client (3.9.0) for Windows released | See release notes for details. | August 3, 2023 |
| AWS provided client (3.8.0) for Ubuntu released | See release notes for details. | August 3, 2023 |
| AWS provided client (3.7.0) for macOS released | See release notes for details. | August 3, 2023 |
| AWS provided client (3.8.0) for Windows released | See release notes for details. | July 15, 2023 |
| AWS provided client (3.7.0) for Windows released | See release notes for details. | July 15, 2023 |
| AWS provided client (3.7.0) for Ubuntu released | See release notes for details. | July 15, 2023 |
| AWS provided client (3.6.0) for macOS released | See release notes for details. | July 15, 2023 |
| AWS provided client (3.6.0) for Ubuntu released | See release notes for details. | July 15, 2023 |
| AWS provided client (3.5.0) for macOS released | See release notes for details. | July 15, 2023 |
| AWS provided client (3.6.0) for Windows released | See release notes for details. | July 14, 2023 |

| | | |
|---|---|---|
| AWS provided client (3.5.0) for Ubuntu released | See release notes for details. | July 14, 2023 |
| AWS provided client (3.4.0) for macOS released | See release notes for details. | July 14, 2023 |
| AWS provided client (3.3.0) for macOS released | See release notes for details. | April 27, 2023 |
| AWS provided client (3.5.0) for Windows released | See release notes for details. | April 3, 2023 |
| AWS provided client (3.4.0) for Windows released | See release notes for details. | March 28, 2023 |
| AWS provided client (3.3.0) for Windows released | See release notes for details. | March 17, 2023 |
| AWS provided client (3.4.0) for Ubuntu released | See release notes for details. | February 14, 2023 |
| AWS provided client (3.2.0) for macOS released | See release notes for details. | January 23, 2023 |
| AWS provided client (3.2.0) for Windows released | See release notes for details. | January 23, 2023 |
| AWS provided client (3.1.0) for macOS released | See release notes for details. | May 23, 2022 |
| AWS provided client (3.1.0) for Windows released | See release notes for details. | May 23, 2022 |
| AWS provided client (3.1.0) for Ubuntu released | See release notes for details. | May 23, 2022 |
| AWS provided client (3.0.0) for macOS released | See release notes for details. | March 3, 2022 |

| | | |
|---|---|---|
| AWS provided client (3.0.0) for Windows released | See release notes for details. | March 3, 2022 |
| AWS provided client (3.0.0) for Ubuntu released | See release notes for details. | March 3, 2022 |
| AWS provided client (2.0.0) for macOS released | See release notes for details. | January 20, 2022 |
| AWS provided client (2.0.0) for Windows released | See release notes for details. | January 20, 2022 |
| AWS provided client (2.0.0) for Ubuntu released | See release notes for details. | January 20, 2022 |
| AWS provided client (1.4.0) for macOS released | See release notes for details. | November 9, 2021 |
| AWS provided client for Windows (1.3.7) released | See release notes for details. | November 8, 2021 |
| AWS provided client (1.0.3) for Ubuntu released | See release notes for details. | November 8, 2021 |
| AWS provided client (1.0.2) for Ubuntu released | See release notes for details. | September 28, 2021 |
| AWS provided client for Windows (1.3.6) and macOS (1.3.5) released | See release notes for details. | September 20, 2021 |
| AWS provided client for Ubuntu 18.04 LTS and Ubuntu 20.04 LTS released | You can use the AWS-provided client on Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. | June 11, 2021 |
| Support for OpenVPN using a certificate from the Windows Certificate System Store | You can use OpenVPN with a certificate from the Windows Certificate System Store. | February 25, 2021 |

| | | |
|---|---|---|
| Self-service portal | You can access a self-service portal to get the latest AWS provided client and configuration file. | October 29, 2020 |
| AWS provided client | You can use the AWS provided client to connect to a Client VPN endpoint. | February 4, 2020 |
| Initial release | This release introduces AWS Client VPN. | December 18, 2018 |