User Guide

AWS Client VPN

AWS Client VPN: User Guide

Table of Contents

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.

Client VPN 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 that are required to establish a VPN connection. You load this file into your chosen VPN client application. The AWS provided client allows you to connect to five concurrent sessions, each session with its own configuration file provided by the Client VPN administrator. For more information about concurrent sessions, see Support for concurrent connections.

Additional resources for configuring Client VPN

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.

Get started with AWS 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 for using Client VPN

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

- Access to the internet
- A supported device
- A supported version of Windows, macOS, or Linux.
- 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.

You can download the Client VPN application through one of two methods, depending on whether the administrator created the endpoint configuration file for the application:

- If your administrator did not set up endpoint configuration files, download and install the client from AWS Client VPN download. After downloading and installing the application, proceed to the section called “Step 2: Get the Client VPN endpoint configuration file” to get the endpoint configuration file from your administrator. If you're connecting to multiple profiles, you'll need a configuration file for each profile.
- If your administrator has already preconfigured the endpoint configuration file, you can download the Client VPN application, along with the configuration file, from the self-service portal. For the steps to download the client and configuration file from the self-service portal, see the section called “Download Client VPN”. After downloading and installing the application and file, go to the section called “Step 3: Connect to the VPN”.

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 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 Download the AWS Client VPN from 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, including importing one or more endpoint configuration files for an AWS provided client, see the following topics:

- Connect to an AWS Client VPN endpoint using an AWS provided client
- Connect to an AWS Client VPN endpoint 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.

Download the AWS Client VPN from the self-service portal

The self-service portal is a web page that enables you to download the latest version of the AWS provided client and the latest versions of Client VPN endpoint configuration files. If your Client VPN endpoint administrator has preconfigured one or more configuration files for the Client VPN client, you can download and install that Client VPN application along with those configuration files, from this portal.

> **Note**
>
> If you're an administrator and want to configure the self-service portal, see Client VPN endpoints in the *AWS Client VPN Administrator Guide*.

Before you begin, you must have the ID of each Client VPN endpoint you want to download Your Client VPN endpoint administrator can provide you with the ID, or can give you a self-service portal URL that includes the ID. For multiple endpoint connections you'll need the endpoint ID for each profile you want to connect to.

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. If you want to connect to multiple endpoints, you'll need to download the configuration file for each endpoint.
   - Download the latest version of the AWS provided client for your platform.
5. Repeat these steps for each endpoint configuration file you want to create a connection profile for.

Connect to an AWS Client VPN endpoint using an AWS provided client

You can connect to a Client VPN endpoint using the AWS provided client, which is supported on Windows, macOS, and Ubuntu. The AWS provided client also supports up to five concurrent connections as well as OpenVPN directives.

Topics

Support for concurrent connections using an AWS provided client

The AWS provided client allows to connect to multiple concurrent sessions. This is helpful if you need access to resources across multiple AWS environments and have different endpoints for those resources. For example, you might need access to a database in an environment at an endpoint that's different from the endpoint you're currently connected to, but you don't want to disconnect the current connection. To enable your AWS provided client to connect to current sessions, download the configuration file that your administrator created for each endpoint, and then and create a connection profile for each file. Using the AWS provided client, you can then connect to multiple sessions without disconnecting from any session currently open. This is supported for AWS provided clients only. For the steps to connect to concurrent sessions, see the following:

- Connect using the AWS provided client for Windows
- Connect using the AWS provided client for macOS
- Connect using the AWS provided client for Linux

When connecting to multiple endpoints, Client VPN implements checks to ensure there are no conflicts with other open endpoint connections — for example, if two sessions have conflicting CIDR blocks or routing policies; or, if you're already connected with a full tunnel connection. If the check finds conflicts, a connection won't be established until you either choose a different connection that isn't in conflict with the open connection, or you disconnect from the open session that's causing the conflict.

Concurrent DNS connections are allowed. The DNS server of one of the DNS-enabled connections will be applied. Depending on the DNS server, you might be prompted for authentication during that reconnection.

> **Note**
>
> The maximum number of allowed concurrent sessions is five.

OpenVPN directives

The AWS provided client supports the following OpenVPN directives. For more information about these directives, see the documentation at the OpenVPN website.

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- ca
- cert
- cipher
- client
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- bb

  dhcp-option
- ifconfig-ipv6

- inactive
- keepalive
- key
- mssfix
- nobind
- persist-key
- persist-tun
- ping
- ping-exit
- 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
- tap-sleep
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN for Windows

These sections describe 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.

Requirements

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

- Windows 10 or Windows 11 (64-bit operating system, x64 processor)
- .NET Framework 4.7.2 or higher

For Client VPN endpoints that use SAML-based federated authentication (single sign-on), the client reserves TCP ports 8096-8115 on your computer.

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. If you want to connect to multiple profiles simultaneously, you'll need a configuration file for each profile.

Topics

Connect to AWS Client VPN with an AWS provided client for Windows

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. If you want to create multiple connections, repeat the **Add Profile** steps for each configuration file you want to add. You can add as many profiles as you like, but you can only have up to five open connections.
7. In the **AWS VPN Client** window, choose the profile that you want to connect to, 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. Repeat this step for each profile connection you want to initiate, connecting up to five concurrent endpoints.

   > **Note**
   >
   > If any profile you connect to conflicts with a currently open session, you won't be able to make the connection. Either choose a new connection or disconnect from the session causing the conflict.

8. To view statistics for a connection, choose **Connection** in the **AWS VPN client** window, choose **Show Details**, and then choose the connection you want to see details about.
9. To disconnect a connection, choose a connection in the **AWS VPN client** window, and then choose **Disconnect**. If you have multiple open connections, you must close each connection individually. Alternatively, choose the client icon on the Windows taskbar, and then choose **Disconnect**.

AWS Client VPN for Windows 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 might be affected by usability and/or security issues. See release notes for details.

Version	Changes	Date	Download link and SHA256
5.2.2	Improved security posture.	June 2, 2025	[Download version 5.2.2] sha256: f27cb0eed 7c9c5354c aa5d7e375 95eefbb04 8d7481bf6 98b2e5fb6 53b667c190
5.2.1	- Added support for the `ping-exit` OpenVPN flag. - Updated the OpenSSL library. - Minor bug fixes and enhancements.	April 21, 2025	No longer supported.
5.2.0	- Minor enhancements. - Added support for Client Route Enforcement.	April 8, 2025	No longer supported.
5.1.0	- Fixed an issue that caused AWS Client VPN version 5.0.x to automatically reconnect to VPN after an inactivity timeout disconnect. - Minor bug fixes and enhancements.	March 17, 2025	No longer supported.
5.0.2	- Fixed a DNS issue for concurrent connections. - Fixed sporadic issues when installing new TAP adapters.	February 24, 2025	No longer supported.
5.0.1	Fixed an issue that led to sporadic VPN connection errors on Windows client version 5.0.0.	January 30, 2025	No longer supported.

Version	Changes	Date	Download link and SHA256
5.0.0	- Added support for concurrent connections. - Updated the TAP driver version. - Updated the graphical user interface. - Minor bug fixes and enhancements	January 21, 2025	No longer supported.
4.1.0	Minor bug fixes and enhancements.	November 12, 2024	No longer supported.
4.0.0	Minor enhancements.	September 25, 2024	Download version 4.0.0 sha256: 6532f9113 85ec8fac1 494d0847c 8f90a999b 3bd738084 4e2ea4318 e9db4a2ebc
3.14.2	Added support for the `mssfix` OpenVPN flag.	September 4, 2024	Download version 3.14.2 sha256: c171639d7 e07e5fd48 998cf76f7 4e6e49e5c be3356c62 64a67b4a9 bf473b5f5d

Version	Changes	Date	Download link and SHA256
3.14.1	Minor bug fixes and enhancements.	August 22, 2024	Download version 3.14.1 sha256: f743a7b4b c82daa4b8 03c299439 0529997bb 57a4bb54d 1f5195ab2 8827283335
3.14.0	- Added support for the `tap-sleep` OpenVPN flag. - Updated the OpenVPN and OpenSSL libraries.	August 12, 2024	Download version 3.14.0 sha256: 812fb2f6d 263288c66 4d598f6bd 70e3f601d 11dcb89e6 3b281b0a9 6b96354516
3.13.0	Updated the OpenVPN and OpenSSL libraries.	July 29, 2024	Download version 3.13.0 sha256: c9cc896e8 1a7441184 0951e349e ed9384507 c53337fb7 03c5ec64d 522c29388b

Version	Changes	Date	Download link and SHA256
3.12.1	Fixed issue that prevents Windows client version 3.12.0 from establishing VPN connection for some users.	July 18, 2024	Download version 3.12.1 sha256: 5ed34aee6 c03aa281e 625acdbed 272896c67 046364a9e 5846ca697 e05dbfec08
3.12.0	- Automatically reconnect when local area network ranges change. - Removed automatic application focus when connected with SAML endpoints.	May 21, 2024	No longer supported
3.11.2	Resolved a SAML authentication issue with Chromium-based browsers since version 123.	April 11, 2024	Download version 3.11.2 sha256: 8ba258dd1 5bea3e861 adad108f8 a6d6d4bcd 8fe42cb9e f8bbc294e 72f365c7cc

Version	Changes	Date	Download link and SHA256
3.11.1	• Fixed a buffer overflow action that could potentially allow a local actor to execute arbitrary commands with elevated permissions. • Improved security posture.	February 16, 2024	Download version 3.11.1 sha256: fb67b60aa 837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	• Fixed a connectivity issue caused by Windows VMs. • Fixed connectivity issues for some LAN configurations. • Improved accessibility.	December 6, 2023	Download version 3.11.0 sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9
3.10.0	• Fixed a connectivity issue when NAT64 is enabled in the client network. • Fixed a connectivity issue when Hyper-V network adapters are installed on the client machine. • Minor bug fixes and enhancements.	August 24, 2023	Download version 3.10.0 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 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. - Automatically detect when updated versions of the client are available. - 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. - Fixed TAP Windows driver naming causing other driver names to be affected. - Fixed the banner message not being displayed when using federated authentication. - Fixed banner text display for longer text. - Enhanced security posture.	March 3, 2022	No longer supported
2.0.0	- Added support for banner text after new connection is established. - Removed ability to use pull-filter in relation to echo. i.e. pull-filter * echo - Minor bug fixes and enhancements.	January 20, 2022	No longer supported
1.3.7	- Fixed federated authentication connection attempt in some cases. - 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. • 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. • Minor bug fixes and enhancements.	August 4, 2021	No longer supported
1.3.3	• Added support for OpenVPN flags: inactive, pull-filter, route. • Fixed an issue that caused app crashes on disconnect or exit. • Fixed an issue with Active Directory usernames with backslash. • Fixed app crash when manipulating profile list outside of app. • Minor bug fixes and enhancements.	July 1, 2021	No longer supported
1.3.2	• Add IPv6 leak prevention, when it is configured. • 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. • Fixed local log retention to reduce disk usage. • Added support for 'route-ipv6' OpenVPN directive. • 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. • Fixed stale routes between connectio ns. • 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. • 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. • 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. • 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

These sections describe 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.

Requirements

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

- macOS Ventura (13.0), Sonoma (14.0), or Sequoia (15.0).
- x86_64 processor compatible.
- For Client VPN endpoints that use SAML-based federated authentication (single sign-on), the client reserves TCP ports 8096-8115 on your computer.

Note

If you are using Mac with an Apple silicon processor, you need to install Rosetta 2 to run the client software. For further details, see About the Rosetta Translation Environment on Apple's website.

Topics

- Connect to AWS Client VPN with an AWS provided client for macOS
- AWS Client VPN for macOS release notes

Connect to AWS Client VPN with an AWS provided client for macOS

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. If you want to connect to multiple profiles simultaneously, you'll need a configuration file for each profile.

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 and then select the configuration file that you received from your Client VPN administrator, and choose **Add Profile**.
6. If you want to create multiple connections, repeat the **Add Profile** steps for each configuration file you want to add. You can add as many profiles as you like, but you can only have up to five open connections.
7. In the **AWS VPN Client** window, choose the profile that you want to connect to, 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. Repeat this step for each profile connection you want to initiate, connecting up to five concurrent endpoints.

> **Note**
>
> If any profile you connect to conflicts with a currently open session, you won't be able to make the connection. Either choose a new connection or disconnect from the session causing the conflict.

8. To view statistics for a connection, choose **Connection** in the **AWS VPN client** window, choose **Show Details**, and then choose the connection you want to see details about.
9. To disconnect a connection, choose a connection in the **AWS VPN client** window, and then choose **Disconnect**. If you have multiple open connections, you must close each connection individually.

AWS Client VPN for macOS 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
5.2.1	• Added support for the ping-exit OpenVPN flag. • Updated the OpenSSL library. • Improved security posture. • Minor bug fixes and enhancements.	June 18, 2025	Download version 5.2.1 sha256: 906f77fbc a3334fbdc d1145dd6f 2725beab8 2a30b9b51 eafd1a25c 3fe7d669eb

Version	Changes	Date	Download link
5.2.0	- Minor enhancements. - Added support for Client Route Enforcement.	April 8, 2025	Download version 5.2.0 sha256: f062e971a 84e98d8a6 1caced3d7 f6be322c2 8dab02ec8 1194c0f9a 3e62bd8249
5.1.0	- Fixed an issue that caused AWS Client VPN version 5.0.x to automatically reconnect to VPN after an inactivity timeout disconnect. - Fixed an issue that prevented AWS Client VPN from establishing a VPN connection for configuration files with Windows-style line endings. - Minor bug fixes and enhancements.	March 17, 2025	Download version 5.1.0 sha256: ef7ff34ae 85a29f902 12514568c 93849ef6e 67f30b2c8 3ae1494d3 07f7650e10
5.0.3	Minor bug fixes and enhancements.	March 6, 2025	Download version 5.0.3 sha256: 8ce0f91ce 81c322cea d3ed27948 ddeda4d5a 61f5ed5a6 115ab8e18 f5d8963f6b

Version	Changes	Date	Download link
5.0.2	Fixed an issue that led to sporadic errors when choosing **Connect**.	February 17, 2025	[Download version 5.0.2] sha256: e81287746 08147e65b 14f992a4b 5a6d75364 6424fe3b6 8fab23181 0addac1f7c
5.0.1	Fixed an issue that prevented client version 5.0.0 from establishing a VPN connection for profile names that contained spaces.	January 22, 2025	[Download version 5.0.1] sha256: 7d9de8c89 154c9a99b fd56b1966 00a9a09eb 6a952cb10 a7b16d01b dbadb0e57a
5.0.0	• Added support for concurrent connections. • Updated the graphical user interface. • Minor bug fixes and enhancements.	January 21, 2025	[Download version 5.0.0] sha256:e9 c95ecdd6d 582e72e1a f0b05d03f e678f96b8 b1028b5f5 69f962902 943ecf02

Version	Changes	Date	Download link
4.1.0	Minor bug fixes and enhancements.	November 12, 2024	Download version 4.1.0 sha256:afe1ec8a6d7e2e1d618a6507f44a8c41db744fb55f94573e318d75bc5e96cd269
4.0.0	Minor enhancements.	September 25, 2024	Download version 4.0.0 sha256: ad574475a80b614499c97ae75612ef1ff905bb4aa1b5f7109420e80bf95aefcbd
3.12.1	Added support for the `mssfix` OpenVPN flag.	September 4, 2024	Download version 3.12.1 sha256: a5c31d3e0e8bf8937682805c9fff76ca9205875e009e949ad1b0532f449cee47

Version	Changes	Date	Download link
3.12.0	• Added support for the `tap-sleep` OpenVPN flag. • Updated the OpenVPN and OpenSSL libraries.	August 12, 2024	[Download version 3.12.0] sha256: 37de7736e 19da380b0 341f72227 1e2f5aca8 faeae33ac 18ecedafd 366d9e4b13
3.11.0	• Updated the OpenVPN and OpenSSL libraries.	July 29, 2024	[Download version 3.11.0] sha256: 44b5e6f84 788bf45dd b77871d74 3e09007e1 597555850 6221b8cae a81732848f
3.10.0	• Automatically reconnect when local area network ranges change. • Fixed a DNS restoration issue during network switch. • Removed automatic application focus when connected with SAML endpoints.	May 21, 2024	[Download version 3.10.0] sha256: 28bf26fa1 34b01ff12 703cf59ff fa4adba7c 44ceb793d ce4addd44 04e84287dd

Version	Changes	Date	Download link
3.9.2	- Resolved a SAML authentication issue with Chromium-based browsers since version 123. - Added support for macOS Sonoma. Deprecate support for macOS Big Sur. - Improved security posture.	April 11, 2024	Download version 3.9.2 sha256: 374467d99 1e8953b50 32e5b985c da80a0ea2 7fb5d5f23 cf16c556a 1568b0d480
3.9.1	- Fixed a buffer overflow action that could potentially allow a local actor to execute arbitrary commands with elevated permissions. - Fixed application update download progress bar. - Improved security posture.	February 16, 2024	Download version 3.9.1 sha256: 9bba4b27a 635e75038 703e2cf4c d814aa753 06179fac8 e500e2c7a f4e899e971
3.9.0	- Fixed connectivity issues for some LAN configurations. - Improved accessibility.	December 6, 2023	Download version 3.9.0 sha256: f0f6a5579 fe9431577 452e8aac0 7241c36cb 34c2b3f02 8dfdd07f4 1d00ff80d8

Version	Changes	Date	Download link
3.8.0	- Fixed a connectivity issue when NAT64 is enabled in the client network. - Minor bug fixes and enhancements.	August 24, 2023	Download version 3.8.0 sha256: d5a229b12 efa2e8862 7127a6dc2 7f5c6a1bc 9c426a8c4 66131ecbd bd6bbb4461
3.7.0	- Improved security posture.	August 3, 2023	Download version 3.7.0 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
3.4.0	- Improved security posture.	July 14, 2023	No longer supported
3.3.0	- Added support for macOS Ventura (13.0). - Minor bug fixes and enhancements.	April 27, 2023	No longer supported

Version	Changes	Date	Download link
3.2.0	• Added support for "verify-x509-name" OpenVPN flag. • Automatically detect when updated versions of the client are available. • 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. • Fixed issue for drive type detection. • Improved security posture.	May 23, 2022	No longer supported
3.0.0	• Fixed the banner message not being displayed when using federated authentication. • Fixed banner text display for longer text. • Enhanced security posture.	March 3, 2022	No longer supported.
2.0.0	• Added support for banner text after new connection is established. • Removed ability to use pull-filter in relation to echo. i.e. pull-filter * echo • Minor bug fixes and enhancements.	January 20, 2022	No longer supported.
1.4.0	• Added DNS server monitoring during connection. Settings will be re-configured if they do not match VPN settings. • Fixed federated authentication connection attempt in some cases. • Minor bug fixes and enhancements.	November 9, 2021	No longer supported.

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

Version	Changes	Date	Download link
1.3.1	• Added support for macOS Big Sur (10.16). • Fixed issue that removed DNS settings configured by other applications. • Fixed issue when using a non-valid certificate for mutual authentication causing connectivity issues. • Added support for 'route-ipv6' OpenVPN directive. • 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. • Added an error message for TLS handshake errors. • Fixed an uninstall bug that was affecting some users.	October 8, 2020	No longer supported.
1.2.2	Minor bug fixes and enhancements.	August 12, 2020	No longer supported.
1.2.1	• Added support for uninstalling application. • Minor bug fixes and enhancements.	July 1, 2020	No longer supported.

Version	Changes	Date	Download link
1.2.0	• Added support for SAML 2.0-based federated authentication. • 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. • Fixed an app crash issue caused by longer connections. • Fixed an MFA issue.	April 2, 2020	No longer supported.
1.1.0	• Added support for macOS DNS configuration. • Added support for OpenVPN static challenge echo functionality to hide or show the text displayed in the user interface. • 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

These sections describe installing the AWS provided client for Linux and then establishing establish a VPN connection using the AWS provided client. The AWS provided client for Linux does not support automatic updates. For the latest updates and downloads, see the the section called "Release notes".

Requirements for connecting to Client VPN with an AWS provided client for Linux

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

- Ubuntu 22.04 LTS (AMD64) or Ubuntu 24.04 LTS (AMD64 only)

For Client VPN endpoints that use SAML-based federated authentication (single sign-on) the client reserves TCP ports 8096-8115 on your computer.

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. If you want to connect to multiple profiles simultaneously, you'll need a configuration file for each profile.

Topics

Install the provided AWS Client VPN for Linux

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 following command to add the repository to your Ubuntu OS (version 22.04 and above):

```
echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
 ubuntu 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.

Connect to the provided AWS Client VPN for Linux

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. If you want to create multiple connections, repeat the **Add Profile** steps for each configuration file you want to add. You can add as many profiles as you like, but you can only have up to five open connections.
8. In the **AWS VPN Client** window, choose the profile that you want to connect to, 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. Repeat this step for each profile connection you want to initiate, connecting up to five concurrent endpoints.

   > **Note**
   >
   > If any profile you connect to conflicts with a currently open session, you won't be able to make the connection. Either choose a new connection or disconnect from the session causing the conflict.

9. To view statistics for a connection, choose **Connection** in the **AWS VPN client** window, choose **Show Details**, and then choose the connection you want to see details about.
10. To disconnect a connection, choose a connection in the **AWS VPN client** window, and then choose **Disconnect**. If you have multiple open connections, you must close each connection individually.

AWS Client VPN for Linux 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
5.2.0	• Minor enhancements. • Added support for Client Route Enforcement.	April 8, 2025	Download version 5.2.0 sha256: ef7189f085db30ef0c521adcdfec892075cb005c8e0014fdbcc590218509891f
5.1.0	• Fixed an issue that caused AWS Client VPN version 5.0.x to automatically reconnect to VPN after an inactivity timeout disconnect. • Minor bug fixes and enhancements.	March 17, 2025	Download version 5.1.0 sha256: 14f26c05b11b0cc484b08a8f8d20739de3d815c268db3bba9ac70c0e766b70ba
5.0.0	• Added support for multiple concurrent connections. • Updated the graphical user interface. • Minor bug fixes and enhancements.	January 21, 2025	Download version 5.0.0 sha256: 645126b5698cb550e9dc822e58ed899a5730d2e204f28f4023ec671915fdda0c

Version	Changes	Date	Download link
4.1.0	- Added support for Ubuntu 22.04 and 24.04. - Bug fixes.	November 12, 2024	Download version 4.1.0 sha256: 334d00222 458fbfe9d ade16c99f e97e9ebcb d51fff017 d0d6b1d1b 764e7af472
4.0.0	Minor enhancements.	September 25, 2024	Download version 4.0.0 sha256: c26327187 4217d7978 3fcca1820 25ace27dd bf8f9661b 56df48843 fa17922686
3.15.1	Added support for the `mssfix` OpenVPN flag.	September 4, 2024	Download version 3.15.1 sha256: ffb65c0bc 93e8d611c bce2deb6b 82f600e64 34e4d03c6 b44c53d61 a2efcaadc2

Version	Changes	Date	Download link
3.15.0	• Added support for the `tap-sleep` OpenVPN flag. • Updated the OpenVPN and OpenSSL libraries.	August 12, 2024	Download version 3.15.0 sha256: 5cf3eb08d e96821b0a d3d0c9317 4b2e30804 1d5490a3e db772dfd8 9a6d89d012
3.14.0	• Updated the OpenVPN and OpenSSL libraries.	July 29, 2024	Download version 3.14.0 sha256: bd2b401a1 ede6057d7 25a13c77e f92147a79 e0c5e0020 d379e44f3 19b5334f60
3.13.0	• Automatically reconnect when local area network ranges change.	May 21, 2024	Download version 3.13.0 sha256: e89f3bb7f c24c148e3 044b80777 4fcfe05e7 eae9e5518 63a38a2dc d7e0ac05f1

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 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. • Improved security posture.	February 16, 2024	Download version 3.12.1 sha256: 547c4ffd3 e35c54db8 e0b792aed 9de1510f6 f31a6009e 55b8af4f0 c2f5cf31d0
3.12.0	• Fixed connectivity issues for some LAN configurations.	December 19, 2023	Download version 3.12.0 sha256: 9b7398730 9f1dca196 0a322c5dd 86eec1568 ed270bfd2 5f78cc430 e3b5f85cc1

Version	Changes	Date	Download link
3.11.0	- Rollback for "Fixed connectivity issues for some LAN configurations". - Improved accessibility.	December 6, 2023	Download version 3.11.0 sha256: 86c0fa1bf 1c9719408 2835a739e c7f1c87e5 40194955f 414a35c67 9b94538970
3.10.0	- Fixed connectivity issues for some LAN configurations. - Improved accessibility.	December 6, 2023	Download version 3.10.0 sha256: e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51
3.9.0	- Fixed a connectivity issue when NAT64 is enabled in the client network. - Minor bug fixes and enhancements.	August 24, 2023	Download version 3.9.0 sha256: 6cde9cfff 82754119e 6a68464d4 bb350da3c b3e1ebf91 40dacf24e 4fd2197454

Version	Changes	Date	Download link
3.8.0	- Improved security posture.	August 3, 2023	Download version 3.8.0 sha256: 5fe479236 cc0a1940b a37fe168e 551096f8d ae4c68d45 560a164e4 1edea3e5bd
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
3.1.0	- Fixed issue for drive type detection. - Improved security posture.	May 23, 2022	No longer supported
3.0.0	- Fixed the banner message not being displayed when using federated authentication. - Fixed banner text display for longer text and specific character sequences. - Enhanced security posture.	March 3, 2022	No longer supported.

Version	Changes	Date	Download link
2.0.0	• Added support for banner text after new connection is established. • Removed ability to use pull-filter in relation to echo. i.e. pull-filter * echo • Minor bug fixes and enhancements.	January 20, 2022	No longer supported.
1.0.3	• Fixed federated authentication connection attempt in some cases. • 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. • Minor bug fixes and enhancements.	September 28, 2021	No longer supported.
1.0.1	• Enabled option to quit from Ubuntu application bar. • Added support for OpenVPN flags: inactive, pull-filter, route. • Minor bug fixes and enhancements.	August 4, 2021	No longer supported.
1.0.0	The initial release.	June 11, 2021	No longer supported.

Connect to an AWS Client VPN endpoint using an OpenVPN client

You can establish a connection to a Client VPN endpoint using common Open VPN client applications. Client VPN is supported on the following operating systems:

- **Windows**

  Use a certificate and private key from the Windows Certificate Store. Once you've generated the certificate and key you can establish an AWS Client connection using either the OpenVPN GUI client application or the OpenVPN GUI Connect Client. For the steps to create the certificate and key, see Establish a VPN connection using a certificate on Windows.
- **Android and iOS**

  Establish a VPN connection using the OpenVPN client application on an Android or iOS device. For more information see Client VPN connections on Android and iOS.
- **macOS**

  Establish a VPN connection using a configuration file for macOS-based Tunnelblick or for AWS Client VPN. For more information, see Establish a VPN connection on macOS.
- **Linux**

  Establish a VPN connection on Linux using either the **OpenVPN - Network Manager** interface or the OpenVPN application. To use the **OpenVPN - Network Manager** interface you'll first need to install the network manager module if it's not already installed. For more information, see Establish a VPN connection on Linux.

> **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. This includes any ARM-based architectures. If you are using a device with an ARM processor (such as Apple Silicon Macs or ARM-based Windows devices), you must use SAML-based VPN endpoints with the AWS provided client instead of OpenVPN clients.

Client applications

- Connect to an AWS Client VPN endpoint using a Windows client application
- AWS Client VPN connections on Android and iOS applications
- Connect to an AWS Client VPN endpoint using a macOS client application
- Connect to an AWS Client VPN endpoint using an OpenVPN client application

Connect to an AWS Client VPN endpoint using a Windows client application

These sections describe 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. If you want to connect to multiple profiles simultaneously, you'll need a configuration file for each profile.

For troubleshooting information, see Troubleshooting AWS Client VPN connections with Windows-based clients.

> ⚠ **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. This includes any ARM-based architectures. If you are using a device with an ARM processor (such as Apple Silicon Macs or ARM-based Windows devices), you must use SAML-based VPN endpoints with the AWS provided client instead of OpenVPN clients.

Tasks

- Use a certificate and establish an AWS Client VPN connection on Windows

Use a certificate and establish an AWS Client VPN connection on Windows

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 a certificate and establish a connection

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 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 website.

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

5. After you complete the configuration, use OpenVPN to establish a VPN connection by doing one of the following:

   - **Use the OpenVPN GUI client application**
     1. Start the OpenVPN client application.
     2. On the Windows taskbar, choose **Show/Hide icons**. Right-click **OpenVPN GUI**, and then 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 then choose **Connect**.

- **Use the OpenVPN GUI Connect Client**
  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**.

AWS Client VPN connections on Android and iOS applications

⚠ **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. This includes any ARM-based architectures. If you are using a device with an ARM processor (such as Apple Silicon Macs or ARM-based Windows devices), you must use SAML-based VPN endpoints with the AWS provided client instead of OpenVPN clients.

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 downloading and using the OpenVPN client application for iOS or Android, see the OpenVPN Connect User Guide 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. If you want to connect to multiple profiles simultaneously, you'll need a configuration file for each profile.

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

Connect to an AWS Client VPN endpoint using a macOS client application

These sections describe how to establish a VPN connection using the macOS-based VPN client, Tunnelblick or AWS Client VPN.

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. If you want to connect to multiple profiles simultaneously, you'll need a configuration file for each profile.

For troubleshooting information, see Troubleshooting AWS Client VPN connections with macOS clients.

⚠ **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. This includes any ARM-based architectures. If you are using a device with an ARM processor (such as Apple Silicon Macs or ARM-based Windows devices), you must use SAML-based VPN endpoints with the AWS provided client instead of OpenVPN clients.

Topics

Establish an AWS Client VPN connection on macOS

You can 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 using Tunnelblick

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**.

To establish a VPN connection using AWS Client VPN.

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 to an AWS Client VPN endpoint using an OpenVPN client application

These sections describe how to establish a VPN connection using either OpenVPN - Network Manager or OpenVPN.

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. If you want to connect to multiple profiles simultaneously, you'll need a configuration file for each profile.

For troubleshooting information, see Troubleshooting AWS Client VPN connections with Linux-based clients.

⚠ **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. This includes any ARM-based architectures. If you are using a device with an ARM processor (such as Apple Silicon Macs or ARM-based Windows devices), you must use SAML-based VPN endpoints with the AWS provided client instead of OpenVPN clients.

Topics

Establish an AWS Client VPN connection on Linux

Establish a VPN connection using the using either the Network Manager GUI on an Ubuntu computer or the OpenVPN application.

To establish a VPN connection using OpenVPN - Network Manager

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.

To establish a VPN connection using OpenVPN

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 AWS Client VPN connections

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

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 AWS provided client has an option for sending 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.

Send 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.

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

Troubleshooting AWS Client VPN connections with Windows-based clients

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

AWS provided client event logs

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
```

Troubleshooting 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
- VPN disconnects with a pop up message
- Client crash occurs on Dell PCs using Windows 10 or 11
- OpenVPN GUI

- OpenVPN connect client
- Unable to resolve DNS
- Missing PKI alias

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*.

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
```

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**.

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).

Troubleshooting AWS Client VPN connections with macOS clients

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.

AWS provided client event logs

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.

```
/var/log/AWSVPNClient/AcvcHelperErrLog.txt
/var/log/AWSVPNClient/AcvcHelperOutLog.txt
```

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

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

Troubleshooting topics

- Client cannot connect
- Client is stuck in a reconnecting state
- Client cannot create profile
- Helper tool is required error
- Tunnelblick
- Cipher algorithm 'AES-256-GCM' not found
- Connection stops responding and resets
- Extended key usage (EKU)
- Expired certificate
- OpenVPN

- Cannot resolve DNS

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*.

Helper tool is required error

Problem

You get the following error when you try to connect the VPN.

```
AWS VPN Client Helper Tool is required to establish the connection.
```

Solution

See the following article on AWS re:Post. AWS VPN Client - Helper tool is required error

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*.

Troubleshooting AWS Client VPN connections with Linux-based clients

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 event logs

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/
```

For example, you can check the following log files to find errors in the DNS up/down scripts that cause the connection to fail:

- `/var/log/aws-vpn-client/configure-dns-up.log`
- `/var/log/aws-vpn-client/configure-dns-down.log`

DNS queries go to a default nameserver

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*.

Troubleshooting common AWS Client VPN 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 (5.2.1) for macOS released	See release notes for details.	June 18, 2025
AWS provided client (5.2.2) for Windows released	See release notes for details.	June 2, 2025
AWS provided client (5.2.1) for Windows released	See release notes for details.	April 21, 2025
AWS provided client (5.2.0) for macOS released	See release notes for details.	April 8, 2025
AWS provided client (5.2.0) for Windows released	See release notes for details.	April 8, 2025
AWS provided client (5.2.0) for Ubuntu released	See release notes for details.	April 8, 2025
AWS provided client (5.1.0) for macOS released	See release notes for details.	March 17, 2025
AWS provided client (5.1.0) for Windows released	See release notes for details.	March 17, 2025
AWS provided client (5.1.0) for Ubuntu released	See release notes for details.	March 17, 2025
Removed support for macOS Monterey and added support for macOS Sonoma (14.0)	See Client VPN for macOS Requirements for details.	March 12, 2025
Removed support for both Ubuntu 18.0.4 (LTS) and	See Client VPN for Linux Requirements for details.	March 12, 2025

Ubuntu 20.04 LTS (AMD64 only)		
AWS provided client (5.0.3) for macOS released	See release notes for details.	March 6, 2025
AWS provided client (5.0.2) for Windows released	See release notes for details.	February 24, 2025
AWS provided client (5.0.2) for macOS released	See release notes for details.	February 17, 2025
AWS provided client (5.0.1) for Windows released	See release notes for details.	January 30, 2025
AWS provided client (5.0.1) for macOS released	See release notes for details.	January 22, 2025
The AWS provided client now supports up to five concurrent connections	See Support for concurrent connections using an AWS provided client for details.	January 21, 2025
AWS provided client (5.0.0) for macOS released	See release notes for details.	January 21, 2025
AWS provided client (5.0.0) for Windows released	See release notes for details.	January 21, 2025
AWS provided client (5.0.0) for Ubuntu released	See release notes for details.	November 12, 2024
AWS provided client (4.1.0) for macOS released	See release notes for details.	November 12, 2024
AWS provided client (4.1.0) for Windows released	See release notes for details.	November 12, 2024
AWS provided client (4.1.0) for Ubuntu released	See release notes for details.	November 12, 2024

AWS provided client (4.0.0) for macOS released	See release notes for details.	September 25, 2024
AWS provided client (4.0.0) for Windows released	See release notes for details.	September 25, 2024
AWS provided client (4.0.0) for Ubuntu released	See release notes for details.	September 25, 2024
AWS provided client (3.15.1) for Ubuntu released	See release notes for details.	September 4, 2024
AWS provided client (3.14.2) for Windows released	See release notes for details.	September 4, 2024
AWS provided client (3.12.1) for macOS released	See release notes for details.	September 4, 2024
AWS provided client (3.14.1) for Windows released	See release notes for details.	August 22, 2024
AWS provided client (3.15.0) for Ubuntu released	See release notes for details.	August 12, 2024
AWS provided client (3.14.0) for Windows released	See release notes for details.	August 12, 2024
AWS provided client (3.12.0) for macOS released	See release notes for details.	August 12, 2024
AWS provided client (3.14.0) for Ubuntu released	See release notes for details.	July 29, 2024
AWS provided client (3.13.0) for Windows released	See release notes for details.	July 29, 2024
AWS provided client (3.11.0) for macOS released	See release notes for details.	July 29, 2024

AWS provided client (3.12.1) for Windows released	See release notes for details.	July 18, 2024
AWS provided client (3.13.0) for Ubuntu released	See release notes for details.	May 21, 2024
AWS provided client (3.12.0) for Windows released	See release notes for details.	May 21, 2024
AWS provided client (3.10.0) for macOS released	See release notes for details.	May 21, 2024
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