AWS Client VPN

User Guide

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.

Components

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

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

Additional resources

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

Getting started with Client VPN

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

For more information about creating a Client VPN endpoint, see the AWS Client VPN Administrator Guide.

Topics

Prerequisites

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

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

Step 1: Get a VPN client application

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

The AWS provided client is a supported on Windows and macOS. You can download the client at AWS Client VPN download.

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

Step 2: Get the Client VPN endpoint configuration file

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

Step 3: Connect to the VPN

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

- Connect using the AWS provided client (p. 4)
- Connect using an OpenVPN client (p. 11)

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.

Connect using the AWS provided client

The following topics provide steps for connecting to a Client VPN endpoint using the AWS provided client.

The AWS provided client does not support automatic updates. You can download the latest version at AWS Client VPN download.

The AWS provided client is currently supported on Windows and macOS only.

Topics

Windows

The following procedure shows how to establish a VPN connection using the AWS provided client for Windows. You can download and install the client at AWS Client VPN download.

Requirements

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

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

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

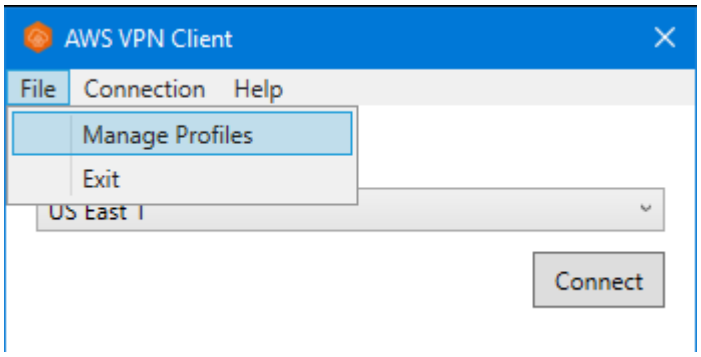
Before you begin, ensure that your Client VPN administrator has created a Client VPN endpoint and provided you with the Client VPN endpoint configuration file.

Connecting

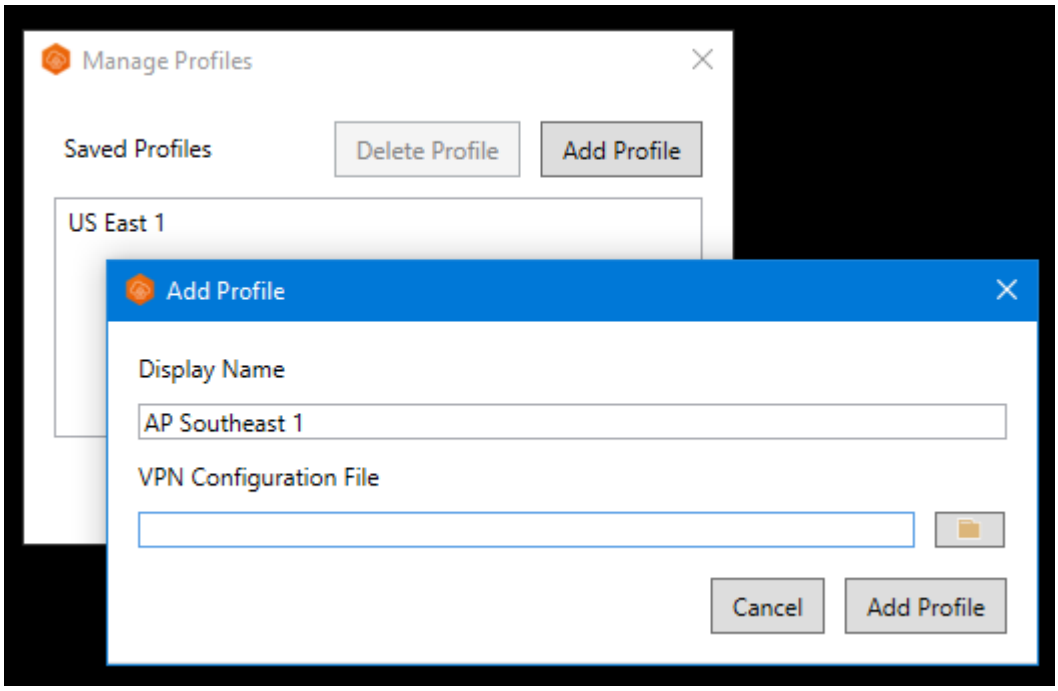
Before you begin, ensure that you've read the requirements (p. 4). The AWS provided client is also referred to as *AWS VPN Client* in the following steps.

To connect using the AWS provided client for Windows

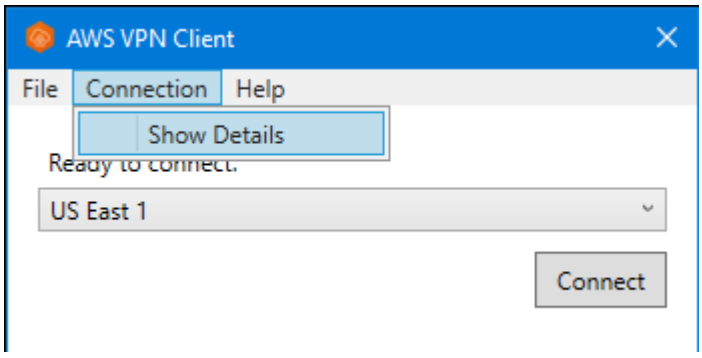
1. Open the **AWS VPN Client** app.
2. Choose **File**, **Manage Profiles**.



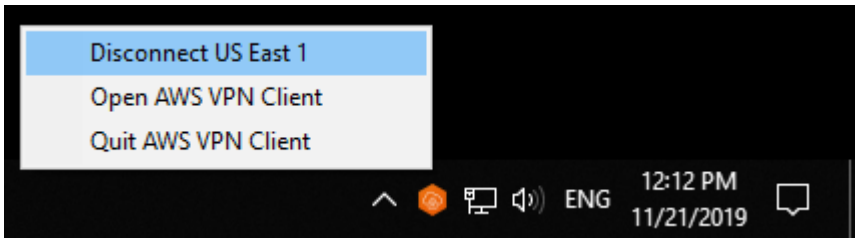
3. Choose **Add Profile**.



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



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



Troubleshooting

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

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

For troubleshooting information, see Troubleshooting your Client VPN connection (p. 16).

macOS

The following procedure shows how to establish a VPN connection using the AWS provided client for macOS. You can download and install the client at AWS Client VPN download.

Requirements

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

- 64-bit macOS High Sierra (10.13), Mojave (10.14), or Catalina (10.15)

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

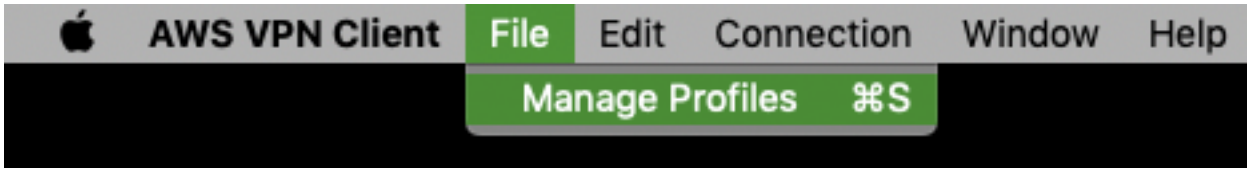
Before you begin, ensure that your Client VPN administrator has created a Client VPN endpoint and provided you with the Client VPN endpoint configuration file.

Connecting

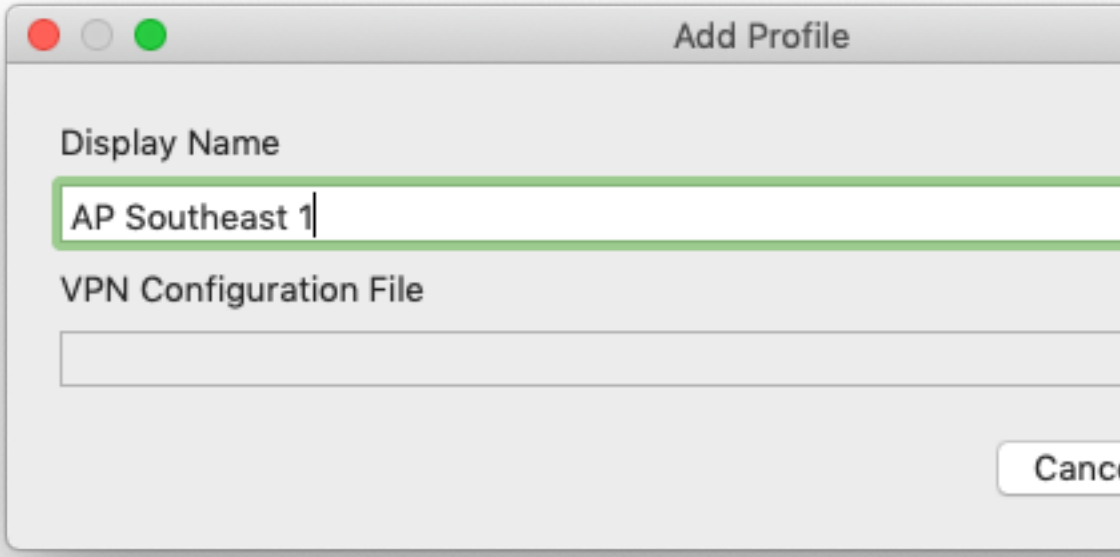
Before you begin, ensure that you've read the requirements (p. 6). The AWS provided client is also referred to as *AWS VPN Client* in the following steps.

To connect using the AWS provided client for macOS

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

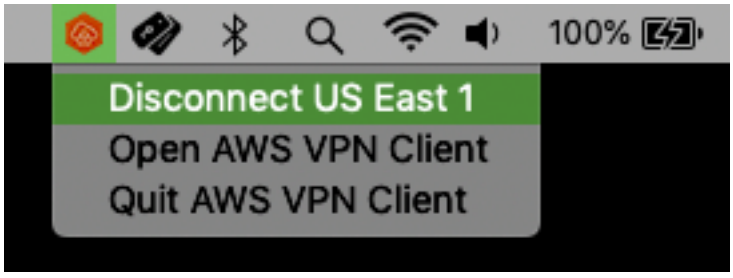


3. Choose **Add Profile**.
4. For **Display Name**, enter a name for the profile.



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

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



Troubleshooting

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

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

For troubleshooting information, see Troubleshooting your Client VPN connection (p. 16).

Release notes for the AWS provided client

The following tables contain the release notes and download links for the current and previous versions of the AWS provided client.

You can also download the latest version of the client at AWS Client VPN download.

Platform: Windows

Version	Changes	Date	Download link
1.2.5	• Added support for comments in the OpenVPN configuration • Added an error message for TLS handshake errors	October 8, 2020	Download version 1.2.5
1.2.4	Minor bug fixes and enhancements.	September 1, 2020	Download version 1.2.4
1.2.3	Roll back changes in version 1.2.2.	August 20, 2020	Download version 1.2.3
1.2.1	Minor bug fixes and enhancements.	July 1, 2020	Download version 1.2.1
1.2.0	• Added support for SAML 2.0-based federated authentication • Deprecated support for the Windows 7 platform	May 19, 2020	Download version 1.2.0
1.1.1	Minor bug fixes and enhancements.	April 21, 2020	Download version 1.1.1
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	Download version 1.1.0

Version	Changes	Date	Download link
1.0.0	The initial release of the AWS provided client.	February 4, 2020	Download version 1.0.0

Platform: macOS

Version	Changes	Date	Download link
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	Download version 1.2.3
1.2.2	Minor bug fixes and enhancements.	August 12, 2020	Download version 1.2.2
1.2.1	• Added support for uninstalling application • Minor bug fixes and enhancements	July 1, 2020	Download version 1.2.1
1.2.0	• Added support for SAML 2.0-based federated authentication • Added support for macOS Catalina (10.15)	May 19, 2020	Download version 1.2.0
1.1.2	Minor bug fixes and enhancements.	April 21, 2020	Download version 1.1.2
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	Download version 1.1.1
1.1.0	• Added support for macOS DNS configuration • Added support for OpenVPN static challenge echo functionality to hide or show the text	March 9, 2020	Download version 1.1.0

Version	Changes	Date	Download link
	displayed in the user interface • Minor bug fixes and enhancements		
1.0.0	The initial release of the AWS provided client.	February 4, 2020	Download version 1.0.0

Supported OpenVPN directives

The AWS provided client supports the following OpenVPN directives:

- client
- dev
- proto
- remote
- remote-random-hostname
- resolv-retry
- nobind
- persist-key
- persist-tun
- remote-cert-tls
- cipher
- verb
- ca
- reneg-sec
- cert
- key
- auth-user-pass
- connect-retry
- static-challenge
- tun-mtu
- tun-mtu-extra

Connect using an OpenVPN client

The following topics provide steps for connecting to a VPN using common VPN client applications.

Topics

Windows

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

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

For troubleshooting information, see Windows troubleshooting (p. 16).

> **Important**
> If the Client VPN endpoint has been configured to use SAML-based federated authentication, you must use the AWS-provided client (p. 4) to connect.

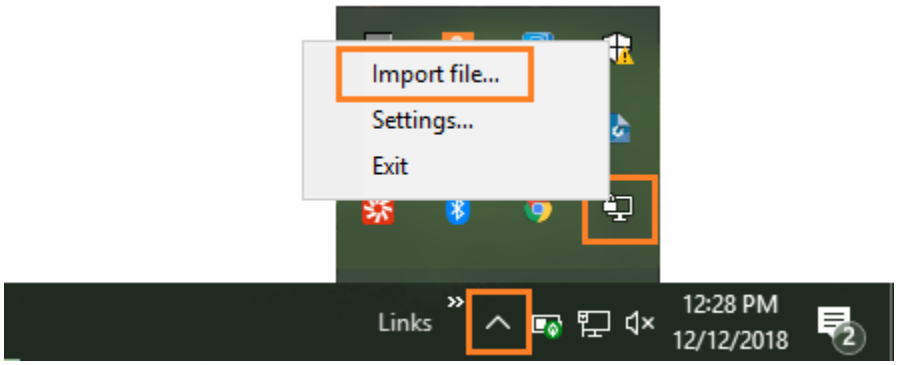
OpenVPN GUI

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

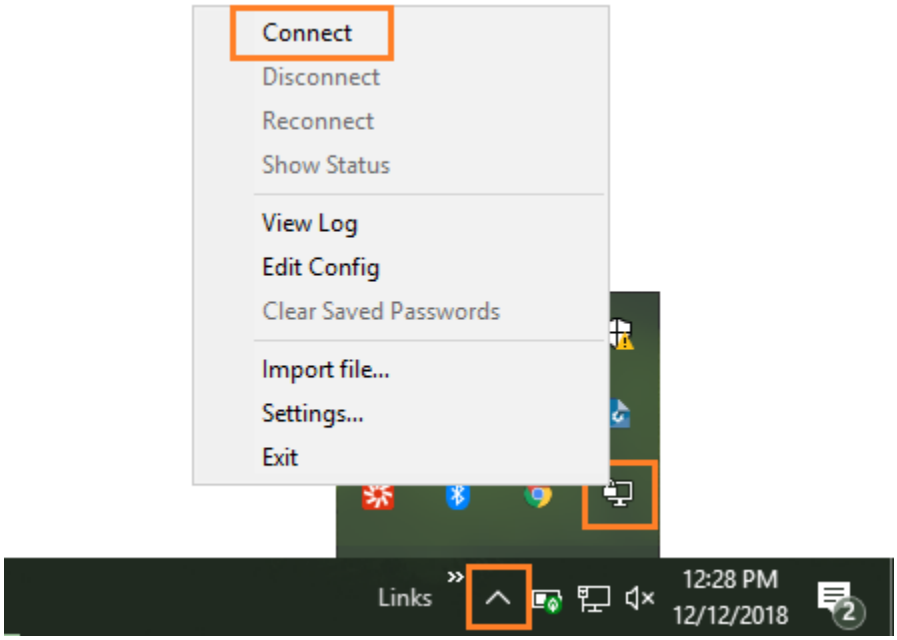
> **Note**
> For information about the OpenVPN client application, see Community Downloads on the OpenVPN website.

To establish a VPN connection

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



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



OpenVPN Connect Client

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

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

To establish a VPN connection

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

Android and iOS

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

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

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

To establish a VPN connection

1. Start the OpenVPN client application and choose **OVPN Profile**.

2. Select the configuration file you received from your Client VPN administrator and choose **Import**. If you received the configuration file as a .ovpn attachment in a mail, you can open the file using OpenVPN.

3. Choose **Add**.

4. Choose the toggle next to the OpenVPN profile.

5. To view the connection log file, choose Log File (top-right corner).

MacOS

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

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

For troubleshooting information, see MacOS troubleshooting (p. 21).

Important
If the Client VPN endpoint has been configured to use SAML-based federated authentication, you must use the AWS-provided client (p. 4) to connect.

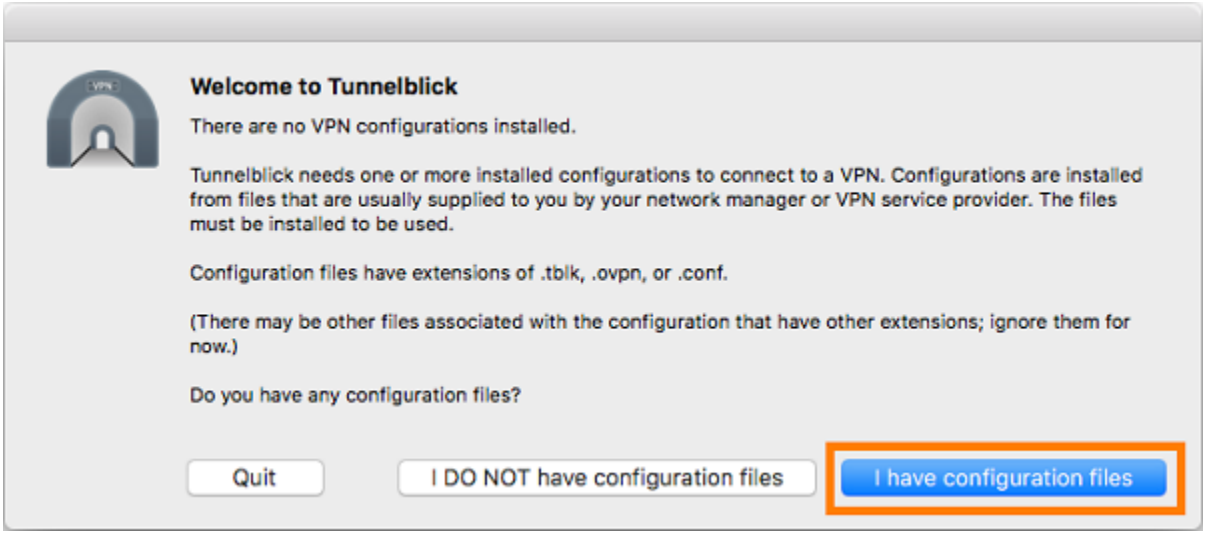
Tunnelblick

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

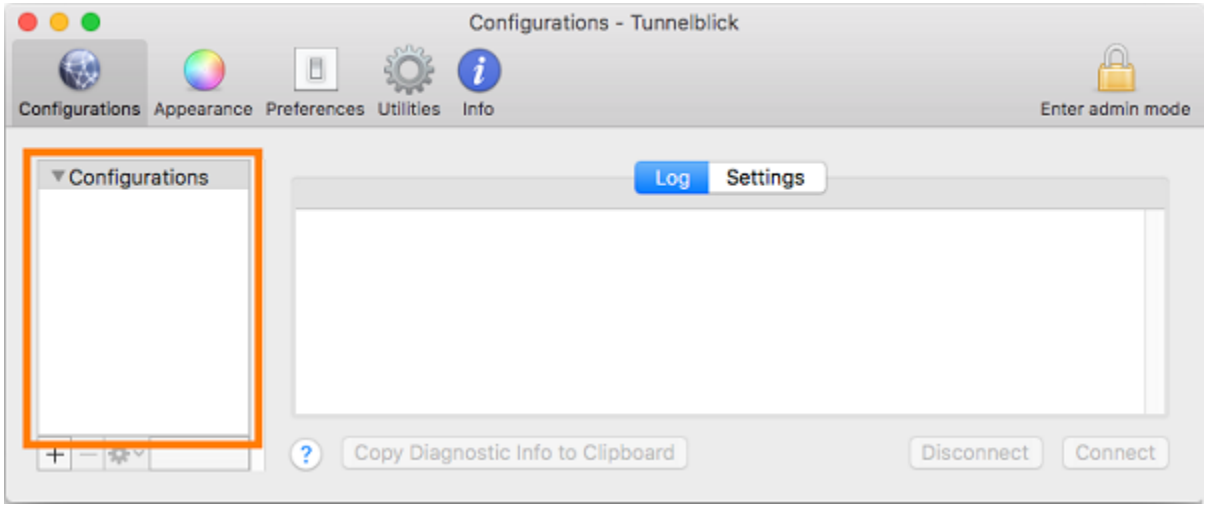
Note
For more information about the Tunnelblick client application for macOS, see the Tunnelblick documentation on the Tunnelblick website.

To establish a VPN connection

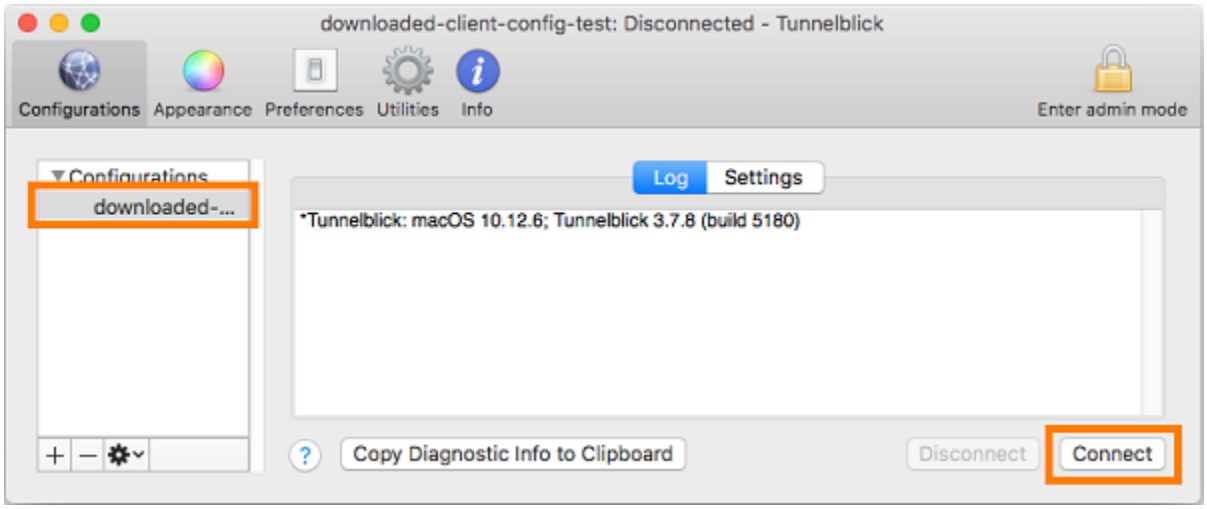
1. Start the Tunnelblick client application and choose **I have configuration files**.



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



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



OpenVPN Connect Client

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

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

To establish a VPN connection

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

Ubuntu

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

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

For troubleshooting information, see Ubuntu troubleshooting (p. 26).

Important
If the Client VPN endpoint has been configured to use SAML-based federated authentication, you must use the AWS-provided client (p. 4) to connect.

OpenVPN - Network Manager

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

To establish a VPN connection

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

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

2. Go to **Settings**, **Network**.
3. Choose the plus symbol (**+**) next to **VPN**, and then choose **Import from file...**.
4. Navigate to the configuration file that you received from your VPN administrator and choose **Open**.
5. In the **Add VPN** window, choose **Add**.
6. Start the connection by enabling the toggle next to the VPN profile that you added.

OpenVPN

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

To establish a VPN connection

1. Install OpenVPN using the following command.

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

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

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

Troubleshooting your Client VPN connection

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

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*.

Windows troubleshooting

The following are problems you might have when using Windows-based clients to connect to a Client VPN endpoint.

Topics

AWS provided client

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

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

The following types of logs are available:

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

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

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

Topics

Client cannot connect

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 invalid.

Solution

Check that there are no 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:

- The configuration file contains the correct client key and certificate. For more information, see Export Client Configuration in the *AWS Client VPN Administrator Guide*.
- 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:

- You 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

Check 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 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 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*.

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).

Certificate error

Problem

The connection fails with the following error.

```
VERIFY ERROR: depth=3, error=unable to get issuer certificate: C=US, ST=Arizona,
 L=Scottsdale, O=Starfield Technologies, Inc., CN=Starfield Services Root Certificate
 Authority - G2
```

Cause

Certificate Authority (CA) chain information is missing in the Client VPN configuration file provided by Amazon, which causes validation to fail.

This issue can occur for certificates generated by AWS Certificate Manager.

Solution

Open the Client VPN configuration file (the .ovpn file) and replace the third certificate in the <ca> section in with the following certificate, and then save the file.

```
-----BEGIN CERTIFICATE-----
MIID7zCCAtegAwIBAgIBADANBgkqhkiG9w0BAQsFADCBmDELMAkGA1UEBhMCVVMx
EDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxJTAjBgNVBAoT
HFN0YXJmaWVsZCBUZWNobm9sb2dpZXMsIEluYy4xOzA5BgNVBAMTMlN0YXJmaWVs
ZCBTZXJ2aWNlcyBSb290IENlcnRpZmljYXRlIEF1dGhvcml0eSAtIEcyMB4XDTA5
MDkwMTAwMDAwMFoXDTM3MTIzMTIzNTk1OVowgZgxCzAJBgNVBAYTAlVTMRAwDgYD
VQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY290dHNkYWxlMSUwIwYDVQQKExxTdGFy
ZmllbGQgVGVjaG5vbG9naWVzLCBJbmMuMTswOQYDVQQDEzJTdGFyZmllbGQgU2Vy
dmljZXMgUm9vdCBDZXJ0aWZpY2F0ZSBBdXRob3JpdHkgLSBHMjCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBANUMOsQq+U7i9b4Zl1+OiFOxHz/Lz58gE20p
OsgPfTz3a3Y4Y9k2YKibXlwAgLIvWX/2h/klQ4bnaRtSmpDhcePYLQ1Ob/bISdm2
8xpWriu2dBTrz/sm4xq6HZYuajtYlIlHVv8loJNwU4PahHQUw2eeBGg6345AWh1K
Ts9DkTvnVtYAcMtS7nt9rjrnvDH5RfbCYM8TWQIrgMw0R9+53pBlbQLPLJGmpufe
hRhJfGZOozptqbXuNC66DQO4M99H67FrjSXZm86B0UVGMpZwh94CDklDhbZsc7tk
6mFBrMnUVN+HL8cisibMn1lUaJ/8viovxFUcdUBgF4UCVTmLfwUCAwEAAaNCMEAw
DwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFJxfAN+q
AdcwKziIorhtSpzyEZGDMA0GCSqGSIb3DQEBCwUAA4IBAQBLNqaEd2ndOxmfZyMI
bw5hyf2E3F/YNoHN2BtBLZ9g3ccaaNnRbobhiCPPE95Dz+I0swSdHynVv/heyNXB
ve6SbzJ08pGCL72CQnqtKrcgfU28elUSwhXqvfdqlS5sdJ/PHLTyxQGjhdByPq1z
qwubdQxtRbeOlKyWN7Wg0I8VRw7j6IPdj/3vQQF3zCepYoUz8jcI73HPdwbeyBkd
iEDPfUYd/x7H4c7/I9vG+o1VTqkC50cRRj70/b17KSa7qWFiNyi2LSr2EIZkyXCn
0q23KXB56jzaYyWf/Wi3MOxw+3WKt21gZ7IeyLnp2KhvAotnDU0mV3HaIPzBSlCN
sSi6
-----END CERTIFICATE-----
```

Import the updated configuration file to the OpenVPN Connect Client software and connect to the Client VPN endpoint.

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
```

Certificate error

Problem

The connection fails with the following error.

```
VERIFY ERROR: depth=3, error=unable to get issuer certificate: C=US, ST=Arizona,
 L=Scottsdale, O=Starfield Technologies, Inc., CN=Starfield Services Root Certificate
 Authority - G2
```

Cause

CA chain information is missing in the Client VPN configuration file provided by Amazon, which causes validation to fail.

This issue can occur for certificates generated by AWS Certificate Manager.

Solution

See the solution for Certificate error (p. 19).

MacOS troubleshooting

The following are problems you might have when using MacOS-based clients to connect to a Client VPN endpoint.

Topics

AWS provided client

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

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

The following types of logs are available:

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

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

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

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

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

Topics

- Client cannot create profile (p. 22)

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 invalid.

Solution

Check that there are no 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:

- The configuration file contains the correct client key and certificate. For more information, see Export Client Configuration in the *AWS Client VPN Administrator Guide*.
- 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:

- You 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

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

Client cannot create profile

Problem

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

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

Cause

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

Solution

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

Tunnelblick

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

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

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

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

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

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

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

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

Cipher algorithm 'AES-256-GCM' not found

Problem

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

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

Cause

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

Solution

Choose a compatible OpenVPN version by doing the following:

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

Connection stops responding and resets

Problem

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

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

Cause

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

Solution

Request a new configuration file from your Client VPN administrator.

Invalid certificate

Problem

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

```
VERIFY ERROR: depth=1, error=unable to get issuer certificate: C=US, O=Let's Encrypt,
 CN=Let's Encrypt Authority X3
OpenSSL: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed
TLS_ERROR: BIO read tls_read_plaintext error
TLS Error: TLS object -> incoming plaintext read error
TLS Error: TLS handshake failed
Fatal TLS error (check_tls_errors_co), restarting
SIGUSR1[soft,tls-error] received, process restarting
```

Cause

The issuer certificate is not valid in the .ovpn configuration file.

Solution

Open the Client VPN configuration file (the .ovpn file) in a text editor, and add the following certificate to the file.

```
-----BEGIN CERTIFICATE-----
MIIDSjCCAjKgAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/
MSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMT
DkRTVCBSb290IENBIFgzMB4XDTAwMDkzMDIxMTIxOVoXDTIxMDkzMDE0MDExNVow
PzEkMCIGA1UEChMbRGlnaXRhbCBTaWduYXR1cmUgVHJ1c3QgQ28uMRcwFQYDVQQD
Ew5EU1QgUm9vdCBDQSBYMzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AN+v6ZdQCINXtMxiZfaQguzH0yxrMMpb7NnDfcdAwRgUi+DoM3ZJKuM/IUmTrE4O
rz5Iy2Xu/NMhD2XSKtkyj4zl93ewEnu1lcCJo6m67XMuegwGMoOifooUMM0RoOEq
OLl5CjH9UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGiifSKOeDNoJjj4XLh7dIN9b
xiqKqy69cK3FCxolkHRyxXtqqzTWMIn/5WgTe1QLyNau7Fqckh49ZLOMxt+/yUFw
7BZy1SbsOFU5Q9D8/RhcQPGX69Wam40dutolucbY38EVAjqr2m7xPi71XAicPNaD
aeQQmxkqtilX4+U9m5/wAl0CAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBVghYkQMA0GCSqG
```

```
SIb3DQEBBQUAA4IBAQCjGiybFwBcqR7uKGY3Or+Dxz9LwwmglSBd49lZRNI+DT69
ikugdB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADq1cEmv8uXr
AvHRAosZy5Q6XkjEGB5YGV8eAlrwDPGxrancWYaLbumR9YbK+rlmM6pZW87ipxZz
R8srzJmwN0jP41ZL9c8PDHIyh8bwRLtTcm1D9SZImlJnt1ir/md2cXjbDaJWFBM5
JDGFoqgCWjBH4d1QB7wCCZAA62RjYJsWvIjJEubSfZGL+T0yjWW06XyxV3bqxbYo
Ob8VZRzI9neWagqNdwvYkQsEjgfbKbYK7p2CNTUQ
-----END CERTIFICATE-----
```

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

Ensure 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*.

Ubuntu troubleshooting

The following are problems you might have when using Ubuntu-based clients to connect to a Client VPN endpoint, including the following:

- OpenVPN through Network Manager (GUI)
- OpenVPN (command line)

Ensure that you are running the latest version of these clients.

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

```
/var/log/syslog
```

You can enable advanced debugging using the OpenVPN command line client. Open the Client VPN configuration file (the .ovpn file) and replace verb 3 with verb 5 or higher, and specify the log location, as shown in the following example.

```
log /var/log/vpn-log.log
```

Run the OpenVPN client using the `--log` option, as shown in the following example.

```
sudo openvpn --log vpn-log.log --config test1.ovpn
```

DNS server configuration

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
   ```

Cannot resolve DNS

Problem

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

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

Cause

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

Solution

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

Common problems

The following are common problems 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 that the firewall rules on your computer are not blocking inbound or outbound TCP or UDP traffic on ports 443 or 1194. Ask your Client VPN administrator to verify the following information:

- The firewall rules for the Client VPN endpoint do not block TCP or UDP traffic on ports 443 or 1194.
- The configuration file contains the correct client key and certificate. For more information, see Export Client Configuration in the *AWS Client VPN Administrator Guide*.

- 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.

update-history-change	update-history-description	update-history-date
AWS provided client	You can use the AWS provided client to connect to a Client VPN endpoint.	February 4, 2020
Initial release (p. 30)	This release introduces AWS Client VPN.	December 18, 2018