



Panduan Pengguna

AWS Klien VPN



AWS Klien VPN: Panduan Pengguna

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

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan kekayaan masing-masing pemiliknya, yang mungkin atau mungkin tidak berafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apa itu AWS KlienVPN?	1
VPNKomponen klien	1
Sumber daya tambahan untuk mengkonfigurasi Klien VPN	1
Memulai dengan Klien VPN	2
Prasyarat untuk menggunakan Klien VPN	2
Langkah 1: Dapatkan aplikasi VPN klien	2
Langkah 2: Dapatkan file konfigurasi VPN titik akhir Klien	3
Langkah 3: Connect ke VPN	3
Unduh Klien VPN	4
Connect menggunakan klien yang AWS disediakan	6
Windows	7
Persyaratan	8
Connect menggunakan klien	8
Catatan rilis	9
macOS	16
Persyaratan	16
Connect menggunakan klien	17
Catatan rilis	18
Linux	26
Persyaratan untuk menghubungkan ke Klien VPN dengan klien yang AWS disediakan untuk Linux	26
Instal klien	26
Connect menggunakan klien	28
Catatan rilis	28
Connect menggunakan VPN klien Terbuka	34
Windows	34
Gunakan sertifikat	35
Gunakan Terbuka VPN GUI	36
Gunakan Klien Open VPN Connect	36
Android dan iOS	37
macOS	38
Buat koneksi menggunakan Tunnelblick	38
Connect menggunakan Open VPN Connect Client	39
Linux	39

Connect menggunakan Open VPN - Network Manager	40
Connect menggunakan Open VPN	40
Pemecahan Masalah	42
Pemecahan masalah VPN titik akhir klien untuk administrator	42
Kirim log diagnostik ke AWS Support klien yang AWS disediakan	42
Mengirim log diagnostik	17
Pemecahan masalah Windows	44
AWS klien yang disediakan	44
Buka VPN GUI	50
Buka klien VPN koneksi	50
Pemecahan masalah macOS	51
AWS klien yang disediakan	52
Tunnelblick	54
Buka VPN	57
Pemecahan masalah Linux	58
AWS klien yang disediakan	44
Buka VPN (baris perintah)	60
Buka VPN melalui Network Manager (GUI)	61
Masalah umum	62
TLSNegosiasi kunci gagal	62
Riwayat dokumen	63
.....	Ixix

Apa itu AWS KlienVPN?

AWS Klien VPN adalah VPN layanan berbasis klien terkelola yang memungkinkan Anda mengakses AWS sumber daya dan sumber daya dengan aman di jaringan lokal Anda.

Panduan ini menyediakan langkah-langkah untuk membuat VPN koneksi ke VPN titik akhir Klien menggunakan aplikasi klien di perangkat Anda.

VPNKomponen klien

Berikut ini adalah komponen kunci untuk menggunakan AWS KlienVPN.

- VPNTitik akhir Klien — VPN Administrator Klien Anda membuat dan mengonfigurasi titik VPN akhir Klien di AWS Administrator Anda mengontrol jaringan dan sumber daya mana yang dapat Anda akses saat membuat VPN koneksi.
- VPNaplikasi klien — Aplikasi perangkat lunak yang Anda gunakan untuk terhubung ke VPN titik akhir Klien dan membuat VPN koneksi yang aman.
- File konfigurasi VPN titik akhir klien — File konfigurasi yang disediakan untuk Anda oleh VPN administrator Klien Anda. File tersebut mencakup informasi tentang VPN titik akhir Klien dan sertifikat yang diperlukan untuk membuat VPN koneksi. Anda memuat file ini ke dalam aplikasi VPN klien pilihan Anda.

Sumber daya tambahan untuk mengkonfigurasi Klien VPN

Jika Anda VPN administrator Klien, lihat [Panduan AWS Client VPN Administrator](#) untuk informasi selengkapnya tentang membuat dan mengonfigurasi titik VPN akhir Klien.

Memulai dengan AWS Client VPN

Sebelum Anda dapat membuat VPN sesi, VPN administrator Klien Anda harus membuat dan mengkonfigurasi VPN titik akhir Klien. Administrator Anda mengontrol jaringan dan sumber daya yang dapat Anda akses saat Anda membuat VPN sesi. Anda kemudian menggunakan aplikasi VPN klien untuk terhubung ke VPN titik akhir Klien dan membuat VPN koneksi yang aman.

Jika Anda seorang administrator yang perlu membuat VPN titik akhir Klien, lihat [Panduan AWS Client VPN Administrator](#).

Topik

- [Prasyarat untuk menggunakan Klien VPN](#)
- [Langkah 1: Dapatkan aplikasi VPN klien](#)
- [Langkah 2: Dapatkan file konfigurasi VPN titik akhir Klien](#)
- [Langkah 3: Connect ke VPN](#)
- [Unduh AWS Client VPN dari portal swalayan](#)

Prasyarat untuk menggunakan Klien VPN

Untuk membuat VPN koneksi, Anda harus memiliki yang berikut:

- Mengakses ke internet
- Perangkat yang didukung
- Untuk VPN endpoint Klien yang menggunakan autentikasi federasi SAML berbasis (single sign-on), salah satu browser berikut:
 - Apple Safari
 - Google Chrome
 - Microsoft Edge
 - Mozilla Firefox

Langkah 1: Dapatkan aplikasi VPN klien

Anda dapat terhubung ke VPN titik akhir Klien dan membuat VPN koneksi menggunakan klien yang AWS disediakan atau aplikasi klien VPN berbasis Terbuka lainnya.

Klien yang AWS disediakan didukung pada Windows, macOS, Ubuntu 18.04LTS, dan Ubuntu 20.04.LTS

Anda dapat mengunduh VPN aplikasi Klien melalui salah satu dari dua metode, tergantung pada apakah administrator membuat file konfigurasi titik akhir untuk aplikasi:

- Jika administrator Anda tidak menyiapkan file konfigurasi titik akhir, unduh dan instal klien dari [VPNUnduhan AWS Klien](#). Setelah mengunduh dan menginstal aplikasi, lanjutkan [the section called “Langkah 2: Dapatkan file konfigurasi VPN titik akhir Klien”](#) untuk mendapatkan file konfigurasi titik akhir dari administrator Anda.
- Jika administrator Anda telah mengkonfigurasi file konfigurasi titik akhir, Anda dapat mengunduh VPN aplikasi Klien, bersama dengan file konfigurasi, dari portal swalayan. Untuk langkah-langkah mengunduh file klien dan konfigurasi dari portal swalayan, lihat [the section called “Unduh Klien VPN”](#). Setelah mengunduh dan menginstal aplikasi dan file, buka [the section called “Langkah 3: Connect ke VPN”](#).

Atau, unduh dan instal aplikasi VPN klien Terbuka pada perangkat tempat Anda ingin membuat VPN koneksi.

Langkah 2: Dapatkan file konfigurasi VPN titik akhir Klien

Anda mendapatkan file konfigurasi VPN titik akhir Klien dari administrator Anda. File konfigurasi mencakup informasi tentang VPN titik akhir Klien dan sertifikat yang diperlukan untuk membuat VPN koneksi.

Atau, jika VPN administrator Klien Anda telah mengonfigurasi portal layanan mandiri untuk VPN titik akhir Klien, Anda dapat mengunduh versi terbaru dari klien yang AWS disediakan dan versi terbaru dari file konfigurasi VPN titik akhir Klien sendiri. Untuk informasi selengkapnya, lihat [Unduh AWS Client VPN dari portal swalayan](#).

Langkah 3: Connect ke VPN

Impor file konfigurasi VPN titik akhir Klien ke klien yang AWS disediakan atau ke aplikasi VPN klien Terbuka Anda dan sambungkan ke file. VPN Untuk langkah-langkah untuk menyambung keVPN, termasuk mengimpor file konfigurasi titik akhir, lihat topik berikut:

- [Connect ke VPN endpoint Klien menggunakan klien yang AWS disediakan](#)

- [Connect ke VPN endpoint Klien menggunakan klien Terbuka VPN](#)

Untuk VPN titik akhir Klien yang menggunakan otentikasi Active Directory, Anda akan diminta untuk memasukkan nama pengguna dan kata sandi Anda. Jika otentikasi multi-faktor (MFA) telah diaktifkan untuk direktori, Anda juga akan diminta untuk memasukkan kode Anda. MFA

Untuk VPN titik akhir Klien yang menggunakan otentikasi federasi SAML berbasis (sistem masuk tunggal), klien yang AWS disediakan membuka jendela browser di komputer Anda. Anda akan diminta untuk memasukkan kredensi perusahaan Anda sebelum dapat terhubung ke titik akhir Klien. VPN

Unduh AWS Client VPN dari portal swalayan

Portal swalayan adalah halaman web yang memungkinkan Anda mengunduh versi terbaru dari klien yang AWS disediakan dan versi terbaru dari file konfigurasi VPN titik akhir Klien. Jika administrator VPN titik akhir Klien Anda telah mengkonfigurasi file konfigurasi untuk klien VPN Klien, Anda dapat mengunduh dan menginstal VPN aplikasi Klien itu bersama dengan file konfigurasi, dari portal ini.

Note

Jika Anda seorang administrator dan ingin mengonfigurasi portal layanan mandiri, lihat [VPNTitik akhir klien di Panduan AWS Client VPN Administrator](#).

Sebelum memulai, Anda harus memiliki ID dari VPN titik akhir Klien. Administrator VPN endpoint Klien Anda dapat memberi Anda ID, atau dapat memberi Anda portal layanan mandiri URL yang menyertakan ID.

Untuk mengakses portal layanan mandiri

1. Buka portal swalayan di <https://self-service.clientvpn.amazonaws.com/>, atau gunakan URL yang diberikan kepada Anda oleh administrator Anda.
2. Jika diperlukan, masukkan ID VPN titik akhir Klien, misalnya, `cvpn-endpoint-0123456abcd123456`. Pilih Berikutnya.
3. Masukkan nama pengguna dan kata sandi Anda dan pilih Masuk. Ini adalah nama pengguna dan kata sandi yang sama yang Anda gunakan untuk terhubung ke VPN titik akhir Klien.
4. Di portal layanan mandiri, Anda dapat melakukan hal berikut:

- Unduh versi terbaru dari file konfigurasi klien untuk VPN titik akhir Klien.
- Unduh versi terbaru dari klien yang AWS disediakan untuk platform Anda.

Connect ke VPN endpoint Klien menggunakan klien yang AWS disediakan

Anda dapat terhubung ke VPN titik akhir Klien menggunakan klien yang AWS disediakan. Klien yang AWS disediakan didukung pada Windows, macOS, Ubuntu 18.04LTS, dan Ubuntu 20.04. LTS

Klien

- [AWS Client VPN untuk Windows](#)
- [AWS Client VPN untuk macOS](#)
- [AWS Client VPN untuk Linux](#)

VPN Arahan terbuka

Klien AWS yang disediakan mendukung VPN arahan Terbuka berikut:

- auth-federasi
- auth-nocache
- auth-coba lagi
- auth-user-pass
- ca
- sertifikat
- cipher
- klien
- sambungkan-coba lagi
- connect-retry-max
- cryptoapicert
- dev
- tipe dev-
- dhcp-opisi
- ifconfig-ipv6
- tidak aktif

- keepalive
- kunci
- bangsawan
- kunci persisten
- persist-tun
- ping
- ping-restart
- proto
- tarik
- saringan tarik
- rcvbuf
- terpencil
- remote-cert-tls
- remote-random-hostname
- reneg-sec
- selesaikan-coba lagi
- rute
- rute-ipv6
- server-poll-timeout
- tantangan statis
- tun-mtu
- tun-mtu-extra
- kata kerja
- verify-x509-nama

AWS Client VPN untuk Windows

Bagian ini menjelaskan cara membuat VPN koneksi menggunakan klien yang AWS disediakan untuk Windows. Anda dapat mengunduh dan menginstal klien di [VPNUnduhan AWS Klien](#). Klien yang AWS disediakan tidak mendukung pembaruan otomatis.

Persyaratan

Untuk menggunakan klien yang AWS disediakan untuk Windows, berikut ini diperlukan:

- Windows 10 atau Windows 11 (sistem operasi 64-bit, prosesor x64)
- .NETFramework 4.7.2 atau lebih tinggi

Klien menyimpan TCP port 8096 di komputer Anda. Untuk VPN titik akhir Klien yang menggunakan otentikasi federasi SAML berbasis (sistem masuk tunggal), klien mencadangkan port 35001. TCP

Sebelum memulai, pastikan bahwa VPN administrator Klien Anda telah [membuat VPN titik akhir Klien](#) dan memberi Anda file [konfigurasi VPN titik akhir Klien](#).

Topik

- [Connect to Client VPN dengan klien yang AWS disediakan untuk Windows](#)
- [AWS Client VPN untuk catatan rilis Windows](#)

Connect to Client VPN dengan klien yang AWS disediakan untuk Windows

Sebelum memulai, pastikan Anda telah membaca [persyaratan](#). Klien yang AWS disediakan juga disebut sebagai AWS VPN Klien dalam langkah-langkah berikut.

Untuk terhubung menggunakan klien yang AWS disediakan untuk Windows

1. Buka aplikasi AWS VPN Klien.
2. Pilih File, Mengelola Profil.
3. Pilih Tambah profil.
4. Untuk Nama tampilan, masukkan nama untuk profil.
5. Untuk File VPN Konfigurasi, telusuri ke lalu pilih file konfigurasi yang Anda terima dari VPN administrator Klien, lalu pilih Tambahkan Profil.
6. Di jendela AWS VPN Klien, pastikan bahwa profil Anda dipilih, lalu pilih Hubungkan. Jika VPN titik akhir Klien telah dikonfigurasi untuk menggunakan otentikasi berbasis kredensial, Anda akan diminta untuk memasukkan nama pengguna dan kata sandi.
7. Untuk melihat statistik koneksi Anda, pilih Koneksi, Tampilkan Detail.
8. Untuk memutuskan hubungan, di jendela AWS VPN Klien, pilih Putuskan Hubungan. Atau, pilih ikon klien pada taskbar Windows, kemudian pilih Putuskan Hubungan.

AWS Client VPN untuk catatan rilis Windows

Tabel berikut berisi catatan rilis dan tautan unduhan untuk versi Windows saat ini dan sebelumnya.
AWS Client VPN

Note

Kami terus memberikan kegunaan dan perbaikan keamanan dengan setiap rilis. Kami sangat menyarankan Anda menggunakan versi terbaru untuk setiap platform. Versi sebelumnya mungkin dipengaruhi oleh masalah kegunaan dan/atau keamanan. Lihat catatan rilis untuk detailnya.

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
3.14.0	<ul style="list-style-type: none"> Menambahkan dukungan untuk VPN bendera tap-sleep Terbuka. Memperbarui SSL perpustakaan Terbuka VPN dan Terbuka. 	Agustus 12, 2024	Unduh versi 3.14.0 sha256:81 2fb2f6d26 3288c664d 598f6bd70 e3f601d11 dcb89e63b 281b0a96b 96354516
3.13.0	Memperbarui SSL perpustakaan Terbuka VPN dan Terbuka.	Juli 29, 2024	Unduh versi 3.13.0 sha256: c9cc896e8 1a7441184 0951e349e ed9384507 c53337fb7 03c5ec64d 522c29388b

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
3.12.1	Memperbaiki masalah yang mencegah klien Windows versi 3.12.0 membuat VPN koneksi untuk beberapa pengguna.	Juli 18, 2024	Unduh versi 3.12.1 sha256:5e d34aee6c0 3aa281e62 5acdbed27 2896c6c67 046364a9e 5846ca697 e05dbfec08
3.12.0	<ul style="list-style-type: none"> Sambungkan kembali secara otomatis ketika rentang jaringan area lokal berubah. Fokus aplikasi otomatis dihapus saat terhubung dengan SAML titik akhir. 	21 Mei 2024	Tidak lagi didukung
3.11.2	Menyelesaikan masalah SAML otentikasi dengan browser berbasis Chromium sejak versi 123.	April 11, 2024	Unduh versi 3.11.2 sha256:8b a258dd15b ea3e861ad ad108f8a6 d6d4bcd8f e42cb9ef8 bbc294e72 f365c7cc

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
3.11.1	<ul style="list-style-type: none"> • Memperbaiki tindakan buffer overflow yang berpotensi memungkinkan aktor lokal menjalankan perintah arbitrer dengan izin yang ditinggikan. • Postur keamanan yang ditingkatkan. 	Februari 16, 2024	Unduh versi 3.11.1 sha256: fb67b60aa 837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	<ul style="list-style-type: none"> • Memperbaiki masalah konektivitas yang disebabkan oleh WindowsVMs. • Memperbaiki masalah konektivitas untuk beberapa LAN konfigurasi. • Peningkatan aksesibilitas. 	6 Desember 2023	Unduh versi 3.11.0 sha256:9b 6b7def99d 76c59a97b 067b6a73b dc6ee1c6b 89a206328 6f542e96b 32df5ae9
3.10.0	<ul style="list-style-type: none"> • Memperbaiki masalah konektivitas saat NAT64 diaktifkan di jaringan klien. • Memperbaiki masalah konektivitas saat adaptor jaringan Hyper-V diinstal pada mesin klien. • Perbaiki bug minor dan peningkatan. 	24 Agustus 2023	Unduh versi 3.10.0 sha256: d46721aad 40ccb816f 163e406c3 66ff03b11 20abbb43a 20607e06d 3b1fa8667f

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
3.9.0	Postur keamanan yang ditingkatkan.	3 Agustus 2023	Unduh versi 3.9.0 sha256: de9a3800e a23491555 40bd32bba e472404c6 36d8d8d82 67a0e1fb2 173a8aae21ed
3.8.0	Postur keamanan yang ditingkatkan.	15 Juli 2023	Tidak lagi didukung
3.7.0	Menggulung kembali perubahan dari 3.6.0.	15 Juli 2023	Tidak lagi didukung
3.6.0	Postur keamanan yang ditingkatkan.	14 Juli 2023	Tidak lagi didukung
3.5.0	Perbaikan bug minor dan peningkatan.	3 April 2023	Tidak lagi didukung
3.4.0	Menggulung kembali perubahan dari versi 3.3.0.	Maret 28, 2023	Tidak lagi didukung
3.3.0	Perbaikan bug minor dan peningkatan.	Maret 17, 2023	Tidak lagi didukung
3.2.0	<ul style="list-style-type: none"> • Ditambahkan dukungan untuk “verify-x 509-name” Buka bendera. VPN • Secara otomatis mendeteksi ketika versi klien yang diperbarui tersedia. • Ditambahkan kemampuan untuk secara otomatis menginstal versi klien baru bila tersedia. 	23 Januari 2023	Tidak lagi didukung
3.1.0	Postur keamanan yang ditingkatkan.	23 Mei 2022	Tidak lagi didukung

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
3.0.0	<ul style="list-style-type: none"> • Menambahkan dukungan Windows 11. • Memperbaiki penamaan driver TAP Windows yang menyebabkan nama driver lain terpengaruh. • Memperbaiki pesan banner yang tidak ditampilkan saat menggunakan otentikasi federasi. • Tampilan teks banner tetap untuk teks yang lebih panjang. • Postur keamanan yang ditingkatkan. 	3 Maret 2022	Tidak lagi didukung
2.0.0	<ul style="list-style-type: none"> • Ditambahkan dukungan untuk teks banner setelah koneksi baru dibuat. • Kemampuan yang dihapus untuk menggunakan saringan tarik dalam kaitannya dengan gema. yaitu filter* pull-filter* echo • Perbaiki bug minor dan peningkatan. 	20 Januari 2022	Tidak lagi didukung
1.3.7	<ul style="list-style-type: none"> • Memperbaiki upaya koneksi otentikasi federasi dalam beberapa kasus. • Perbaiki bug minor dan peningkatan. 	November 8, 2021	Tidak lagi didukung
1.3.6	<ul style="list-style-type: none"> • Menambahkan dukungan untuk Open VPN flags: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, . server-poll-timeout • Perbaiki bug minor dan peningkatan. 	September 20, 2021	Tidak lagi didukung
1.3.5	Patch untuk menghapus file log windows besar.	16 Agustus 2021	Tidak lagi didukung

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
1.3.4	<ul style="list-style-type: none">• Ditambahkan dukungan untuk Open VPN flag: dhcp-option.• Perbaiki bug minor dan peningkatan.	4 Agustus 2021	Tidak lagi didukung
1.3.3	<ul style="list-style-type: none">• Menambahkan dukungan untuk VPN bendera Terbuka: tidak aktif, filter tarik, rute.• Perbaiki masalah yang menyebabkan aplikasi terganggu saat koneksi terputus atau keluar.• Perbaiki masalah dengan nama pengguna Direktori Aktif dengan garis miring terbalik.• Perbaiki kerusakan aplikasi saat memanipulasi daftar profil di luar aplikasi.• Perbaiki bug minor dan penyempurnaan.	1 Juli 2021	Tidak lagi didukung
1.3.2	<ul style="list-style-type: none">• Tambahkan pencegahan IPv6 kebocoran, ketika dikonfigurasi.• Perbaiki potensi gangguan ketika Anda menggunakan opsi Tampilkan Detail di bawah Koneksi.	12 Mei 2021	Tidak lagi didukung

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
1.3.1	<ul style="list-style-type: none"> • Penambahan dukungan untuk beberapa sertifikat klien dengan subjek yang sama. Sertifikat kedaluwarsa akan diabaikan. • Perbaiki retensi log lokal dalam mengurangi penggunaan disk. • Ditambahkan dukungan untuk 'route-ip v6' Open direktif. VPN • Perbaiki bug minor dan peningkatan. 	5 April 2021	Tidak lagi didukung
1.3.0	Penambahan fitur dukungan seperti pelaporan kesalahan, pengiriman log diagnostik, dan analitik.	8 Maret 2021	Tidak lagi didukung
1.2.7	<ul style="list-style-type: none"> • Ditambahkan dukungan untuk cryptoapi cert Open direktif. VPN • Perbaiki rute usang antar koneksi. • Perbaiki bug minor dan penyempurnaan. 	25 Februari 2021	Tidak lagi didukung
1.2.6	Perbaiki bug minor dan penyempurnaan.	26 Oktober 2020	Tidak lagi didukung
1.2.5	<ul style="list-style-type: none"> • Ditambahkan dukungan untuk komentar dalam VPN konfigurasi Open. • Menambahkan pesan kesalahan untuk kesalahan TLS jabat tangan. 	8 Oktober 2020	Tidak lagi didukung
1.2.4	Perbaiki bug minor dan penyempurnaan.	1 September 2020	Tidak lagi didukung
1.2.3	Kembali ke perubahan dalam versi 1.2.2.	20 Agustus 2020	Tidak lagi didukung

Versi	Perubahan	Tanggal	Tautan unduhan dan SHA256
1.2.1	Perbaiki bug minor dan penyempurnaan.	1 Juli 2020	Tidak lagi didukung
1.2.0	<ul style="list-style-type: none"> Menambahkan dukungan untuk SAMLotentikasi federasi berbasis 2.0. Dukungan tidak lagi digunakan pada platform Windows 7. 	19 Mei 2020	Tidak lagi didukung
1.1.1	Perbaiki bug minor dan penyempurnaan.	21 April 2020	Tidak lagi didukung
1.1.0	<ul style="list-style-type: none"> Menambahkan dukungan untuk fungsi gema tantangan VPN statis Terbuka untuk menyembunyikan atau menampilkan teks yang ditampilkan di antarmuka pengguna. Perbaiki bug minor dan peningkatan. 	9 Maret 2020	Tidak lagi didukung
1.0.0	Rilis awal.	4 Februari 2020	Tidak lagi didukung

AWS Client VPN untuk macOS

Bagian ini menjelaskan cara membuat VPN koneksi menggunakan klien yang AWS disediakan untuk macOS. Anda dapat mengunduh dan menginstal klien di [VPNunduhan AWS Klien](#). Klien yang AWS disediakan tidak mendukung pembaruan otomatis.

Persyaratan

Untuk menggunakan klien yang AWS disediakan untuk macOS, berikut ini diperlukan:

- macOS Monterey (12.0), Ventura (13.0), atau Sonoma (14.0).
- prosesor x86_64 kompatibel.
- Klien menyimpan TCP port 8096 di komputer Anda.

- Untuk VPN titik akhir Klien yang menggunakan otentikasi federasi SAML berbasis (sistem masuk tunggal), klien mencadangkan port 35001. TCP

Note

Jika Anda menggunakan Mac dengan prosesor silikon Apple, Anda perlu menginstal [Rosetta 2](#) untuk menjalankan perangkat lunak klien. Untuk detail lebih lanjut, lihat [Tentang Lingkungan Terjemahan Rosetta di situs](#) web Apple.

Topik

- [Connect to Client VPN dengan klien yang AWS disediakan untuk macOS](#)
- [AWS Client VPN untuk catatan rilis macOS](#)

Connect to Client VPN dengan klien yang AWS disediakan untuk macOS

Sebelum memulai, pastikan bahwa VPN administrator Klien Anda telah [membuat VPN titik akhir Klien](#) dan memberi Anda file [konfigurasi VPN titik akhir Klien](#).

Juga, pastikan bahwa Anda telah membaca [persyaratan](#). Klien yang AWS disediakan juga disebut sebagai AWS VPN Klien dalam langkah-langkah berikut.

Untuk terhubung menggunakan klien yang AWS disediakan untuk macOS

1. Buka aplikasi AWS VPN Klien.
2. Pilih File, Mengelola Profil.
3. Pilih Tambah profil.
4. Untuk Nama tampilan, masukkan nama untuk profil.
5. Untuk File VPN Konfigurasi, telusuri ke file konfigurasi yang Anda terima dari VPN administrator Klien Anda. Pilih Buka.
6. Pilih Tambah profil.
7. Di jendela AWS VPN Klien, pastikan bahwa profil Anda dipilih, lalu pilih Hubungkan. Jika VPN titik akhir Klien telah dikonfigurasi untuk menggunakan otentikasi berbasis kredensial, Anda akan diminta untuk memasukkan nama pengguna dan kata sandi.
8. Untuk melihat statistik koneksi Anda, pilih Koneksi, Tampilkan Detail.

9. Untuk memutuskan hubungan, di jendela AWS VPN Klien, pilih Putuskan Hubungan. Atau, pilih ikon klien pada bilah menu, lalu pilih Putuskan sambungan < your-profile-name >.

AWS Client VPN untuk catatan rilis macOS

Tabel berikut berisi catatan rilis dan tautan unduhan untuk versi macOS saat ini dan sebelumnya.
AWS Client VPN

Note

Kami terus memberikan kegunaan dan perbaikan keamanan dengan setiap rilis. Kami sangat menyarankan Anda menggunakan versi terbaru untuk setiap platform. Versi sebelumnya dapat dipengaruhi oleh kegunaan dan/atau masalah keamanan. Lihat catatan rilis untuk detailnya.

Versi	Perubahan	Tanggal	Tautan unduh
3.12.0	<ul style="list-style-type: none"> Menambahkan dukungan untuk VPN bendera tap-sleep Terbuka. Memperbarui SSL perpustakaan Terbuka VPN dan Terbuka. 	Agustus 12, 2024	Unduh versi 3.12.0 sha256:37 de7736e19 da380b034 1f722271e 2f5aca8fa eae33ac18 ecedafd36 6d9e4b13
3.11.0	<ul style="list-style-type: none"> Memperbarui SSL perpustakaan Terbuka VPN dan Terbuka. 	Juli 29, 2024	Unduh versi 3.11.0 sha256:44 b5e6f8478 8bf45ddb7 7871d743e 09007e159 755585062

Versi	Perubahan	Tanggal	Tautan unduh
			21b8caea8 1732848f
3.10.0	<ul style="list-style-type: none"> Sambungkan kembali secara otomatis ketika rentang jaringan area lokal berubah. Memperbaiki masalah DNS restorasi selama sakelar jaringan. Fokus aplikasi otomatis dihapus saat terhubung dengan SAML titik akhir. 	21 Mei 2024	Unduh versi 3.10.0 sha256:28 bf26fa134 b01ff12703cf59fffa 4adba7c44 ceb793dce 4addd4404 e84287dd
3.9.2	<ul style="list-style-type: none"> Menyelesaikan masalah SAML otentikasi dengan browser berbasis Chromium sejak versi 123. Menambahkan dukungan untuk macOS Sonoma. Menanggalkan dukungan untuk macOS Big Sur. Postur keamanan yang ditingkatkan. 	April 11, 2024	Unduh versi 3.9.2 sha256:37 4467d991e 8953b5032 e5b985cda 80a0ea27f b5d5f23cf 16c556a15 68b0d480
3.9.1	<ul style="list-style-type: none"> Memperbaiki tindakan buffer overflow yang berpotensi memungkinkan aktor lokal menjalankan perintah arbitrer dengan izin yang ditinggikan. Bilah kemajuan unduhan pembaruan aplikasi tetap. Postur keamanan yang ditingkatkan. 	Februari 16, 2024	Unduh versi 3.9.1 sha256:9b ba4b27a63 5e7503870 3e2cf4cd8 14aa75306 179fac8e5 00e2c7af4 e899e971

Versi	Perubahan	Tanggal	Tautan unduh
3.9.0	<ul style="list-style-type: none"> • Memperbaiki masalah konektivitas untuk beberapa LAN konfigurasi. • Peningkatan aksesibilitas. 	6 Desember 2023	Unduh versi 3.9.0 sha256: f0f6a5579 fe9431577 452e8aac0 7241c36cb 34c2b3f02 8dfdd07f4 1d00ff80d8
3.8.0	<ul style="list-style-type: none"> • Memperbaiki masalah konektivitas saat NAT64 diaktifkan di jaringan klien. • Perbaiki bug minor dan peningkatan. 	24 Agustus 2023	Unduh versi 3.8.0 sha256: d5a229b12 efa2e8862 7127a6dc2 7f5c6a1bc 9c426a8c4 66131ecbd bd6bbb4461
3.7.0	<ul style="list-style-type: none"> • Postur keamanan yang ditingkatkan. 	3 Agustus 2023	Unduh versi 3.7.0 sha256:4a 34b25b482 33b02d610 7638a3868 f7e419a84 d20bb4989 f7b394aae 9a9de00a
3.6.0	<ul style="list-style-type: none"> • Postur keamanan yang ditingkatkan. 	15 Juli 2023	Tidak lagi didukung
3.5.0	<ul style="list-style-type: none"> • Perubahan yang digulirkan kembali dari 3.4.0. 	15 Juli 2023	Tidak lagi didukung

Versi	Perubahan	Tanggal	Tautan unduh
3.4.0	<ul style="list-style-type: none"> • Postur keamanan yang ditingkatkan. 	14 Juli 2023	Tidak lagi didukung
3.3.0	<ul style="list-style-type: none"> • Menambahkan dukungan untuk macOS Ventura (13.0). • Perbaiki bug minor dan peningkatan. 	27 April 2023	Tidak lagi didukung
3.2.0	<ul style="list-style-type: none"> • Ditambahkan dukungan untuk “verify-x 509-name” Buka bendera. VPN • Secara otomatis mendeteksi ketika versi klien yang diperbarui tersedia. • Ditambahkan kemampuan untuk secara otomatis menginstal versi klien baru bila tersedia. 	23 Januari 2023	Tidak lagi didukung
3.1.0	<ul style="list-style-type: none"> • Menambahkan dukungan untuk macOS Monterey. • Memperbaiki masalah untuk deteksi tipe drive. • Postur keamanan yang ditingkatkan. 	23 Mei 2022	Tidak lagi didukung
3.0.0	<ul style="list-style-type: none"> • Memperbaiki pesan banner yang tidak ditampilkan saat menggunakan otentikasi federasi. • Tampilan teks banner tetap untuk teks yang lebih panjang. • Postur keamanan yang ditingkatkan. 	3 Maret 2022	Tidak lagi didukung.
2.0.0	<ul style="list-style-type: none"> • Ditambahkan dukungan untuk teks banner setelah koneksi baru dibuat. • Kemampuan yang dihapus untuk menggunakan saringan tarik dalam kaitannya dengan gema. yaitu filter* pull-filter* echo • Perbaiki bug minor dan peningkatan. 	20 Januari 2022	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
1.4.0	<ul style="list-style-type: none">• Menambahkan pemantauan DNS server selama koneksi. Pengaturan akan dikonfigurasi ulang jika tidak cocok dengan VPN pengaturan.• Memperbaiki upaya koneksi otentikasi federasi dalam beberapa kasus.• Perbaiki bug minor dan peningkatan.	November 9, 2021	Tidak lagi didukung.
1.3.5	<ul style="list-style-type: none">• Menambahkan dukungan untuk Open VPN flags: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout• Perbaiki bug minor dan peningkatan.	September 20, 2021	Tidak lagi didukung.
1.3.4	<ul style="list-style-type: none">• Ditambahkan dukungan untuk Open VPN flag: dhcp-option.• Perbaiki bug minor dan peningkatan.	4 Agustus 2021	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
1.3.3	<ul style="list-style-type: none">• Menambahkan dukungan untuk VPN bendera Terbuka: tidak aktif, filter tarik, rute.• Perbaiki masalah pada nama file konfigurasi dengan spasi atau Unicode.• Perbaiki masalah yang menyebabkan aplikasi terganggu saat koneksi terputus atau keluar.• Perbaiki masalah dengan nama pengguna Direktori Aktif dengan garis miring terbalik.• Perbaiki kerusakan aplikasi saat memanipulasi daftar profil di luar aplikasi.• Perbaiki bug minor dan penyempurnaan.	1 Juli 2021	Tidak lagi didukung.
1.3.2	<ul style="list-style-type: none">• Tambahkan pencegahan IPv6 kebocoran, ketika dikonfigurasi.• Perbaiki potensi gangguan ketika Anda menggunakan opsi Tampilkan Detail di bawah Koneksi.• Tambahkan rotasi log daemon.	12 Mei 2021	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
1.3.1	<ul style="list-style-type: none"> • Penambahan dukungan untuk macOS Big Sur (10.16). • Memperbaiki masalah yang menghapus DNS pengaturan yang dikonfigurasi oleh aplikasi lain. • Perbaiki masalah saat menggunakan sertifikat non-valid untuk autentikasi bersama yang menyebabkan masalah konektivitas. • Ditambahkan dukungan untuk 'route-ip v6' Open direktif. VPN • Perbaiki bug minor dan peningkatan. 	5 April 2021	Tidak lagi didukung.
1.3.0	Penambahan fitur dukungan seperti pelaporan kesalahan, pengiriman log diagnostik, dan analitik.	8 Maret 2021	Tidak lagi didukung.
1.2.5	Perbaiki bug minor dan penyempurnaan.	25 Februari 2021	Tidak lagi didukung.
1.2.4	Perbaiki bug minor dan penyempurnaan.	26 Oktober 2020	Tidak lagi didukung.
1.2.3	<ul style="list-style-type: none"> • Ditambahkan dukungan untuk komentar dalam VPN konfigurasi Open. • Menambahkan pesan kesalahan untuk kesalahan TLS jabat tangan. • Perbaiki bug penghapusan instalasi yang memengaruhi beberapa pengguna. 	8 Oktober 2020	Tidak lagi didukung.
1.2.2	Perbaiki bug minor dan penyempurnaan.	12 Agustus 2020	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
1.2.1	<ul style="list-style-type: none"> • Penambahan dukungan untuk menghapus aplikasi. • Perbaiki bug minor dan penyempurnaan. 	1 Juli 2020	Tidak lagi didukung.
1.2.0	<ul style="list-style-type: none"> • Menambahkan dukungan untuk SAMLotentikasi federasi berbasis 2.0. • Penambahan dukungan untuk macOS Catalina (10.15). 	19 Mei 2020	Tidak lagi didukung.
1.1.2	Perbaiki bug minor dan penyempurnaan.	21 April 2020	Tidak lagi didukung.
1.1.1	<ul style="list-style-type: none"> • Memperbaiki masalah DNS yang tidak diselesaikan. • Perbaiki masalah kerusakan aplikasi yang disebabkan oleh koneksi yang terlalu lama. • Memperbaiki MFA masalah. 	2 April 2020	Tidak lagi didukung.
1.1.0	<ul style="list-style-type: none"> • Menambahkan dukungan untuk konfigurasi macOS DNS. • Menambahkan dukungan untuk fungsi gema tantangan VPN statis Terbuka untuk menyembunyikan atau menampilkan teks yang ditampilkan di antarmuka pengguna. • Perbaiki bug minor dan peningkatan. 	9 Maret 2020	Tidak lagi didukung.
1.0.0	Rilis awal.	4 Februari 2020	Tidak lagi didukung.

AWS Client VPN untuk Linux

Bagian ini menjelaskan menginstal klien yang AWS disediakan untuk Linux dan kemudian membangun membangun VPN koneksi menggunakan klien yang AWS disediakan. Klien yang AWS disediakan untuk Linux tidak mendukung pembaruan otomatis. Untuk pembaruan dan unduhan terbaru, lihat [the section called “Catatan rilis”](#).

Persyaratan untuk menghubungkan ke Klien VPN dengan klien yang AWS disediakan untuk Linux

Untuk menggunakan klien yang AWS disediakan untuk Linux, berikut ini diperlukan:

- Ubuntu 18.04 LTS atau Ubuntu 20.04 LTS (hanya) AMD64

Klien menyimpan TCP port 8096 di komputer Anda. Untuk VPN titik akhir Klien yang menggunakan otentikasi federasi SAML berbasis (sistem masuk tunggal), klien mencadangkan port 35001. TCP

Sebelum memulai, pastikan bahwa VPN administrator Klien Anda telah [membuat VPN titik akhir Klien](#) dan memberi Anda file [konfigurasi VPN titik akhir Klien](#).

Topik

- [Instal klien AWS yang disediakan untuk Linux](#)
- [Connect ke klien AWS yang disediakan untuk Linux](#)
- [AWS Client VPN untuk catatan rilis Linux](#)

Instal klien AWS yang disediakan untuk Linux

Ada beberapa metode yang dapat digunakan untuk menginstal klien yang AWS disediakan untuk Linux. Gunakan salah satu metode yang disediakan dalam pilihan berikut. Sebelum memulai, pastikan Anda telah membaca [persyaratan](#).

Opsi 1: Instal melalui repositori paket

1. Tambahkan kunci publik AWS VPN Klien ke OS Ubuntu Anda.

```
wget -q0- https://d20adtpz83p9s.cloudfront.net/GTK/latest/debian-repo/awsvpnclient_public_key.asc | sudo tee /etc/apt/trusted.gpg.d/awsvpnclient_public_key.asc
```

- Gunakan perintah yang berlaku untuk menambah repositori ke OS Ubuntu Anda, tergantung pada versi Ubuntu Anda:

Ubuntu 18.04

```
echo "deb [arch=amd64] https://d20adtpz83p9s.cloudfront.net/GTK/latest/debian-repo/ubuntu-18.04 main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
```

Ubuntu 20.04

```
echo "deb [arch=amd64] https://d20adtpz83p9s.cloudfront.net/GTK/latest/debian-repo/ubuntu-20.04 main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
```

- Gunakan perintah berikut untuk memperbarui repositori pada sistem Anda.

```
sudo apt-get update
```

- Gunakan perintah berikut untuk menginstal klien yang AWS disediakan untuk Linux.

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

Opsi 2: Instal menggunakan file paket.deb

- Unduh file.deb dari [VPNunduhan AWS Klien](#) atau dengan menggunakan perintah berikut.

```
curl https://d20adtpz83p9s.cloudfront.net/GTK/latest/awsvpnclient_amd64.deb -o awsvpnclient_amd64.deb
```

- Instal klien AWS yang disediakan untuk Linux menggunakan dpkg utilitas.

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

Opsi 3 — Instal paket .deb menggunakan Ubuntu Software Center

1. Unduh file paket.deb dari unduhan [AWS Klien VPN](#).
2. Setelah men-download paket file .deb, gunakan Ubuntu Software Center untuk menginstal paket. Ikuti langkah-langkah untuk menginstal dari paket .deb mandiri menggunakan Ubuntu Software Center, seperti yang dijelaskan pada [Wiki Ubuntu](#).

Connect ke klien AWS yang disediakan untuk Linux

Klien yang AWS disediakan juga disebut sebagai AWS VPN Klien dalam langkah-langkah berikut.

Untuk terhubung menggunakan klien yang AWS disediakan untuk Linux

1. Buka aplikasi AWS VPN Klien.
2. Pilih File, Mengelola Profil.
3. Pilih Tambah profil.
4. Untuk Nama tampilan, masukkan nama untuk profil.
5. Untuk File VPN Konfigurasi, telusuri ke file konfigurasi yang Anda terima dari VPN administrator Klien Anda. Pilih Buka.
6. Pilih Tambah profil.
7. Di jendela AWS VPN Klien, pastikan bahwa profil Anda dipilih, lalu pilih Hubungkan. Jika VPN titik akhir Klien telah dikonfigurasi untuk menggunakan otentikasi berbasis kredensial, Anda akan diminta untuk memasukkan nama pengguna dan kata sandi.
8. Untuk melihat statistik koneksi Anda, pilih Koneksi, Tampilkan Detail.
9. Untuk memutuskan hubungan, di jendela AWS VPN Klien, pilih Putuskan Hubungan.

AWS Client VPN untuk catatan rilis Linux

Tabel berikut berisi catatan rilis dan tautan unduhan untuk versi Linux saat ini dan sebelumnya. AWS Client VPN

Note

Kami terus memberikan kegunaan dan perbaikan keamanan dengan setiap rilis. Kami sangat menyarankan Anda menggunakan versi terbaru untuk setiap platform. Versi sebelumnya

dapat dipengaruhi oleh kegunaan dan/atau masalah keamanan. Lihat catatan rilis untuk detailnya.

Versi	Perubahan	Tanggal	Tautan unduh
3.15.0	<ul style="list-style-type: none"> Menambahkan dukungan untuk VPN bendera tap-sleep Terbuka. Memperbarui SSL perpustakaan Terbuka VPN dan Terbuka. 	Agustus 12, 2024	Unduh versi 3.15.0 sha256:5c f3eb08de9 6821b0ad3 d0c93174b 2e308041d 5490a3edb 772dfd89a 6d89d012
3.14.0	<ul style="list-style-type: none"> Memperbarui SSL perpustakaan Terbuka VPN dan Terbuka. 	Juli 29, 2024	Unduh versi 3.14.0 sha256: bd2b401a1 ede6057d7 25a13c77e f92147a79 e0c5e0020 d379e44f3 19b5334f60
3.13.0	<ul style="list-style-type: none"> Sambungkan kembali secara otomatis ketika rentang jaringan area lokal berubah. 	21 Mei 2024	Unduh versi 3.13.0 sha256: e89f3bb7f c24c148e3 044b80777 4fcfe05e7 eae9e5518 63a38a2dc d7e0ac05f1

Versi	Perubahan	Tanggal	Tautan unduh
3.12.2	<ul style="list-style-type: none">Menyelesaikan masalah SAML otentikasi dengan browser berbasis Chromium sejak versi 123.	April 11, 2024	Unduh versi 3.12.2 sha256: f7178c337 97740bd59 6a14cbe7b 6f5f58fb79d17af79f 88bd88013 53a7571a7d
3.12.1	<ul style="list-style-type: none">Memperbaiki tindakan buffer overflow yang berpotensi memungkinkan aktor lokal menjalankan perintah arbitrer dengan izin yang ditinggikan.Postur keamanan yang ditingkatkan.	Februari 16, 2024	Unduh versi 3.12.1 sha256:54 7c4ffd3e3 5c54db8e0 b792aed9d e1510f6f3 1a6009e55 b8af4f0c2f5cf31d0
3.12.0	<ul style="list-style-type: none">Memperbaiki masalah konektivitas untuk beberapa LAN konfigurasi.	Desember 19, 2023	Unduh versi 3.12.0 sha256:9b 73987309f 1dca1960a 322c5dd86 eec1568ed 270bfd25f 78cc430e3 b5f85cc1

Versi	Perubahan	Tanggal	Tautan unduh
3.11.0	<ul style="list-style-type: none"> Rollback untuk “Memperbaiki masalah konektivitas untuk beberapa LAN konfigurasi”. Peningkatan aksesibilitas. 	6 Desember 2023	Unduh versi 3.11.0 sha256:86 c0fa1bf1c 971940828 35a739ec7 f1c87e540 194955f41 4a35c679b 94538970
3.10.0	<ul style="list-style-type: none"> Memperbaiki masalah konektivitas untuk beberapa LAN konfigurasi. Peningkatan aksesibilitas. 	6 Desember 2023	Unduh versi 3.10.0 sha256: e7450b249 0f3b96ab7 d589a8000 d838d9fd2 adcdd72ae 80666c4c0 d900687e51
3.9.0	<ul style="list-style-type: none"> Memperbaiki masalah konektivitas saat NAT64 diaktifkan di jaringan klien. Perbaiki bug minor dan peningkatan. 	24 Agustus 2023	Unduh versi 3.9.0 sha256:6c de9cfff82 754119e6a 68464d4bb 350da3cb3 e1ebf9140 dacf24e4f d2197454

Versi	Perubahan	Tanggal	Tautan unduh
3.8.0	<ul style="list-style-type: none"> Postur keamanan yang ditingkatkan. 	3 Agustus 2023	Unduh versi 3.8.0 sha256:5f e479236cc 0a1940ba3 7fe168e55 1096f8dae 4c68d4556 0a164e41e dea3e5bd
3.7.0	<ul style="list-style-type: none"> Postur keamanan yang ditingkatkan. 	15 Juli 2023	Tidak lagi didukung
3.6.0	<ul style="list-style-type: none"> Menggulung kembali perubahan dari 3.5.0. 	15 Juli 2023	Tidak lagi didukung
3.5.0	<ul style="list-style-type: none"> Postur keamanan yang ditingkatkan. 	14 Juli 2023	Tidak lagi didukung
3.4.0	<ul style="list-style-type: none"> Ditambahkan dukungan untuk “verify-x 509-name” Buka bendera. VPN 	14 Februari 2023	Tidak lagi didukung
3.1.0	<ul style="list-style-type: none"> Memperbaiki masalah untuk deteksi tipe drive. Postur keamanan yang ditingkatkan. 	23 Mei 2022	Tidak lagi didukung
3.0.0	<ul style="list-style-type: none"> Memperbaiki pesan banner yang tidak ditampilkan saat menggunakan otentikasi federasi. Tampilan teks spanduk tetap untuk teks yang lebih panjang dan urutan karakter tertentu. Postur keamanan yang ditingkatkan. 	3 Maret 2022	Tidak lagi didukung.

Versi	Perubahan	Tanggal	Tautan unduh
2.0.0	<ul style="list-style-type: none"> Ditambahkan dukungan untuk teks banner setelah koneksi baru dibuat. Kemampuan yang dihapus untuk menggunakan saringan tarik dalam kaitannya dengan gema. yaitu filter* pull-filter* echo Perbaiki bug minor dan peningkatan. 	20 Januari 2022	Tidak lagi didukung.
1.0.3	<ul style="list-style-type: none"> Memperbaiki upaya koneksi otentikasi federasi dalam beberapa kasus. Perbaiki bug minor dan peningkatan. 	November 8, 2021	Tidak lagi didukung.
1.0.2	<ul style="list-style-type: none"> Menambahkan dukungan untuk Open VPN flags: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, . server-poll-timeout Perbaiki bug minor dan peningkatan. 	September 28, 2021	Tidak lagi didukung.
1.0.1	<ul style="list-style-type: none"> Opsi yang diaktifkan untuk berhenti dari bilah aplikasi Ubuntu. Menambahkan dukungan untuk VPN bendera Terbuka: tidak aktif, filter tarik, rute. Perbaiki bug minor dan peningkatan. 	4 Agustus 2021	Tidak lagi didukung.
1.0.0	Rilis awal.	11 Juni 2021	Tidak lagi didukung.

Connect ke VPN endpoint Klien menggunakan klien Terbuka VPN

Anda dapat terhubung ke VPN titik akhir Klien menggunakan aplikasi VPN klien Terbuka yang umum.

Important

Jika VPN titik akhir Klien telah dikonfigurasi untuk menggunakan [otentikasi federasi SAML berbasis](#), Anda tidak dapat menggunakan VPN klien VPN berbasis Terbuka untuk terhubung ke titik akhir Klien. VPN

Aplikasi klien

- [Connect ke VPN endpoint Klien menggunakan aplikasi klien Windows](#)
- [Connect ke VPN endpoint Klien menggunakan aplikasi VPN klien Android atau iOS](#)
- [Connect ke VPN endpoint Klien menggunakan aplikasi klien macOS](#)
- [Connect ke VPN endpoint Klien menggunakan aplikasi VPN klien Terbuka](#)

Connect ke VPN endpoint Klien menggunakan aplikasi klien Windows

Bagian ini menjelaskan cara membuat VPN koneksi menggunakan klien berbasis WindowsVPN.

Sebelum memulai, pastikan bahwa VPN administrator Klien Anda telah [membuat VPN titik akhir Klien](#) dan memberi Anda file [konfigurasi VPN titik akhir Klien](#).

Untuk informasi pemecahan masalah, lihat [Memecahkan masalah VPN koneksi Klien dengan klien berbasis Windows](#).

Important

Jika VPN titik akhir Klien telah dikonfigurasi untuk menggunakan [otentikasi federasi SAML berbasis](#), Anda tidak dapat menggunakan VPN klien VPN berbasis Terbuka untuk terhubung ke titik akhir Klien. VPN

Tugas

- [Gunakan sertifikat dari Windows Certificate System Store dengan Open VPN](#)
- [Gunakan Terbuka VPN GUI](#)
- [Gunakan Klien Open VPN Connect](#)

Gunakan sertifikat dari Windows Certificate System Store dengan Open VPN

Anda dapat mengkonfigurasi VPN klien Terbuka untuk menggunakan sertifikat dan kunci pribadi dari Windows Certificate System Store. Opsi ini berguna ketika Anda menggunakan kartu pintar sebagai bagian dari VPN koneksi Klien Anda. Untuk informasi tentang opsi Open VPN client cryptoapicert, lihat [Manual Referensi untuk Buka VPN di situs web Buka](#). VPN

Note

Sertifikat harus disimpan di komputer lokal.

Untuk menggunakan opsi cryptoapicert dengan Open VPN

1. Buat file .pfx yang berisi sertifikat klien dan kunci privat.
2. Impor file .pfx ke penyimpanan sertifikat pribadi Anda, pada komputer lokal. Untuk informasi selengkapnya, lihat [Cara: Melihat sertifikat dengan MMC snap-in](#) di situs web Microsoft.
3. Verifikasi bahwa akun Anda memiliki izin untuk membaca sertifikat komputer lokal. Anda juga dapat menggunakan Konsol Manajemen Microsoft untuk mengubah izin. Untuk informasi selengkapnya, lihat [Hak untuk melihat penyimpanan sertifikat komputer lokal](#) di situs web Microsoft Technet.
4. Perbarui file VPN konfigurasi Buka dan tentukan sertifikat dengan menggunakan subjek sertifikat, atau cap jempol sertifikat.

Berikut ini adalah contoh untuk menentukan sertifikat dengan menggunakan subjek.

```
cryptoapicert "SUBJ:Jane Doe"
```

Berikut ini adalah contoh untuk menentukan sertifikat dengan menggunakan sidik jari. Anda dapat menemukan sidik jari dengan menggunakan Konsol Manajemen Microsoft. Untuk

informasi selengkapnya, lihat [Cara: Mengambil Thumbprint Sertifikat](#) di situs web Microsoft Technet.

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

Setelah Anda menyelesaikan konfigurasi, Anda menggunakan Buka VPN untuk membuat koneksi.

Gunakan Terbuka VPN GUI

Prosedur berikut menunjukkan cara membuat VPN koneksi menggunakan aplikasi VPN GUI klien terbuka pada komputer Windows.

Note

Untuk informasi tentang aplikasi VPN Klien Terbuka, lihat [Unduhan Komunitas](#) di VPN situs web Buka.

Untuk membuat VPN koneksi

1. Mulai aplikasi VPN Klien Terbuka.
2. Pada bilah tugas Windows, pilih Tampilkan/Sembunyikan ikon. Klik kanan Buka VPN GUI, lalu pilih Impor file.
3. Di kotak dialog Buka, pilih file konfigurasi yang Anda terima dari VPN administrator Klien Anda dan pilih Buka.
4. Pada bilah tugas Windows, pilih Tampilkan/Sembunyikan ikon. Klik kanan Buka VPN GUI, lalu pilih Connect.

Gunakan Klien Open VPN Connect

Prosedur berikut menunjukkan cara membuat VPN koneksi menggunakan aplikasi Open VPN Connect Client pada komputer Windows.

Note

Untuk informasi selengkapnya, lihat [Menghubungkan ke Akses Server dengan Windows](#) di VPN situs web Buka.

Untuk membuat VPN koneksi

1. Mulai aplikasi Open VPN Connect Client.
2. Pada bilah tugas Windows, pilih Tampilkan/Sembunyikan ikon. Klik kanan Buka VPN, lalu pilih Impor profil.
3. Pilih Impor dari File dan pilih file konfigurasi yang Anda terima dari VPN administrator Klien Anda.
4. Untuk memulai koneksi, pilih profil koneksi.

Connect ke VPN endpoint Klien menggunakan aplikasi VPN klien Android atau iOS

Important

Jika VPN titik akhir Klien telah dikonfigurasi untuk menggunakan [otentikasi federasi SAML berbasis](#), Anda tidak dapat menggunakan VPN klien VPN berbasis Terbuka untuk terhubung ke titik akhir Klien. VPN

Informasi berikut menunjukkan cara membuat VPN koneksi menggunakan aplikasi VPN klien Terbuka di perangkat seluler Android atau iOS. Langkah-langkah untuk Android dan iOS sama.

Note

Untuk informasi selengkapnya tentang mengunduh dan menggunakan aplikasi VPN klien Terbuka untuk iOS atau Android, lihat [Panduan Pengguna Open VPN Connect](#) di VPN situs web Terbuka.

Sebelum memulai, pastikan bahwa VPN administrator Klien Anda telah [membuat VPN titik akhir Klien](#) dan memberi Anda file [konfigurasi VPN titik akhir Klien](#).

Untuk membuat koneksi, mulai aplikasi Open VPN client, dan kemudian impor file yang Anda terima dari VPN administrator Klien Anda.

Connect ke VPN endpoint Klien menggunakan aplikasi klien macOS

Bagian ini menjelaskan cara membuat VPN koneksi menggunakan klien berbasis macOSVPN.

Sebelum memulai, pastikan bahwa VPN administrator Klien Anda telah [membuat VPN titik akhir Klien](#) dan memberi Anda file [konfigurasi VPN titik akhir Klien](#).

Untuk informasi pemecahan masalah, lihat [Memecahkan masalah VPN koneksi Klien dengan klien macOS](#).

Important

Jika VPN titik akhir Klien telah dikonfigurasi untuk menggunakan [otentikasi federasi SAML berbasis](#), Anda tidak dapat menggunakan VPN klien VPN berbasis Terbuka untuk terhubung ke titik akhir Klien. VPN

Topik

- [Mulai Tunnelblick untuk membuat koneksi AWS Client VPN](#)
- [Connect ke AWS Client VPN endpoint menggunakan Open VPN Connect Client](#)

Mulai Tunnelblick untuk membuat koneksi AWS Client VPN

Prosedur berikut menunjukkan cara membuat VPN koneksi menggunakan aplikasi klien Tunnelblick pada komputer macOS.

Note

Untuk informasi selengkapnya tentang aplikasi klien Tunnelblick untuk macOS, lihat [dokumentasi Tunnelblick](#) di situs web Tunnelblick.

Untuk membuat VPN koneksi

1. Mulai aplikasi klien Tunnelblick dan pilih Saya memiliki file konfigurasi.
2. Seret dan lepas file konfigurasi yang Anda terima dari VPN administrator di panel Konfigurasi.
3. Pilih file konfigurasi dalam panel Konfigurasi dan pilih Hubungkan.

Connect ke AWS Client VPN endpoint menggunakan Open VPN Connect Client

Prosedur berikut menunjukkan cara membuat VPN koneksi menggunakan aplikasi Open VPN Connect Client di komputer macOS.

Note

Untuk informasi selengkapnya, lihat [Menghubungkan ke Server Akses dengan macOS](#) di situs web BukaVPN.

Untuk membuat VPN koneksi

1. Mulai VPN aplikasi Buka, dan pilih Impor, Dari file lokal... .
2. Arahkan ke file konfigurasi yang Anda terima dari VPN administrator Anda, dan pilih Buka.

Connect ke VPN endpoint Klien menggunakan aplikasi VPN klien Terbuka

Bagian ini menjelaskan cara membuat VPN koneksi menggunakan VPN klien VPN berbasis terbuka.

Sebelum memulai, pastikan bahwa VPN administrator Klien Anda telah [membuat VPN titik akhir Klien](#) dan memberi Anda file [konfigurasi VPN titik akhir Klien](#).

Untuk informasi pemecahan masalah, lihat [Memecahkan masalah VPN koneksi Klien dengan klien berbasis Linux](#).

⚠ Important

Jika VPN titik akhir Klien telah dikonfigurasi untuk menggunakan [otentikasi federasi SAML berbasis](#), Anda tidak dapat menggunakan VPN klien VPN berbasis Terbuka untuk terhubung ke titik akhir Klien. VPN

Topik

- [Buat koneksi untuk AWS Client VPN menggunakan Open VPN - Network Manager](#)
- [Buat koneksi untuk AWS Client VPN menggunakan Open VPN](#)

Buat koneksi untuk AWS Client VPN menggunakan Open VPN - Network Manager

Prosedur berikut menunjukkan cara membuat VPN koneksi menggunakan VPN aplikasi Open melalui Network Manager GUI pada komputer Ubuntu.

Untuk membuat VPN koneksi

1. Instal modul network manager menggunakan perintah berikut.

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

2. Buka Pengaturan, Jaringan.
3. Pilih simbol plus (+) di samping VPN, lalu pilih Impor dari file... .
4. Arahkan ke file konfigurasi yang Anda terima dari VPN administrator Anda dan pilih Buka.
5. Di VPN jendela Tambah, pilih Tambah.
6. Mulai koneksi dengan mengaktifkan sakelar di sebelah VPN profil yang Anda tambahkan.

Buat koneksi untuk AWS Client VPN menggunakan Open VPN

Prosedur berikut menunjukkan cara membuat VPN koneksi menggunakan VPN aplikasi Open pada komputer Ubuntu.

Untuk membuat VPN koneksi

1. Instal Buka VPN menggunakan perintah berikut.

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

2. Mulai koneksi dengan memuat file konfigurasi yang Anda terima dari VPN administrator Anda.

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

Memecahkan masalah koneksi Klien VPN

Gunakan topik berikut untuk memecahkan masalah yang mungkin Anda miliki saat menggunakan aplikasi klien untuk terhubung ke titik akhir KlienVPN.

Topik

- [Pemecahan masalah VPN titik akhir klien untuk administrator](#)
- [Kirim log diagnostik ke AWS Support klien yang AWS disediakan](#)
- [Memecahkan masalah VPN koneksi Klien dengan klien berbasis Windows](#)
- [Memecahkan masalah VPN koneksi Klien dengan klien macOS](#)
- [Memecahkan masalah VPN koneksi Klien dengan klien berbasis Linux](#)
- [Memecahkan masalah umum Klien VPN](#)

Pemecahan masalah VPN titik akhir klien untuk administrator

Beberapa langkah dalam panduan ini dapat dilakukan oleh Anda. Langkah-langkah lain harus dilakukan oleh VPN administrator Klien Anda pada VPN titik akhir Klien itu sendiri. Bagian berikut memberi tahu kapan Anda perlu menghubungi administrator Anda.

Untuk informasi tambahan tentang pemecahan masalah VPN titik akhir Klien, lihat [Memecahkan Masalah Klien VPN](#) di Panduan Administrator.AWS Client VPN

Kirim log diagnostik ke AWS Support klien yang AWS disediakan

Jika Anda memiliki masalah dengan klien yang AWS disediakan dan Anda perlu menghubungi AWS Support untuk membantu memecahkan masalah, klien yang AWS disediakan memiliki opsi untuk mengirim log diagnostik ke AWS Support. Opsi ini tersedia pada aplikasi Windows, MacOS dan Linux client.

Sebelum Anda mengirim file, Anda harus setuju untuk mengizinkan AWS Support untuk mengakses log diagnostik Anda. Setelah Anda setuju, kami memberi Anda nomor referensi yang dapat Anda berikan AWS Support sehingga mereka dapat segera mengakses file.

Mengirim log diagnostik

Klien yang AWS disediakan juga disebut sebagai AWS VPN Klien dalam langkah-langkah berikut.

Untuk mengirim log diagnostik menggunakan klien yang AWS disediakan untuk Windows

1. Buka aplikasi client AWS VPN .
2. Pilih Bantuan, Kirim Log Diagnostik.
3. Di dalam jendela Kirim Log Diagnostik, pilih Ya.
4. Di dalam jendela Kirim Log Diagnostik, lakukan salah satu operasi berikut:
 - Untuk menyalin nomor referensi ke clipboard, pilih Ya, dan kemudian pilih OKE.
 - Untuk melacak nomor referensi secara manual, pilih Tidak.

Saat Anda menghubungi AWS Support, Anda harus memberi mereka nomor referensi.

Untuk mengirim log diagnostik menggunakan klien yang AWS disediakan untuk macOS

1. Buka aplikasi client AWS VPN .
2. Pilih Bantuan, Kirim Log Diagnostik.
3. Di dalam jendela Kirim Log Diagnostik, pilih Ya.
4. Perhatikan nomor referensi dari jendela konfirmasi, dan kemudian pilih OKE.

Saat Anda menghubungi AWS Support, Anda harus memberi mereka nomor referensi.

Untuk mengirim log diagnostik menggunakan klien yang AWS disediakan untuk Ubuntu

1. Buka aplikasi client AWS VPN .
2. Pilih Bantuan, Kirim Log Diagnostik.
3. Di dalam jendela Kirim Log Diagnostik, pilih Kirim.
4. Perhatikan nomor referensi dari jendela konfirmasi. Anda diberi pilihan untuk menyalin informasi ke clipboard Anda.

Saat Anda menghubungi AWS Support, Anda harus memberi mereka nomor referensi.

Memecahkan masalah VPN koneksi Klien dengan klien berbasis Windows

Bagian berikut berisi informasi tentang masalah yang mungkin Anda miliki saat menggunakan klien berbasis Windows untuk terhubung ke titik akhir KlienVPN.

Topik

- [AWS klien yang disediakan](#)
- [Buka VPN GUI](#)
- [Buka klien VPN koneksi](#)

AWS klien yang disediakan

Klien yang AWS disediakan membuat log peristiwa dan menyimpannya di lokasi berikut di komputer Anda.

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

Jenis-jenis log berikut tersedia:

- Log aplikasi: Berisi informasi tentang aplikasi. Log-log ini diawali dengan 'aws_vpn_client_'.
- Buka VPN log: Berisi informasi tentang VPN proses Buka. Log-log ini diawali dengan 'ovpn_aws_vpn_client_'.

Klien yang AWS disediakan menggunakan layanan Windows untuk melakukan operasi root. Log layanan Windows disimpan di dalam lokasi berikut di komputer Anda.

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

Topik

- [Client tidak dapat mengoneksikan](#)
- [Klien tidak dapat terhubung dengan pesan log “no TAP -Windows adapters”](#)
- [Client berada dalam status mengoneksikan ulang.](#)
- [VPNproses koneksi berhenti secara tak terduga](#)

- [Aplikasi gagal diluncurkan](#)
- [Client tidak dapat membuat profil](#)
- [Client crash terjadi pada Dell PCs menggunakan Windows 10 atau 11](#)
- [VPN terputus dengan pesan pop up](#)

Client tidak dapat mengoneksikan

Masalah

Klien AWS yang disediakan tidak dapat terhubung ke VPN titik akhir Klien.

Penyebab

Penyebab dari masalah ini mungkin salah satu dari yang berikut:

- VPN Proses terbuka lainnya sudah berjalan di komputer Anda, yang mencegah klien terhubung.
- File (.ovpn) konfigurasi milik Anda tidak valid.

Solusi

Periksa untuk melihat apakah ada VPN aplikasi Open lain yang berjalan di komputer Anda. Jika ada, hentikan atau hentikan proses ini dan coba sambungkan ke VPN titik akhir Klien lagi. Periksa VPN log Buka untuk kesalahan, dan minta VPN administrator Klien Anda untuk memverifikasi informasi berikut:

- Bahwa file konfigurasi berisi kunci dan sertifikat klien yang benar. Untuk informasi selengkapnya, lihat [Ekspor Konfigurasi client](#) dalam Panduan administrator AWS Client VPN .
- Bahwa CRL masih valid. Untuk informasi selengkapnya, lihat [Klien Tidak Dapat Menyambung ke VPN Titik Akhir Klien](#) di Panduan AWS Client VPN Administrator.

Klien tidak dapat terhubung dengan pesan log “no TAP -Windows adapters”

Masalah

Klien yang AWS disediakan tidak dapat terhubung ke VPN titik akhir Klien dan pesan kesalahan berikut muncul di log aplikasi: “Tidak ada adaptor TAP -Windows pada sistem ini. Anda harus dapat membuat adaptor TAP -Windows dengan membuka Mulai -> Semua Program -> TAP -Windows -> Utilitas -> Tambahkan adaptor ethernet virtual TAP -Windows baru”.

Solusi

Anda dapat mengatasi masalah ini dengan mengambil satu atau lebih tindakan berikut:

- Mulai ulang adaptor TAP -Windows.
- Instal ulang driver TAP -Windows.
- Buat adaptor TAP -Windows baru.

Client berada dalam status mengoneksikan ulang.

Masalah

Klien yang AWS disediakan mencoba untuk terhubung ke VPN titik akhir Klien, tetapi terjebak dalam keadaan menyambung kembali.

Penyebab

Penyebab dari masalah berikut mungkin adalah salah satu dari hal-hal berikut:

- Komputer Anda tidak terkoneksi ke internet.
- DNSNama host tidak menyelesaikan ke alamat IP.
- VPNProses Terbuka tanpa batas mencoba terhubung ke titik akhir.

Solusi

Verifikasi bahwa komputer Anda terkoneksi ke internet. Minta VPN administrator Klien Anda untuk memverifikasi bahwa remote arahan dalam file konfigurasi diselesaikan ke alamat IP yang valid. Anda juga dapat memutuskan sambungan VPN sesi dengan memilih Putuskan sambungan di jendela AWS VPN Klien, dan coba sambungkan lagi.

VPNproses koneksi berhenti secara tak terduga

Masalah

Saat menghubungkan ke VPN titik akhir Klien, klien berhenti secara tak terduga.

Penyebab

TAP-Windows tidak diinstal pada komputer Anda. Perangkat lunak ini diperlukan untuk dapat menjalankan client.

Solusi

Jalankan kembali penginstal klien yang AWS disediakan untuk menginstal semua dependensi yang diperlukan.

Aplikasi gagal diluncurkan

Masalah

Pada Windows 7, klien yang AWS disediakan tidak diluncurkan ketika Anda mencoba membukanya.

Penyebab

.NETFramework 4.7.2 atau lebih tinggi tidak diinstal pada komputer Anda. Ini diperlukan untuk menjalankan client.

Solusi

Jalankan kembali penginstal klien yang AWS disediakan untuk menginstal semua dependensi yang diperlukan.

Client tidak dapat membuat profil

Masalah

Anda akan menemukan kesalahan berikut ketika Anda mencoba untuk membuat profil menggunakan klien yang disediakan oleh AWS .

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

Penyebab

Jika VPN titik akhir Klien menggunakan otentikasi timbal balik, file konfigurasi (.ovpn) tidak berisi sertifikat dan kunci klien.

Solusi

Pastikan VPN administrator Klien Anda menambahkan sertifikat klien dan kunci ke file konfigurasi. Untuk informasi selengkapnya, lihat [Ekspor Konfigurasi client](#) dalam Panduan administrator AWS Client VPN .

Client crash terjadi pada Dell PCs menggunakan Windows 10 atau 11

Masalah

Pada Dell tertentu PCs (desktop dan laptop) yang menjalankan Windows 10 atau 11, crash dapat terjadi ketika Anda menjelajahi sistem file Anda untuk mengimpor file VPN konfigurasi. Jika masalah ini terjadi, Anda akan melihat pesan seperti berikut di log klien yang AWS disediakan:

```
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()
```

Penyebab

Sistem Pencadangan dan Pemulihan Dell di Windows 10 dan 11 dapat menyebabkan konflik dengan klien yang AWS disediakan, terutama dengan tiga DLLs berikut:

- DBRShellExtension.dll
- DBROverlayIconBackup.dll
- DBROverlayIconNotBackup.dll

Solusi

Untuk menghindari masalah ini, pertama-tama pastikan bahwa klien Anda up to date dengan versi terbaru dari klien yang AWS disediakan. Buka [VPNunduhan AWS Klien](#) dan jika versi yang lebih baru tersedia, tingkatkan ke versi terbaru.

Selain itu, lakukan salah satu hal berikut:

- Jika Anda menggunakan aplikasi Backup and Recovery Dell, pastikan itu up to date. [Posting forum Dell](#) menyatakan bahwa masalah ini diselesaikan di versi aplikasi yang lebih baru.
- Jika Anda tidak menggunakan aplikasi Backup and Recovery Dell, beberapa tindakan masih perlu diambil jika Anda mengalami masalah ini. Jika Anda tidak ingin memutakhirkan aplikasi, sebagai

alternatif, Anda dapat menghapus atau mengganti nama DLL file. Namun, perhatikan bahwa ini akan mencegah aplikasi Backup and Recovery Dell berfungsi sepenuhnya.

Hapus atau ganti nama file DLL

1. Buka Windows Explorer dan telusuri ke lokasi di mana Dell Backup and Recovery diinstal. Biasanya dipasang di lokasi berikut, tetapi Anda mungkin perlu mencari untuk menemukannya.

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

2. Hapus DLL file berikut secara manual dari direktori instalasi, atau ganti namanya. Tindakan apa pun akan mencegahnya dimuat.
 - DBRShellExtension.dll
 - DBROverlayIconBackupped.dll
 - DBROverlayIconNotBackupped.dll

Anda dapat mengganti nama file dengan menambahkan “.bak” ke akhir nama file, misalnya, DBROverlayIconBackupped .dll.bak.

VPNterputus dengan pesan pop up

Masalah

VPNTerputus dengan pesan pop up yang mengatakan: “VPNSambungan sedang dihentikan karena ruang alamat jaringan lokal yang terhubung dengan perangkat Anda telah berubah. Tolong buat VPN koneksi baru.”

Penyebab

TAP-Adaptor Windows tidak berisi deskripsi yang diperlukan.

Solusi

Jika Description bidang tidak cocok di bawah ini, pertama-tama hapus adaptor TAP -Windows, lalu jalankan kembali penginstal klien yang AWS disediakan untuk menginstal semua dependensi yang diperlukan.

```
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
```

Buka VPN GUI

Informasi pemecahan masalah berikut diuji pada versi 11.10.0.0 dan 11.11.0.0 dari VPN GUI perangkat lunak Open pada Windows 10 Home (64-bit) dan Windows Server 2016 (64-bit).

File konfigurasi disimpan di dalam lokasi berikut di komputer Anda.

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

Log koneksi disimpan di dalam lokasi berikut di komputer Anda.

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

Buka klien VPN koneksi

Informasi pemecahan masalah berikut diuji pada versi 2.6.0.100 dan 2.7.1.101 dari perangkat lunak Open VPN Connect Client pada Windows 10 Home (64-bit) dan Windows Server 2016 (64-bit).

File konfigurasi disimpan di dalam lokasi berikut di komputer Anda.

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

Log koneksi disimpan di dalam lokasi berikut di komputer Anda.

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

Tidak dapat menyelesaikan DNS

Masalah

Koneksi gagal dengan galat berikut.

```
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.
```

Penyebab

DNSNama tidak dapat diselesaikan. Klien harus menambahkan string acak ke DNS nama untuk mencegah DNS caching; Namun, beberapa klien tidak melakukan ini.

Solusi

Lihat solusi [untuk Tidak Dapat Menyelesaikan DNS Nama VPN Titik Akhir Klien](#) di Panduan AWS Client VPN Administrator.

PKIAlias hilang

Masalah

Koneksi ke VPN titik akhir Klien yang tidak menggunakan otentikasi timbal balik gagal dengan kesalahan berikut.

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

Penyebab

Perangkat lunak Open VPN Connect Client memiliki masalah yang diketahui di mana ia mencoba untuk mengautentikasi menggunakan otentikasi timbal balik. Jika file konfigurasi tidak berisi kunci dan sertifikat client, autentikasi akan gagal.

Solusi

Tentukan kunci klien acak dan sertifikat dalam file VPN konfigurasi Klien dan impor konfigurasi baru ke dalam perangkat lunak Open VPN Connect Client. Atau, gunakan klien yang berbeda, seperti klien Terbuka (v11.12.0.0) atau VPN GUI klien Viskositas (v.1.7.14).

Memecahkan masalah VPN koneksi Klien dengan klien macOS

Bagian berikut berisi informasi tentang pencatatan log serta masalah yang mungkin Anda hadapi saat menggunakan macOS client. Pastikan bahwa Anda menjalankan versi terbaru client-client tersebut.

Topik

- [AWS klien yang disediakan](#)
- [Tunnelblick](#)
- [Buka VPN](#)

AWS klien yang disediakan

Klien yang AWS disediakan membuat log peristiwa dan menyimpannya di lokasi berikut di komputer Anda.

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

Jenis-jenis log berikut tersedia:

- Log aplikasi: Berisi informasi tentang aplikasi. Log-log ini diawali dengan 'aws_vpn_client_'.
- Buka VPN log: Berisi informasi tentang VPN proses Buka. Log-log ini diawali dengan 'ovpn_aws_vpn_client_'.

Klien AWS yang disediakan menggunakan daemon klien untuk melakukan operasi root. Log-log daemon disimpan di dalam lokasi berikut di komputer Anda.

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

Klien yang AWS disediakan menyimpan file konfigurasi di lokasi berikut di komputer Anda.

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

Topik

- [Client tidak dapat mengoneksikan](#)
- [Client berada dalam status mengoneksikan ulang.](#)
- [Client tidak dapat membuat profil](#)
- [Alat pembantu diperlukan kesalahan](#)

Client tidak dapat mengoneksikan

Masalah

Klien AWS yang disediakan tidak dapat terhubung ke VPN titik akhir Klien.

Penyebab

Penyebab dari masalah ini mungkin salah satu dari yang berikut:

- VPNProses terbuka lainnya sudah berjalan di komputer Anda, yang mencegah klien terhubung.
- File (.ovpn) konfigurasi milik Anda tidak valid.

Solusi

Periksa untuk melihat apakah ada VPN aplikasi Open lain yang berjalan di komputer Anda. Jika ada, hentikan atau hentikan proses ini dan coba sambungkan ke VPN titik akhir Klien lagi. Periksa VPN log Buka untuk kesalahan, dan minta VPN administrator Klien Anda untuk memverifikasi informasi berikut:

- Bahwa file konfigurasi berisi kunci dan sertifikat klien yang benar. Untuk informasi selengkapnya, lihat [Ekspor Konfigurasi client](#) dalam Panduan administrator AWS Client VPN .
- Bahwa CRL masih valid. Untuk informasi selengkapnya, lihat [Klien Tidak Dapat Menyambung ke VPN Titik Akhir Klien](#) di Panduan AWS Client VPN Administrator.

Client berada dalam status mengoneksikan ulang.

Masalah

Klien yang AWS disediakan mencoba untuk terhubung ke VPN titik akhir Klien, tetapi terjebak dalam keadaan menyambung kembali.

Penyebab

Penyebab dari masalah berikut mungkin adalah sah satu dari hal-hal berikut:

- Komputer Anda tidak terkoneksi ke internet.
- DNSNama host tidak menyelesaikan ke alamat IP.
- VPNProses Terbuka tanpa batas mencoba terhubung ke titik akhir.

Solusi

Verifikasi bahwa komputer Anda terkoneksi ke internet. Minta VPN administrator Klien Anda untuk memverifikasi bahwa remote arahan dalam file konfigurasi diselesaikan ke alamat IP yang valid. Anda juga dapat memutuskan sambungan VPN sesi dengan memilih Putuskan sambungan di jendela AWS VPN Klien, dan coba sambungkan lagi.

Client tidak dapat membuat profil

Masalah

Anda akan menemukan kesalahan berikut ketika Anda mencoba untuk membuat profil menggunakan klien yang disediakan oleh AWS .

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

Penyebab

Jika VPN titik akhir Klien menggunakan otentikasi timbal balik, file konfigurasi (.ovpn) tidak berisi sertifikat dan kunci klien.

Solusi

Pastikan VPN administrator Klien Anda menambahkan sertifikat klien dan kunci ke file konfigurasi. Untuk informasi selengkapnya, lihat [Ekspor Konfigurasi client](#) dalam Panduan administrator AWS Client VPN .

Alat pembantu diperlukan kesalahan

Masalah

Anda mendapatkan kesalahan berikut ketika Anda mencoba menghubungkan fileVPN.

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

Solusi

Lihat artikel berikut di AWS Re:post. [AWSVPNKlien - Alat pembantu diperlukan kesalahan](#)

Tunnelblick

Informasi pemecahan masalah berikut telah diuji pada perangkat lunak Tunnelblick versi 3.7.8 (build 5180) di macOS High Sierra 10.13.6.

File konfigurasi untuk konfigurasi privat telah disimpan di dalam lokasi berikut di komputer Anda.

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

File konfigurasi untuk konfigurasi bersama disimpan di dalam lokasi berikut di komputer Anda.

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

Log koneksi disimpan di dalam lokasi berikut di komputer Anda.

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

Untuk meningkatkan verbositas log, buka aplikasi Tunnelblick, pilih Pengaturan, dan sesuaikan nilai untuk level log. VPN

Algoritma cipher 'AES-256-GCM' tidak ditemukan

Masalah

Koneksi gagal dan mengembalikan galat berikut di dalam log.

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

Penyebab

Aplikasi ini menggunakan VPN versi Open yang tidak mendukung algoritma cipher AES -256-. GCM

Solusi

Pilih VPN versi Buka yang kompatibel dengan melakukan hal berikut:

1. Buka aplikasi Tunnelblick.
2. Pilih Pengaturan.
3. Untuk VPNversi Terbuka, pilih 2.4.6 - SSL Versi terbuka adalah v1.0.2q.

Koneksi berhenti merespons dan mengatur ulang

Masalah

Koneksi gagal dan mengembalikan galat berikut di dalam log.

```
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
```

Penyebab

Sertifikat client telah dicabut. Koneksi berhenti merespons setelah berupaya untuk mengautentikasi dan mengatur ulang dari sisi server.

Solusi

Minta file konfigurasi baru dari VPN administrator Klien Anda.

Penggunaan kunci yang diperluas (EKU)

Masalah

Koneksi gagal dan mengembalikan galat berikut di dalam log.

```
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,,,,,
```

Penyebab

Autentikasi server telah berhasil. Namun, otentikasi klien gagal karena sertifikat klien memiliki bidang penggunaan kunci diperpanjang (EKU) yang diaktifkan untuk otentikasi server.

Solusi

Verifikasi bahwa Anda sedang menggunakan sertifikat dan kunci klien yang benar. Jika perlu, verifikasi dengan VPN administrator Klien Anda. Kesalahan ini mungkin terjadi jika Anda menggunakan sertifikat server dan bukan sertifikat klien untuk terhubung ke VPN titik akhir Klien.

Sertifikat sudah kedaluwarsa

Masalah

Autentikasi server berhasil, namun autentikasi client gagal dengan galat berikut.

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

Penyebab

Validitas sertifikat client telah kedaluwarsa.

Solusi

Minta sertifikat klien baru dari VPN administrator Klien Anda.

Buka VPN

Informasi pemecahan masalah berikut telah diuji pada versi 2.7.1.100 perangkat lunak Open Connect VPN Client di macOS High Sierra 10.13.6.

File konfigurasi disimpan di dalam lokasi berikut di komputer Anda.

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

Log koneksi disimpan di dalam lokasi berikut di komputer Anda.

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

Tidak dapat menyelesaikan DNS

Masalah

Koneksi gagal dengan galat berikut.

```
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
```

Penyebab

Open VPN Connect tidak dapat menyelesaikan VPN DNS nama Klien.

Solusi

Lihat solusi [untuk Tidak Dapat Menyelesaikan DNS Nama VPN Titik Akhir Klien](#) di Panduan AWS Client VPN Administrator.

Memecahkan masalah VPN koneksi Klien dengan klien berbasis Linux

Bagian berikut berisi informasi tentang pencatatan, dan masalah yang mungkin Anda temui saat menggunakan client berbasis Linux. Pastikan bahwa Anda menjalankan client versi terbaru.

Topik

- [AWS klien yang disediakan](#)
- [Buka VPN \(baris perintah\)](#)
- [Buka VPN melalui Network Manager \(GUI\)](#)

AWS klien yang disediakan

Klien yang AWS disediakan menyimpan file log dan file konfigurasi di lokasi berikut di sistem Anda:

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

Proses daemon klien yang AWS disediakan menyimpan file log di lokasi berikut di sistem Anda:

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

Masalah

Dalam beberapa keadaan setelah VPN koneksi dibuat, DNS kueri akan tetap masuk ke server nama sistem default, bukan server nama yang dikonfigurasi untuk titik akhir Klien. VPN

Penyebab

Klien berinteraksi dengan `systemd-resolved`, layanan yang tersedia pada sistem Linux, yang berfungsi sebagai bagian utama dari manajemen. DNS Ini digunakan untuk mengkonfigurasi DNS server yang didorong dari VPN titik akhir Klien. Masalah terjadi karena `systemd-resolved` tidak menetapkan prioritas tertinggi ke DNS server yang disediakan oleh endpoint KlienVPN. Sebagai gantinya, ia menambahkan server ke daftar DNS server yang ada yang dikonfigurasi pada sistem lokal. Akibatnya, DNS server asli mungkin masih memiliki prioritas tertinggi, dan karena itu digunakan untuk menyelesaikan DNS kueri.

Solusi

1. Tambahkan direktif berikut pada baris pertama file VPN konfigurasi Open, untuk memastikan bahwa semua DNS kueri dikirim ke terowongan. VPN

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

2. Gunakan stub resolver yang disediakan oleh `systemd-resolved`. Untuk dapat melakukannya, symlink `/etc/resolv.conf` ke `/run/systemd/resolve/stub-resolv.conf` dengan menjalankan perintah berikut pada sistem.

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

3. (Opsional) Jika Anda tidak ingin `systemd-resolved` ke DNS kueri proxy, dan sebaliknya ingin kueri dikirim ke DNS server nama sebenarnya secara langsung, symlink ke sebagai gantinya. `/etc/resolv.conf /run/systemd/resolve/resolv.conf`

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

Anda mungkin ingin melakukan prosedur ini untuk melewati konfigurasi yang diselesaikan sistem, misalnya untuk caching DNS jawaban, konfigurasi per antarmuka, penegakan, DNSSEC dan DNS sebagainya. Opsi ini sangat berguna ketika Anda memiliki kebutuhan untuk mengganti

catatan publik dengan DNS catatan pribadi saat terhubungVPN. Misalnya, Anda mungkin memiliki DNS resolver pribadi di pribadi Anda VPC dengan catatan untuk `www.example.com`, yang menyelesaikan ke IP pribadi. Opsi ini dapat digunakan untuk meng-override catatan publik `www.example.com`, yang me-resolve ke IP publik.

Buka VPN (baris perintah)

Masalah

Koneksi tidak berfungsi dengan benar karena DNS resolusi tidak berfungsi.

Penyebab

DNSServer tidak dikonfigurasi pada VPN titik akhir Klien, atau tidak dihormati oleh perangkat lunak klien.

Solusi

Gunakan langkah-langkah berikut untuk memeriksa apakah DNS server dikonfigurasi dan berfungsi dengan benar.

1. Pastikan entri DNS server ada di log. Dalam contoh berikut, DNS server `192.168.0.2` (dikonfigurasi di VPN titik akhir Klien) dikembalikan di baris terakhir.

```
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
```

Jika tidak ada DNS server yang ditentukan, minta VPN administrator Klien Anda untuk memodifikasi VPN titik akhir Klien dan memastikan bahwa DNS server (misalnya, VPC DNS server) telah ditentukan untuk titik VPN akhir Klien. Untuk informasi selengkapnya, lihat [VPNTitik Akhir Klien](#) di Panduan AWS Client VPN Administrator.

2. Pastikan bahwa paket `resolvconf` telah diinstal dengan menjalankan perintah berikut.

```
sudo apt list resolvconf
```

Output akan mengembalikan hal-hal berikut.


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

Jika tidak diinstal, instal paket dengan menggunakan perintah berikut.

```
sudo apt install resolvconf
```

3. Buka file VPN konfigurasi Klien (file.ovpn) di editor teks dan tambahkan baris berikut.

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

Periksa log untuk memverifikasi bahwa skrip `resolvconf` telah diminta. Log harus berisi baris yang serupa dengan baris berikut.

```
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
```

Buka VPN melalui Network Manager (GUI)

Masalah

Saat menggunakan VPN klien Network Manager Open, koneksi gagal dengan kesalahan berikut.

```
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, LZ0 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
```

Penyebab

Tanda `remote-random-hostname` tidak diperhitungkan, dan klien tidak dapat membuat hubungan menggunakan paket `network-manager-gnome`.

Solusi

Lihat solusi [untuk Tidak Dapat Menyelesaikan DNS Nama VPN Titik Akhir Klien](#) di Panduan AWS Client VPN Administrator.

Memecahkan masalah umum Klien VPN

Berikut ini adalah masalah umum yang mungkin Anda miliki saat menggunakan klien untuk terhubung ke VPN titik akhir Klien.

TLSNegosiasi kunci gagal

Masalah

TLSNegosiasi gagal dengan kesalahan berikut.

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

Penyebab

Penyebab dari masalah ini mungkin salah satu dari yang berikut:

- Aturan firewall memblokir UDP atau TCP lalu lintas.
- Anda menggunakan kunci dan sertifikat klien yang salah di dalam file (.ovpn) konfigurasi.
- Daftar pencabutan sertifikat klien (CRL) telah kedaluwarsa.

Solusi

Periksa untuk melihat apakah aturan firewall di komputer Anda memblokir masuk atau keluar atau UDP lalu lintas pada port 443 TCP atau 1194. Minta VPN administrator Klien Anda untuk memverifikasi informasi berikut:

- Bahwa aturan firewall untuk VPN titik akhir Klien tidak memblokir TCP atau UDP lalu lintas pada port 443 atau 1194.
- Bahwa file konfigurasi berisi kunci dan sertifikat klien yang benar. Untuk informasi selengkapnya, lihat [Ekspor Konfigurasi client](#) dalam Panduan administrator AWS Client VPN .
- Bahwa CRL masih valid. Untuk informasi selengkapnya, lihat [Klien Tidak Dapat Menyambung ke VPN Titik Akhir Klien](#) di Panduan AWS Client VPN Administrator.

Riwayat dokumen

Tabel berikut menjelaskan pembaruan Panduan VPN Pengguna AWS Klien.

Perubahan	Deskripsi	Tanggal
AWS klien yang disediakan (3.15.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Agustus 12, 2024
AWS klien yang disediakan (3.14.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Agustus 12, 2024
AWS klien yang disediakan (3.12.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Agustus 12, 2024
AWS klien yang disediakan (3.14.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Juli 29, 2024
AWS klien yang disediakan (3.13.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Juli 29, 2024
AWS klien yang disediakan (3.11.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Juli 29, 2024
AWS klien yang disediakan (3.12.1) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Juli 18, 2024
AWS klien yang disediakan (3.13.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	21 Mei 2024
AWS klien yang disediakan (3.12.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	21 Mei 2024
AWS klien yang disediakan (3.10.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	21 Mei 2024
AWS klien yang disediakan (3.9.2) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	April 11, 2024

AWS klien yang disediakan (3.12.2) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	April 11, 2024
AWS klien yang disediakan (3.11.2) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	April 11, 2024
AWS klien yang disediakan (3.9.1) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	Februari 16, 2024
AWS klien yang disediakan (3.12.1) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Februari 16, 2024
AWS klien yang disediakan (3.11.1) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Februari 16, 2024
AWS klien yang disediakan (3.12.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	Desember 19, 2023
AWS klien yang disediakan (3.9.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	6 Desember 2023
AWS klien yang disediakan (3.11.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	6 Desember 2023
AWS klien yang disediakan (3.11.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	6 Desember 2023
AWS klien yang disediakan (3.10.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	6 Desember 2023
AWS klien yang disediakan (3.9.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	24 Agustus 2023
AWS klien yang disediakan (3.8.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	24 Agustus 2023
AWS klien yang disediakan (3.10.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	24 Agustus 2023

AWS klien yang disediakan (3.9.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	3 Agustus 2023
AWS klien yang disediakan (3.8.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	3 Agustus 2023
AWS klien yang disediakan (3.7.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	3 Agustus 2023
AWS klien yang disediakan (3.8.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	15 Juli 2023
AWS klien yang disediakan (3.7.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	15 Juli 2023
AWS klien yang disediakan (3.7.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	15 Juli 2023
AWS klien yang disediakan (3.6.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	15 Juli 2023
AWS klien yang disediakan (3.6.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	15 Juli 2023
AWS klien yang disediakan (3.5.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	15 Juli 2023
AWS klien yang disediakan (3.6.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	14 Juli 2023
AWS klien yang disediakan (3.5.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	14 Juli 2023
AWS klien yang disediakan (3.4.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	14 Juli 2023
AWS klien yang disediakan (3.3.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	27 April 2023

AWS klien yang disediakan (3.5.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	3 April 2023
AWS klien yang disediakan (3.4.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Maret 28, 2023
AWS klien yang disediakan (3.3.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	Maret 17, 2023
AWS klien yang disediakan (3.4.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	14 Februari 2023
AWS klien yang disediakan (3.2.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	23 Januari 2023
AWS klien yang disediakan (3.2.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	23 Januari 2023
AWS klien yang disediakan (3.1.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	23 Mei 2022
AWS klien yang disediakan (3.1.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	23 Mei 2022
AWS klien yang disediakan (3.1.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	23 Mei 2022
AWS klien yang disediakan (3.0.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	3 Maret 2022
AWS klien yang disediakan (3.0.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	3 Maret 2022
AWS klien yang disediakan (3.0.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	3 Maret 2022
AWS klien yang disediakan (2.0.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	20 Januari 2022

AWS klien yang disediakan (2.0.0) untuk Windows dirilis	Lihat catatan rilis untuk detailnya.	20 Januari 2022
AWS klien yang disediakan (2.0.0) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	20 Januari 2022
AWS klien yang disediakan (1.4.0) untuk macOS dirilis	Lihat catatan rilis untuk detailnya.	November 9, 2021
AWS klien yang disediakan untuk Windows (1.3.7) dirilis	Lihat catatan rilis untuk detailnya.	November 8, 2021
AWS klien yang disediakan (1.0.3) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	November 8, 2021
AWS klien yang disediakan (1.0.2) untuk Ubuntu dirilis	Lihat catatan rilis untuk detailnya.	September 28, 2021
AWS klien yang disediakan untuk Windows (1.3.6) dan macOS (1.3.5) dirilis	Lihat catatan rilis untuk detailnya.	September 20, 2021
AWS klien yang disediakan untuk Ubuntu 18.04 LTS dan Ubuntu LTS 20.04 dirilis	Anda dapat menggunakan klien yang AWS disediakan di Ubuntu 18.04 LTS dan Ubuntu 20.04. LTS	11 Juni 2021
Support for Open VPN menggunakan sertifikat dari Windows Certificate System Store	Anda dapat menggunakan Buka VPN dengan sertifikat dari Windows Certificate System Store.	25 Februari 2021
Portal swalayan	Anda dapat mengakses portal swalayan untuk mendapatkan klien dan file konfigurasi terbaru yang AWS disediakan.	29 Oktober 2020

[AWS klien yang disediakan](#)

Anda dapat menggunakan klien yang AWS disediakan untuk terhubung ke VPN titik akhir Klien.

4 Februari 2020

[Rilis awal](#)

Rilis ini memperkenalkan AWS KlienVPN.

18 Desember 2018

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.