



Guida per l'utente

AWS Client VPN



AWS Client VPN: Guida per l'utente

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Cos'è AWS Client VPN?	1
Componenti Client VPN	1
Risorse aggiuntive per la configurazione di Client VPN	1
Inizia a usare Client VPN	2
Prerequisiti per l'utilizzo di Client VPN	2
Fase 1: ottenere un'applicazione client VPN	3
Fase 2: ottenere il file di configurazione dell'endpoint Client VPN	3
Fase 3: Connettersi alla VPN	3
Scarica Client VPN	4
Connect utilizzando un client AWS fornito	6
Sicurezza	6
Support per connessioni simultanee	6
Direttive OpenVPN	7
Windows	9
Requisiti	9
Connect utilizzando il client	10
Compatibilità con la sicurezza degli endpoint	11
Note di rilascio	13
macOS	32
Requisiti	32
Connect utilizzando il client	33
Note di rilascio	34
Linux	45
Requisiti per la connessione a Client VPN con un AWS client fornito per Linux	45
Installa il client	45
Connect utilizzando il client	47
Note di rilascio	48
Connessione mediante un client OpenVPN	53
Windows	54
Stabilisci una connessione VPN utilizzando un certificato su Windows	54
macOS	56
Stabilisci una connessione VPN su macOS	57
Linux	57
Stabilire una connessione VPN su Linux	58

Connessioni Client VPN su Android e iOS	59
Risoluzione dei problemi	60
Risoluzione dei problemi degli endpoint Client VPN per gli amministratori	60
Invia i registri di diagnostica a Supporto AWS nel AWS Client fornito da	60
Inviare registri di diagnostica	61
Risoluzione dei problemi di Windows	62
AWS ha fornito i registri degli eventi dei client	62
Il client non è in grado di connettersi	63
Il client non può connettersi con il messaggio di registro «nessun TAP-Windows adattatore»	63
Il client è bloccato in uno stato di riconnessione	64
Il processo di connessione VPN si chiude in maniera imprevista	64
Impossibile avviare l'applicazione	65
Il client non è in grado di creare un profilo	65
La VPN si disconnette con un messaggio pop-up	66
Si verifica un arresto anomalo del client su PC Dell che utilizzano Windows 10 o 11	66
OpenVPN GUI	68
Client OpenVPN Connect	68
Impossibile risolvere il DNS	69
Alias PKI mancante	69
Risoluzione dei problemi di macOS	70
AWS ha fornito i registri degli eventi del client	70
Il client non è in grado di connettersi	71
Il client è bloccato in uno stato di riconnessione	72
Il client non è in grado di creare un profilo	72
Lo strumento di supporto è un errore obbligatorio	73
Tunnelblick	73
Algoritmo di cifratura " AES-256-GCM non trovato	74
La connessione smette di rispondere e si ripristina	74
Utilizzo chiave esteso (EKU)	75
Certificato scaduto	76
OpenVPN	76
Impossibile risolvere DNS	76
Risoluzione dei problemi di Linux	77
AWS ha fornito i registri degli eventi dei client	62
Le query DNS vanno a un nameserver predefinito	78

OpenVPN (riga di comando)	79
OpenVPN tramite Network Manager (GUI)	80
Problemi comuni	81
Negoziazione chiave TLS non riuscita	81
Cronologia dei documenti	83
.....	xciv

Cos'è AWS Client VPN?

AWS Client VPN è un servizio VPN gestito basato su client che consente di accedere in modo sicuro a AWS risorse e risorse nella rete locale.

Questa guida fornisce le fasi per stabilire una connessione VPN a un endpoint Client VPN utilizzando un'applicazione client sul dispositivo.

Componenti Client VPN

Di seguito sono riportati i componenti chiave per l'utilizzo di AWS Client VPN.

- **Endpoint Client VPN:** l'amministratore Client VPN crea e configura un endpoint Client VPN in AWS. L'amministratore controlla le reti e le risorse cui è possibile accedere quando si stabilisce una connessione VPN.
- **Applicazione client VPN:** l'applicazione software utilizzata per connettersi all'endpoint Client VPN e stabilire una connessione VPN sicura.
- **File di configurazione dell'endpoint Client VPN:** un file di configurazione fornito dall'amministratore Client VPN. Il file include informazioni sull'endpoint Client VPN e sui certificati necessari per stabilire una connessione VPN. Il file viene caricato nell'applicazione client VPN scelta. Il client AWS fornito consente di connettersi a cinque sessioni simultanee, ciascuna sessione con il proprio file di configurazione fornito dall'amministratore Client VPN. Per ulteriori informazioni sulle sessioni simultanee, vedere [Support per connessioni simultanee](#)

Risorse aggiuntive per la configurazione di Client VPN

Se sei un amministratore di Client VPN, consulta la [Guida AWS Client VPN dell'amministratore](#) per ulteriori informazioni sulla creazione e la configurazione di un endpoint Client VPN.

Inizia con AWS Client VPN

Prima di stabilire una sessione VPN, l'amministratore Client VPN deve creare e configurare un endpoint Client VPN. L'amministratore controlla a quali reti e risorse puoi accedere quando stabilisci una sessione VPN. Puoi quindi utilizzare un'applicazione client VPN per connetterti a un endpoint Client VPN e stabilire una connessione VPN sicura.

Se sei un amministratore che deve creare un endpoint Client VPN, consulta la [Guida per l'amministratore di AWS Client VPN](#).

Argomenti

- [Prerequisiti per l'utilizzo di Client VPN](#)
- [Fase 1: ottenere un'applicazione client VPN](#)
- [Fase 2: ottenere il file di configurazione dell'endpoint Client VPN](#)
- [Fase 3: Connettersi alla VPN](#)
- [Scarica il file AWS Client VPN dal portale self-service](#)

Prerequisiti per l'utilizzo di Client VPN

Per stabilire una connessione VPN, è necessario quanto segue:

- Accesso a Internet
- Un dispositivo supportato
- [Una versione supportata di Windows, macOS o Linux.](#)
- Per gli endpoint Client VPN che utilizzano l'autenticazione federata basata su SAML (Single Sign-On), uno dei seguenti browser:
 - Apple Safari
 - Google Chrome
 - Microsoft Edge
 - Mozilla Firefox

Fase 1: ottenere un'applicazione client VPN

Puoi connetterti a un endpoint Client VPN e stabilire una connessione VPN utilizzando il client fornito da AWS o un'altra applicazione client basata su OpenVPN.

È possibile scaricare l'applicazione Client VPN tramite uno dei due metodi seguenti, a seconda che l'amministratore abbia creato il file di configurazione dell'endpoint per l'applicazione:

- Se l'amministratore non ha configurato i file di configurazione degli endpoint, scarica e installa il [AWS client da Client VPN download](#). Dopo aver scaricato e installato l'applicazione, procedi [the section called "Fase 2: ottenere il file di configurazione dell'endpoint Client VPN"](#) a richiedere il file di configurazione dell'endpoint all'amministratore. Se ti connetti a più profili, avrai bisogno di un file di configurazione per ogni profilo.
- Se l'amministratore ha già preconfigurato il file di configurazione dell'endpoint, è possibile scaricare l'applicazione Client VPN, insieme al file di configurazione, dal portale self-service. Per i passaggi per scaricare il client e il file di configurazione dal portale self-service, consulta [the section called "Scarica Client VPN"](#). Dopo aver scaricato e installato l'applicazione e il file, vai [at the section called "Fase 3: Connettersi alla VPN"](#).

In alternativa, scarica e installa un'applicazione client OpenVPN sul dispositivo da cui vuoi stabilire la connessione VPN.

Fase 2: ottenere il file di configurazione dell'endpoint Client VPN

Ottieni il file di configurazione degli endpoint Client VPN dal tuo amministratore. Il file di configurazione include le informazioni sugli endpoint Client VPN e i certificati richiesti per stabilire una connessione VPN.

In alternativa, se l'amministratore di Client VPN ha configurato un portale self-service per l'endpoint Client VPN, puoi scaricare tu stesso l'ultima versione del client AWS fornito e l'ultima versione del file di configurazione dell'endpoint Client VPN. Per ulteriori informazioni, consulta [Scarica il file AWS Client VPN dal portale self-service](#).

Fase 3: Connettersi alla VPN

Importa il file di configurazione dell'endpoint Client VPN nel client AWS fornito o nell'applicazione client OpenVPN e connettiti alla VPN. Per i passaggi per connettersi a una VPN, inclusa

l'importazione di uno o più file di configurazione degli endpoint per un AWS determinato client, consulta i seguenti argomenti:

- [Connect a un AWS Client VPN endpoint utilizzando un client AWS fornito](#)
- [Connect a AWS Client VPN endpoint che utilizza un client OpenVPN](#)

Per gli endpoint Client VPN che utilizzano l'autenticazione di Active Directory, ti verrà richiesto di immettere il nome utente e la password. Se l'autenticazione a più fattori è stata abilitata per la directory, ti verrà anche chiesto di immettere il codice MFA.

Per gli endpoint Client VPN che utilizzano l'autenticazione federata basata su SAML (single sign-on), il client AWS fornito apre una finestra del browser sul computer. Ti verrà richiesto di immettere le credenziali aziendali prima di connetterti all'endpoint Client VPN.

Scarica il file AWS Client VPN dal portale self-service

Il portale self-service è una pagina Web che consente di scaricare la versione più recente del client AWS fornito e le versioni più recenti dei file di configurazione degli endpoint Client VPN. Se l'amministratore dell'endpoint Client VPN ha preconfigurato uno o più file di configurazione per il client Client VPN, è possibile scaricare e installare l'applicazione Client VPN insieme a tali file di configurazione da questo portale.

Note

Se sei un amministratore e desideri configurare il portale self-service, consulta gli [endpoint Client VPN](#) nella Guida per l'AWS Client VPN amministratore.

Prima di iniziare, devi disporre dell'ID di ogni endpoint Client VPN che desideri scaricare.

L'amministratore dell'endpoint Client VPN può fornirti l'ID o può fornirti un URL del portale self-service che includa l'ID. Per connessioni endpoint multiple avrai bisogno dell'ID endpoint per ogni profilo a cui desideri connetterti.

Per accedere al portale self-service

1. Vai al portale self-service all'indirizzo <https://self-service.clientvpn.amazonaws.com/> o utilizza l'URL che ti è stato fornito dall'amministratore.

2. Se necessario, immetti l'ID dell'endpoint Client VPN, ad esempi, `cvpn-endpoint-0123456abcd123456`. Scegli Next (Successivo).
3. Immetti il nome utente e la password e scegli Sign In (Accedi). È lo stesso nome utente e la stessa password che hai utilizzato per connetterti all'endpoint Client VPN.
4. Nel portale self-service puoi effettuare le seguenti operazioni:
 - Scaricare la versione più recente del file di configurazione del client per l'endpoint Client VPN. Se desideri connetterti a più endpoint, dovrai scaricare il file di configurazione per ogni endpoint.
 - Scarica l'ultima versione del client AWS fornito per la tua piattaforma.
5. Ripeti questi passaggi per ogni file di configurazione dell'endpoint per cui desideri creare un profilo di connessione.

Connect a un AWS Client VPN endpoint utilizzando un client AWS fornito

È possibile connettersi a un endpoint Client VPN utilizzando il client AWS fornito, supportato su Windows, macOS e Ubuntu. Il client AWS fornito supporta anche fino a cinque connessioni simultanee e direttive OpenVPN.

Argomenti

- [Support per connessioni simultanee](#)
- [Direttive OpenVPN](#)

Sicurezza

La sicurezza è la massima priorità nel client fornito. AWS Rilasciamo regolarmente patch per migliorare il livello di sicurezza dell'applicazione. Il client fornito da AWS include diverse funzionalità di sicurezza uniche rispetto ad altri client OpenVPN, tra cui l'autenticazione SAML, il Client Routes Enforcement e il monitoraggio delle impostazioni del dispositivo.

Sebbene il client AWS fornito sia progettato per mitigare le minacce provenienti da un ambiente di rete mal configurato o compromesso, non è responsabile della modifica dell'ambiente o dell'eliminazione delle minacce esterne alla fonte. Il client AWS fornito si affida ai clienti per mantenere un ambiente sicuro e ben configurato. Questo include:

- Prevenzione di modifiche o abusi non autorizzati da parte degli utenti locali
- Limitazione dei privilegi amministrativi agli utenti attendibili
- Mantenimento delle patch up-to-date di sicurezza

Support per connessioni simultanee utilizzando un client AWS fornito

Il client AWS fornito consente di connettersi a più sessioni simultanee. Ciò è utile se hai bisogno di accedere alle risorse in più AWS ambienti e disponi di endpoint diversi per tali risorse. Ad esempio, potresti aver bisogno di accedere a un database in un ambiente su un endpoint diverso dall'endpoint a cui sei attualmente connesso, ma non desideri disconnettere la connessione corrente. Per

consentire al client AWS fornito di connettersi alle sessioni correnti, scaricate il file di configurazione creato dall'amministratore per ogni endpoint, quindi create un profilo di connessione per ogni file. Utilizzando il client AWS fornito, è quindi possibile connettersi a più sessioni senza disconnettersi da nessuna sessione attualmente aperta. Questa funzionalità è supportata solo per i client AWS forniti. Per i passaggi per connettersi a sessioni simultanee, consulta quanto segue:

- [Connect utilizzando il client AWS fornito per Windows](#)
- [Connect utilizzando il client AWS fornito per macOS](#)
- [Connect utilizzando il client AWS fornito per Linux](#)

Quando ci si connette a più endpoint, Client VPN implementa controlli per garantire che non vi siano conflitti con altre connessioni endpoint aperte, ad esempio, se due sessioni hanno blocchi CIDR o politiche di routing in conflitto; o se sei già connesso con una connessione tunnel completa. Se il controllo rileva conflitti, non verrà stabilita una connessione finché non si sceglie una connessione diversa che non sia in conflitto con la connessione aperta o non ci si disconnette dalla sessione aperta che causa il conflitto.

Le connessioni DNS simultanee sono consentite. Verrà applicato il server DNS di una delle connessioni abilitate al DNS. A seconda del server DNS, è possibile che venga richiesta l'autenticazione durante la riconnessione.

Note

Il numero massimo di sessioni simultanee consentite è cinque.

Direttive OpenVPN

Il client AWS fornito supporta le seguenti direttive OpenVPN. Per ulteriori informazioni su queste direttive, consulta la documentazione sul sito Web di [OpenVPN](#).

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- block-outside-dns

- ca
- cert
- cipher
- client
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- bb
- dhcp-option
- ifconfig-ipv6
- inactive
- keepalive
- Chiave
- mssfix
- nobind
- persist-key
- persist-tun
- ping
- uscita ping
- ping-restart
- proto
- pull
- pull-filter
- rcvbuf
- remote
- remote-cert-tls
- remote-random-hostname

- `reneg-sec`
- `resolv-retry`
- `route`
- `route-ipv6`
- `server-poll-timeout`
- `static-challenge`
- `tocca e dormi`
- `tun-mtu`
- `tun-mtu-extra`
- `verb`
- `verify-x509-name`

AWS Client VPN per Windows

Queste sezioni descrivono come stabilire una connessione VPN utilizzando il client AWS fornito per i sistemi Windows x64 e Windows Arm64. Puoi scaricare e installare il client dalla pagina [Download di Client VPN AWS](#). Il client AWS fornito non supporta gli aggiornamenti automatici.

Requisiti

Il client AWS fornito supporta i sistemi Windows x64 e Arm64. Per ogni sistema operativo è richiesto quanto segue:

Sistemi operativi Windows Arm64

- Windows 11 (sistema operativo a 64 bit, processore Arm64)
- .NET Framework 4.8.1 o versione successiva

Note

Questa applicazione include processi in background che utilizzano l'emulazione Arm64. Questa funzionalità è completamente supportata e abilitata di default sui dispositivi Windows 11 Arm64, garantendo un funzionamento senza interruzioni senza alcuna configurazione aggiuntiva. Per ulteriori informazioni, consulta [Come funziona l'emulazione](#) su Arm.

Sistemi operativi Windows x64

- Windows 11 (sistema operativo a 64 bit, processore x64)
- .NET Framework 4.7.2 o superiore

Note

Per i sistemi operativi Windows x64 e Arm64, gli endpoint Client VPN che utilizzano l'autenticazione SAML-based federata (Single Sign-on), il client riserva le porte TCP 8096-8115 sul computer.

Prima di iniziare assicurati che l'amministratore Client VPN abbia [creato un endpoint Client VPN](#) e fornito il [file di configurazione dell'endpoint Client VPN](#). Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

Argomenti

- [Connect to \(Connettiti a\) AWS Client VPN con un AWS client fornito per Windows](#)
- [Compatibilità del software di sicurezza degli endpoint](#)
- [AWS Client VPN per le note di rilascio di Windows](#)

Connect to (Connettiti a) AWS Client VPN con un AWS client fornito per Windows

Prima di iniziare, assicurati di leggere i [requisiti](#). Il client AWS fornito viene anche chiamato client AWS VPN nei passaggi seguenti.

Per connettersi utilizzando il AWS client fornito per sistemi Windows x64 o Windows Arm64-based :

1. Apri l'app AWS VPN Client.
2. Scegliere File, Manage Profiles (Gestisci profili).
3. Scegliere Add Profile (Aggiungi profilo).
4. In Display Name (Nome visualizzato), immettere un nome per il profilo.
5. Per VPN Configuration File (File di configurazione VPN), seleziona il file di configurazione ricevuto dall'amministratore Client VPN e scegli Add Profile (Aggiungi profilo).

6. Se desideri creare più connessioni, ripeti i passaggi **Aggiungi profilo** per ogni file di configurazione che desideri aggiungere. Puoi aggiungere tutti i profili che desideri, ma puoi avere solo fino a cinque connessioni aperte.
7. Nella finestra **Client AWS VPN**, scegli il profilo a cui desideri connetterti, quindi scegli **Connetti**. Se l'endpoint **Client VPN** è stato configurato per utilizzare l'autenticazione basata su credenziali, ti verrà richiesto di immettere un nome utente e una password. Ripeti questo passaggio per ogni connessione al profilo che desideri avviare, collegando fino a cinque endpoint simultanei.

Note

Se un profilo a cui ti connetti è in conflitto con una sessione attualmente aperta, non sarai in grado di effettuare la connessione. Scegli una nuova connessione o disconnettiti dalla sessione che causa il conflitto.

8. Per visualizzare le statistiche relative a una connessione, scegli **Connessione** nella finestra del client **AWS VPN**, scegli **Mostra dettagli**, quindi scegli la connessione di cui desideri visualizzare i dettagli.
9. Per disconnettere una connessione, scegli una connessione nella finestra del client **AWS VPN**, quindi scegli **Disconnetti**. Se hai più connessioni aperte, devi chiudere ogni connessione singolarmente. In alternativa, scegliere l'icona client sulla barra delle applicazioni di Windows e selezionare **Disconnect** (**Disconnetti**).

Compatibilità del software di sicurezza degli endpoint

I prodotti aziendali per la sicurezza degli endpoint come firewall basati su host, agenti di rilevamento e risposta degli endpoint (EDR) e software antivirus possono talvolta interferire con le connessioni **Client VPN**. AWS Se si verificano problemi di connettività quando si utilizza il client per Windows AWS fornito, potrebbe essere necessario configurare le esclusioni nel software di sicurezza degli endpoint.

AWS Percorsi eseguibili Client VPN

Il client AWS fornito per Windows installa i seguenti eseguibili chiave. Questi percorsi potrebbero essere necessari per configurare le regole del firewall, gli elenchi di applicazioni consentite o le politiche di sicurezza degli endpoint.

Applicazione client VPN

```
C:\Program Files\Amazon\AWS VPN Client\AWSVPNClient.exe
```

Processo OpenVPN

```
C:\Program Files\Amazon\AWS VPN Client\Resources\openvpn\acvc-openvpn.exe
```

Questo è il processo principale che stabilisce e mantiene la connessione al tunnel VPN.

Servizio Windows

```
C:\Program Files\Amazon\AWS VPN Client\AWSVPNClient.Service.exe
```

Requisiti di rete

Il client AWS fornito richiede l'accesso alla rete in uscita all'endpoint Client VPN per stabilire una connessione VPN. Assicurati che il firewall o il software di sicurezza degli endpoint consentano il traffico in uscita dal `acvc-openvpn.exe` processo alla porta e al protocollo configurati sull'endpoint Client VPN.

Configurazione delle esclusioni di sicurezza degli endpoint

Se il prodotto di sicurezza degli endpoint interferisce con la connettività client AWS fornita, esamina le seguenti categorie di esclusione con il tuo amministratore della sicurezza:

Process-based esclusioni

Aggiungi gli eseguibili elencati all'elenco dei processi o [the section called “AWS Percorsi eseguibili Client VPN”](#) all'elenco di esclusione dei processi consentiti o all'elenco di esclusione del prodotto di sicurezza degli endpoint.

Network-based esclusioni

Consenti il traffico in uscita dal `acvc-openvpn.exe` processo alla porta e al protocollo dell'endpoint Client VPN.

Path-based esclusioni

Escludi la directory di installazione del client AWS fornita dalla scansione in tempo reale o dall'analisi comportamentale:

C:\Program Files\Amazon\AWS VPN Client\

Important

Le istruzioni di configurazione prescrittive per specifici prodotti di sicurezza degli endpoint di terze parti non rientrano nell'ambito della AWS documentazione a causa della variabilità tra le versioni e le configurazioni del prodotto. Consultate la documentazione del fornitore della sicurezza degli endpoint per istruzioni dettagliate sulla configurazione delle esclusioni per il vostro prodotto specifico.

AWS Client VPN per le note di rilascio di Windows

La tabella seguente contiene le note di rilascio e i collegamenti per il download per le versioni correnti e precedenti di AWS Client VPN per sistemi Windows x64 e Windows Arm64-based.

Note

Continuiamo a fornire correzioni di usabilità e sicurezza con ogni versione. Ti consigliamo vivamente di utilizzare la versione più recente per ogni piattaforma. Le versioni precedenti potrebbero essere affette da problemi di and/or sicurezza relativi all'usabilità. Per informazioni dettagliate, consulta le note di rilascio.

Versione	Modifiche	Data	Link per il download e SHA256
5.3.7 (x64 e Arm64)	<ul style="list-style-type: none"> Miglioramenti e correzioni di bug minori. 	15 giugno 2026	<ul style="list-style-type: none"> Scarica la versione 5.3.7 di Windows x64 <p>sha256:64 ee088e60b 3eab83fba e6b1d1db5</p>

Versione	Modifiche	Data	Link per il download e SHA256
			6da1156e8 094ce0b1d 3fdf6e3e2 c285b731
			<ul style="list-style-type: none">Scarica Windows Arm64 versione 5.3.7
			sha256:38 412d18b80 f9a13826e 0a4422f40 3a93fed51 b067f15af feb0727d2 3e76c7d9

Versione	Modifiche	Data	Link per il download e SHA256
5.3.6 (x64 e Arm64)	<ul style="list-style-type: none">• Modifiche ripristinate rispetto alla versione 5.3.5	28 maggio 2026	<ul style="list-style-type: none">• Scarica la versione 5.3.6 di Windows x64 sha256: a16212bdd e30c1547a cb33aae45 a72b12615 dc6e30839 eb0b1a36d 815279e95b• Scarica Windows Arm64 versione 5.3.6 sha256: bc02e64ef ef9559fc9 91553e10b bc605bc27 42f1d2015 74adcf4d7 7d500ee0d7

Versione	Modifiche	Data	Link per il download e SHA256
5.3.5 (x64 e Arm64)	<ul style="list-style-type: none">Miglioramenti e correzioni di bug minori.Assetto di sicurezza migliorato	27 maggio 2026	<ul style="list-style-type: none">Scarica la versione 5.3.5 di Windows x64 sha256:8c fc8f5d7de 80c5b4673 d1c9874b1 50ecc3133 e9628e172 08b5a4de3 0a050608Scarica Windows Arm64 versione 5.3.5 sha256:14 57fe9a852 1cc5b4b07 539ca5799 5714efb94 3265ad713 4e464c1cc 6698e6d0

Versione	Modifiche	Data	Link per il download e SHA256
5.3.4 (x64 e Arm64)	<ul style="list-style-type: none">• Miglioramenti e correzioni di bug minori.• Assetto di sicurezza migliorato	27 marzo 2026	<ul style="list-style-type: none">• Scarica la versione 5.3.4 di Windows x64 sha256:81 a5c510162 4c5f74de8 afdc816f 03ea8ff9e 8c6a5eaa8 890a95779 a94dbe41• Scarica Windows Arm64 versione 5.3.4 sha256:34 10282ebb0 24e64812a 63668b301 17657d470 ed4c51f05 e96fc812b 8871587d

Versione	Modifiche	Data	Link per il download e SHA256
5.3.3 (x64 e Arm64)	<ul style="list-style-type: none">Risolti gli errori di connessione nella versione 5.3.2	28 febbraio 2026	<ul style="list-style-type: none">Scarica la versione 5.3.3 di Windows x64 sha256: bbaebb977 b270add64 97c941505 fed5913b5 8056e980e 372170733 7dc051ac86Scarica Windows Arm64 versione 5.3.3 sha256: c30b6d012 1a5070643 fdbebc27e 7f9569d57 4a5698631 480becb5c b96cac9fde

Versione	Modifiche	Data	Link per il download e SHA256
5.3.2 (x64 e Arm64)	<ul style="list-style-type: none">• Miglioramenti e correzioni di bug minori.• Posizione di sicurezza migliorata.	17 febbraio 2026	<ul style="list-style-type: none">• Scarica la versione 5.3.2 di Windows x64 sha256: dd1e4fb67 18dddbf13 a5aee5421 75761bf8e d854290c5 76a488b98 173a0ccf92• Scarica Windows Arm64 versione 5.3.2 sha256: d2d18d91c a9ef53cc5 57434db18 ef5d0002e 7825a998f 2d739eac4 43b034af00

Versione	Modifiche	Data	Link per il download e SHA256
5.3.1 (x64 e Arm64)	Miglioramenti e correzioni di bug minori.	30 settembre 2025	<ul style="list-style-type: none">• Scarica la versione 5.3.1 di Windows x64 sha256: b71ddbc78 230630963 acf3ebba7 afeb6e525 99843091f f589aed6a fce4c9eb06• Scarica Windows Arm64 versione 5.3.1 sha256: e691bdb0b dcb55b3da 36f4fb2e5 198f20f18 78dc22a00 bf55bc660 999698500b

Versione	Modifiche	Data	Link per il download e SHA256
5.3.0 (Arm64)	<p>Nuovo AWS Client VPN supporto per i sistemi Arm64-based operativi Windows.</p> <p>Questa versione include tutti gli aggiornamenti della versione di Windows (x64) 5.3.0.</p>	26 agosto 2025	<p>Scarica Windows Arm64 versione 5.3.0</p> <p>sha256:3f 1be6b487a f8307dafb b0f7737cd 597cf71dc 64dcd3177 5aeefbf91 d04b8dce</p>
5.3.0	<ul style="list-style-type: none"> • Miglioramenti minori. • È stato aggiunto il supporto per le connessioni IPv6 	14 agosto 2025	<p>Scarica la versione 5.3.0 di Windows x64</p> <p>sha256: e3cf1aff6 e14d79aa4 4378229a3 a0602a9e9 c2a0c6d0d 055df9014 40b6d1454a</p>

Versione	Modifiche	Data	Link per il download e SHA256
5.2.2	Posizione di sicurezza migliorata.	2 giugno 2025	Scarica la versione 5.2.2 sha256: f27cb0eed 7c9c5354c aa5d7e375 95eefbb04 8d7481bf6 98b2e5fb6 53b667c190
5.2.1	<ul style="list-style-type: none"> È stato aggiunto il supporto per il <code>ping-exit</code> flag OpenVPN. Aggiornata la libreria OpenSSL. Miglioramenti e correzioni di bug minori. 	21 aprile 2025	Non è più supportato.
5.2.0	<ul style="list-style-type: none"> Miglioramenti minori. È stato aggiunto il supporto per Client Route Enforcement. 	8 aprile 2025	Non è più supportato.
5.1.0	<ul style="list-style-type: none"> È stato risolto un problema che causava la riconnessione automatica della AWS Client VPN versione 5.0.x alla VPN dopo una disconnessione per timeout di inattività. Miglioramenti e correzioni di bug minori. 	17 marzo 2025	Non è più supportato.
5.0.2	<ul style="list-style-type: none"> È stato risolto un problema DNS per le connessioni simultanee. Risolti alcuni problemi sporadici che si verificavano durante l'installazione di nuovi adattatori TAP. 	24 febbraio 2025	Non è più supportato.

Versione	Modifiche	Data	Link per il download e SHA256
5.0.1	È stato risolto un problema che causava sporadici errori di connessione VPN nella versione 5.0.0 del client Windows.	30 gennaio 2025	Non è più supportato.
5.0.0	<ul style="list-style-type: none"> È stato aggiunto il supporto per le connessioni simultanee. Aggiornata la versione del driver TAP. È stata aggiornata l'interfaccia utente grafica. Miglioramenti e correzioni di bug minori. 	21 gennaio 2025	Non è più supportato.
4.1.0	Miglioramenti e correzioni di bug minori.	12 novembre 2024	Non è più supportato.
4.0.0	Miglioramenti minori.	25 settembre 2024	Scarica la versione 4.0.0 sha256:65 32f911385 ec8fac149 4d0847c8f 90a999b3b d7380844e 2ea4318e9 db4a2ebc

Versione	Modifiche	Data	Link per il download e SHA256
3.14.2	È stato aggiunto il supporto per il <code>mssfix</code> flag OpenVPN.	4 settembre 2024	Scarica la versione 3.14.2 sha256: c171639d7 e07e5fd48 998cf76f7 4e6e49e5c be3356c62 64a67b4a9 bf473b5f5d
3.14.1	Miglioramenti e correzioni di bug minori.	22 agosto 2024	Scarica la versione 3.14.1 sha256: f743a7b4b c82daa4b8 03c299439 0529997bb 57a4bb54d 1f5195ab2 8827283335
3.14.0	<ul style="list-style-type: none"> È stato aggiunto il supporto per il <code>tap-sleep</code> flag OpenVPN. Aggiornate le librerie OpenVPN e OpenSSL. 	12 agosto 2024	Scarica la versione 3.14.0 sha256:81 2fb2f6d26 3288c664d 598f6bd70 e3f601d11 dcb89e63b 281b0a96b 96354516

Versione	Modifiche	Data	Link per il download e SHA256
3.13.0	Aggiornate le librerie OpenVPN e OpenSSL.	29 luglio 2024	Scarica la versione 3.13.0 sha256: c9cc896e8 1a7441184 0951e349e ed9384507 c53337fb7 03c5ec64d 522c29388b
3.12.1	È stato risolto il problema che impediva alla versione 3.12.0 del client Windows di stabilire una connessione VPN per alcuni utenti.	18 luglio 2024	Scarica la versione 3.12.1 sha256:5e d34aee6c0 3aa281e62 5acdbed27 2896c6704 6364a9e58 46ca697e0 5dbfec08
3.12.0	<ul style="list-style-type: none">• Riconnettiti automaticamente quando gli intervalli della rete locale cambiano.• È stato rimosso il focus automatico dell'applicazione quando si è connessi agli endpoint SAML.	21 maggio 2024	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
3.11.2	È stato risolto un problema di autenticazione SAML con Chromium-based i browser a partire dalla versione 123.	11 aprile 2024	Scarica la versione 3.11.2 sha256:8b a258dd15b ea3e861ad ad108f8a6 d6d4bcd8f e42cb9ef8 bbc294e72 f365c7cc
3.11.1	<ul style="list-style-type: none"> • È stata risolta un'azione di buffer overflow che poteva potenzialmente consentire a un attore locale di eseguire comandi arbitrari con autorizzazioni elevate. • Posizione di sicurezza migliorata. 	16 febbraio 2024	Scarica la versione 3.11.1 sha256: fb67b60aa 837019795 8a11ea6f5 7d5bc0512 279560b52 a857ae34c b321eaefd0
3.11.0	<ul style="list-style-type: none"> • È stato risolto un problema di connettività causato dalle macchine virtuali Windows. • Problemi di connettività risolti per alcune configurazioni LAN. • Accessibilità migliorata. 	6 dicembre 2023	Scarica la versione 3.11.0 sha256: 9b6b7def9 9d76c59a9 7b067b6a7 3bdc6ee1c 6b89a2063 286f542e9 6b32df5ae9

Versione	Modifiche	Data	Link per il download e SHA256
3.10.0	<ul style="list-style-type: none"> È stato risolto un problema di connettività quando NAT64 è abilitato nella rete client. È stato risolto un problema di connettività che si verificava quando gli adattatori di rete venivano installati sul computer client. Hyper-V Miglioramenti e correzioni di bug minori. 	24 agosto 2023	Scarica la versione 3.10.0 sha256: d46721aad 40ccb816f 163e406c3 66ff03b11 20abbb43a 20607e06d 3b1fa8667f
3.9.0	Posizione di sicurezza migliorata.	3 agosto 2023	Scarica la versione 3.9.0 sha256: de9a3800e a23491555 40bd32bba e472404c6 36d8d8267 a0e1fb217 3a8aae21ed
3.8.0	Posizione di sicurezza migliorata.	15 luglio 2023	Non è più supportato
3.7.0	Sono state ripristinate le modifiche rispetto alla versione 3.6.0.	15 luglio 2023	Non è più supportato
3.6.0	Posizione di sicurezza migliorata.	14 luglio 2023	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
3.5.0	Miglioramenti e correzioni di bug minori.	3 aprile 2023	Non è più supportato
3.4.0	Sono state ripristinate le modifiche rispetto alla versione 3.3.0.	28 marzo 2023	Non è più supportato
3.3.0	Miglioramenti e correzioni di bug minori.	17 marzo 2023	Non è più supportato
3.2.0	<ul style="list-style-type: none">È stato aggiunto il supporto per il flag OpenVPN «verify-x509-name».Il client di sincronizzazione viene aggiornato automaticamente quando vengono rese disponibili nuove versioni.È stata aggiunta la possibilità di installare automaticamente nuove versioni del client quando disponibili.	23 gennaio 2023	Non è più supportato
3.1.0	Posizione di sicurezza migliorata.	23 maggio 2022	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
3.0.0	<ul style="list-style-type: none"> • Aggiunto il supporto per Windows 11. • Risolto il problema del nome del driver di Windows TAP che influenzava altri nomi di driver. • Risolto il problema del messaggio del banner che non veniva visualizzato quando si utilizza l'autenticazione federata. • Visualizzazione fissa del testo del banner per un testo più lungo. • Posizione di sicurezza migliorata. 	3 marzo 2022	Non è più supportato
2.0.0	<ul style="list-style-type: none"> • Aggiunto il supporto per il testo del banner dopo aver stabilito una nuova connessione. • Rimossa la possibilità di utilizzare pull-filter in relazione a echo, cioè pull-filter * echo • Miglioramenti e correzioni di bug minori. 	20 gennaio 2022	Non è più supportato
1.3.7	<ul style="list-style-type: none"> • In alcuni casi è stato corretto il tentativo di connessione di autenticazione federata. • Miglioramenti e correzioni di bug minori. 	8 novembre 2021	Non è più supportato
1.3.6	<ul style="list-style-type: none"> • Aggiunto il supporto per i flag OpenVPN: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout. • Miglioramenti e correzioni di bug minori. 	20 settembre 2021	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
1.3.5	Patch per eliminare file di log di Windows di grandi dimensioni.	16 agosto 2021	Non è più supportato
1.3.4	<ul style="list-style-type: none"> • Aggiunto il supporto per il flag OpenVPN: dhcp-option. • Miglioramenti e correzioni di bug minori. 	4 agosto 2021	Non è più supportato
1.3.3	<ul style="list-style-type: none"> • Aggiunto il supporto per i flag OpenVPN: inactive, pull-filter, route. • Risolto un problema che causava un arresto anomalo dell'app durante la disconnessione o l'uscita. • Risolto un problema legato ai nomi utente di Active Directory con barra rovesciata. • Risolto l'arresto anomalo dell'app durante la manipolazione dell'elenco dei profili all'esterno dell'app. • Miglioramenti e correzioni di bug minori. 	1 luglio 2021	Non è più supportato
1.3.2	<ul style="list-style-type: none"> • Aggiungere la prevenzione delle perdite IPv6, quando è configurata. • Risolto un potenziale arresto anomalo quando si utilizza l'opzione Show Details (Mostra dettagli) in Connection (Connessione). 	12 maggio 2021	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
1.3.1	<ul style="list-style-type: none"> • Aggiunto il supporto per più certificati client con lo stesso oggetto. I certificati scaduti verranno ignorati. • Risolta la conservazione dei log locali per ridurre l'utilizzo del disco. • Aggiunto il supporto per la direttiva OpenVPN 'route-ipv6'. • Miglioramenti e correzioni di bug minori. 	5 aprile 2021	Non è più supportato
1.3.0	Sono state aggiunte funzionalità di supporto come la segnalazione degli errori, l'invio di log di diagnostica e l'analisi.	8 marzo 2021	Non è più supportato
1.2.7	<ul style="list-style-type: none"> • Aggiunto il supporto per la direttiva OpenVPN 'cryptoapicert'. • Sono state risolte le route obsolete tra le connessioni. • Miglioramenti e correzioni di bug minori. 	25 febbraio 2021	Non è più supportato
1.2.6	Miglioramenti e correzioni di bug minori.	26 ottobre 2020	Non è più supportato
1.2.5	<ul style="list-style-type: none"> • Aggiunto il supporto per i commenti nella configurazione di OpenVPN. • Aggiunto un messaggio di errore per gli errori di handshake TLS. 	8 ottobre 2020	Non è più supportato
1.2.4	Miglioramenti e correzioni di bug minori.	1 settembre 2020	Non è più supportato
1.2.3	Ripristina le modifiche nella versione 1.2.2.	20 agosto 2020	Non è più supportato

Versione	Modifiche	Data	Link per il download e SHA256
1.2.1	Miglioramenti e correzioni di bug minori.	1 luglio 2020	Non è più supportato
1.2.0	<ul style="list-style-type: none"> • Aggiunto il supporto per l'autenticazione federata basata su SAML 2.0. • Il supporto per la piattaforma Windows 7 è obsoleto. 	19 maggio 2020	Non è più supportato
1.1.1	Miglioramenti e correzioni di bug minori.	21 aprile 2020	Non è più supportato
1.1.0	<ul style="list-style-type: none"> • Aggiunto il supporto per la funzionalità OpenVPN static challenge echo per nascondere o mostrare il testo visualizzato nell'interfaccia utente. • Miglioramenti e correzioni di bug minori. 	9 marzo 2020	Non è più supportato
1.0.0	Versione iniziale.	4 febbraio 2020	Non è più supportato

AWS Client VPN per macOS

Queste sezioni descrivono come stabilire una connessione VPN utilizzando il client AWS fornito per macOS. Puoi scaricare e installare il client dalla pagina [Download di Client VPN AWS](#). Il client AWS fornito non supporta gli aggiornamenti automatici.

Requisiti

Per utilizzare il client AWS fornito per macOS, è necessario quanto segue:

- macOS Sonoma (14.0), Sequoia (15.0) o Tahoe (26.0)
- compatibile con ARM64 x86_64 o processore.

- Per Client VPN, endpoint che utilizzano l'autenticazione federata basata su SAML (single sign-on), il client riserva le porte TCP 8096-8115 sul computer.

Argomenti

- [Connect to \(Connettiti a\) AWS Client VPN con un AWS client fornito per macOS](#)
- [AWS Client VPN per macOS: note di rilascio](#)

Connect to (Connettiti a) AWS Client VPN con un AWS client fornito per macOS

Prima di iniziare assicurati che l'amministratore Client VPN abbia [creato un endpoint Client VPN](#) e fornito il [file di configurazione dell'endpoint Client VPN](#). Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

Assicurati, inoltre, di leggere i [requisiti](#). Il client AWS fornito viene anche chiamato client AWS VPN nei passaggi seguenti.

Per connettersi utilizzando il AWS client fornito per macOS

1. Apri l'app AWS VPN Client.
2. Scegliere File, Manage Profiles (Gestisci profili).
3. Scegliere Add Profile (Aggiungi profilo).
4. In Display Name (Nome visualizzato), immettere un nome per il profilo.
5. Per VPN Configuration File (File di configurazione VPN), seleziona il file di configurazione ricevuto dall'amministratore Client VPN e scegli Add Profile (Aggiungi profilo).
6. Se desideri creare più connessioni, ripeti i passaggi Aggiungi profilo per ogni file di configurazione che desideri aggiungere. Puoi aggiungere tutti i profili che desideri, ma puoi avere solo fino a cinque connessioni aperte.
7. Nella finestra Client AWS VPN, scegli il profilo a cui desideri connetterti, quindi scegli Connetti. Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione basata su credenziali, ti verrà richiesto di immettere un nome utente e una password. Ripeti questo passaggio per ogni connessione al profilo che desideri avviare, collegando fino a cinque endpoint simultanei.

Note

Se un profilo a cui ti connetti è in conflitto con una sessione attualmente aperta, non sarai in grado di effettuare la connessione. Scegli una nuova connessione o disconnettiti dalla sessione che causa il conflitto.

8. Per visualizzare le statistiche relative a una connessione, scegli Connessione nella finestra del client AWS VPN, scegli Mostra dettagli, quindi scegli la connessione di cui desideri visualizzare i dettagli.
9. Per disconnettere una connessione, scegli una connessione nella finestra del client AWS VPN, quindi scegli Disconnetti. Se hai più connessioni aperte, devi chiudere ogni connessione singolarmente.

AWS Client VPN per macOS: note di rilascio

La tabella seguente contiene le note di rilascio e i link per il download AWS Client VPN per la versione corrente e precedente di macOS.

Note

Continuiamo a fornire correzioni di usabilità e sicurezza con ogni versione. Ti consigliamo vivamente di utilizzare la versione più recente per ogni piattaforma. Le versioni precedenti potrebbero essere influenzate da problemi di and/or sicurezza relativi all'usabilità. Per informazioni dettagliate, consulta le note di rilascio.

Versione	Modifiche	Data	Collegamento per il download
5.3.5	<ul style="list-style-type: none"> • Miglioramenti e correzioni di bug minori. • Assetto di sicurezza migliorato • Ha abilitato l'aggiornamento automatico al client ARM64 nativo per utenti ARM-based Mac negli aggiornamenti 	14 maggio 2026	<ul style="list-style-type: none"> • Scarica macOS ARM64 versione 5.3.5 <pre>sha256:048c9011b7c ea43720cb92d7c2fe0 64c8d853b391ee4994 08736cba5d9111652</pre>

Versione	Modifiche	Data	Collegamento per il download
	enti futuri, eliminando la necessità di migrazione manuale dal Intel-based client in esecuzione sotto il livello di traduzione Rosetta		<ul style="list-style-type: none"> Scarica macOS x64 versione 5.3.5 <pre>sha256:64a84f529a0 9b2ee9756dd8f5e193 b9624b3239bcd76d9f 20411a72d1f93887c</pre>
5.3.4	<ul style="list-style-type: none"> Rimosso il requisito del livello di compatibilità Intel (Rosetta) sulle macchine ARM Miglioramenti e correzioni di bug minori. 	17 febbraio 2026	Non è più supportato.
5.3.3	<ul style="list-style-type: none"> Miglioramenti e correzioni di bug minori. Posizione di sicurezza migliorata. 	26 dicembre 2025	Non è più supportato.
5.3.2	<ul style="list-style-type: none"> Aggiunto il supporto nativo per l'architettura Apple Silicon e un nuovo programma di installazione macOS ARM64. Miglioramenti e correzioni di bug minori. 	27 ottobre 2025	Non è più supportato.
5.3.1	<ul style="list-style-type: none"> Miglioramenti e correzioni di bug minori. 	9 settembre 2025	Non è più supportato.
5.3.0	<ul style="list-style-type: none"> Miglioramenti minori. È stato aggiunto il supporto per le connessioni IPv6. 	14 agosto 2025	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
5.2.1	<ul style="list-style-type: none"> • Aggiunto il supporto per il flag ping-exit OpenVPN. • Aggiornata la libreria OpenSSL. • Posizione di sicurezza migliorata. • Miglioramenti e correzioni di bug minori. 	18 giugno 2025	Non è più supportato.
5.2.0	<ul style="list-style-type: none"> • Miglioramenti minori. • È stato aggiunto il supporto per Client Route Enforcement. 	8 aprile 2025	Non è più supportato.
5.1.0	<ul style="list-style-type: none"> • È stato risolto un problema che causava la riconnessione automatica della AWS Client VPN versione 5.0.x alla VPN dopo una disconnessione per timeout di inattività. • È stato risolto un problema che AWS Client VPN impediva di stabilire una connessione VPN per i file di configurazione con terminazioni di linea. Windows-style • Miglioramenti e correzioni di bug minori. 	17 marzo 2025	Non è più supportato.
5.0.3	Miglioramenti e correzioni di bug minori.	6 marzo 2025	Non è più supportato.
50,2	È stato risolto un problema che causava errori sporadici nella scelta di Connect.	17 febbraio 2025	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
5.0.1	È stato risolto un problema che impediva alla versione client 5.0.0 di stabilire una connessione VPN per i nomi di profilo contenenti spazi.	22 gennaio 2025	Non è più supportato.
5.0.0	<ul style="list-style-type: none"> È stato aggiunto il supporto per le connessioni simultanee. È stata aggiornata l'interfaccia utente grafica. Miglioramenti e correzioni di bug minori. 	21 gennaio 2025	Non è più supportato.
4.1.0	Miglioramenti e correzioni di bug minori.	12 novembre 2024	Non è più supportato.
4.0.0	Miglioramenti minori.	25 settembre 2024	Non è più supportato.
3.12.1	Aggiunto il supporto per il <code>mssfix</code> flag OpenVPN.	4 settembre 2024	Non è più supportato.
3.12.0	<ul style="list-style-type: none"> Aggiunto il supporto per il <code>tap-sleep</code> flag OpenVPN. Aggiornate le librerie OpenVPN e OpenSSL. 	12 agosto 2024	Non è più supportato.
3.11.0	<ul style="list-style-type: none"> Aggiornate le librerie OpenVPN e OpenSSL. 	29 luglio 2024	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
3.10.0	<ul style="list-style-type: none"> • Riconnettiti automaticamente quando gli intervalli della rete locale cambiano. • Risolto un problema di ripristino DNS durante lo switch di rete. • È stato rimosso il focus automatico dell'applicazione quando si è connessi agli endpoint SAML. 	21 maggio 2024	Non è più supportato.
3.9.2	<ul style="list-style-type: none"> • Risolto un problema di autenticazione SAML con Chromium-based i browser a partire dalla versione 123. • È stato aggiunto il supporto per macOS Sonoma. Supporto obsoleto per macOS Big Sur. • Posizione di sicurezza migliorata. 	11 aprile 2024	Non è più supportato.
3.9.1	<ul style="list-style-type: none"> • È stata risolta un'azione di buffer overflow che poteva potenzialmente consentire a un attore locale di eseguire comandi arbitrari con autorizzazioni elevate. • Barra di avanzamento del download dell'aggiornamento dell'applicazione fissa. • Posizione di sicurezza migliorata. 	16 febbraio 2024	Non è più supportato.
3.9.0	<ul style="list-style-type: none"> • Problemi di connettività risolti per alcune configurazioni LAN. • Accessibilità migliorata. 	6 dicembre 2023	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
3.8.0	<ul style="list-style-type: none"> È stato risolto un problema di connettività quando NAT64 è abilitato nella rete client. Miglioramenti e correzioni di bug minori. 	24 agosto 2023	Non è più supportato.
3.7.0	<ul style="list-style-type: none"> Posizione di sicurezza migliorata. 	3 agosto 2023	Non è più supportato.
3.6.0	<ul style="list-style-type: none"> Posizione di sicurezza migliorata. 	15 luglio 2023	Non è più supportato.
3.5.0	<ul style="list-style-type: none"> Sono state ripristinate le modifiche rispetto alla versione 3.4.0. 	15 luglio 2023	Non è più supportato.
3.4.0	<ul style="list-style-type: none"> Posizione di sicurezza migliorata. 	14 luglio 2023	Non è più supportato.
3.3.0	<ul style="list-style-type: none"> Aggiunto il supporto per macOS Ventura (13.0). Miglioramenti e correzioni di bug minori. 	27 aprile 2023	Non è più supportato.
3.2.0	<ul style="list-style-type: none"> È stato aggiunto il supporto per il flag OpenVPN «verify-x509-name». Il client di sincronizzazione viene aggiornato automaticamente quando vengono rese disponibili nuove versioni. È stata aggiunta la possibilità di installare automaticamente nuove versioni del client quando disponibili. 	23 gennaio 2023	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
3.1.0	<ul style="list-style-type: none"> • È stato aggiunto il supporto per macOS Monterey. • È stato risolto il problema di rilevamento del tipo di unità. • È stata migliorata la posizione di sicurezza. 	23 maggio 2022	Non è più supportato.
3.0.0	<ul style="list-style-type: none"> • Risolto il problema del messaggio banner che non veniva visualizzato quando si utilizza l'autenticazione federata. • Visualizzazione fissa del testo del banner per un testo più lungo. • Posizione di sicurezza migliorata. 	3 marzo 2022	Non è più supportato.
2.0.0	<ul style="list-style-type: none"> • Aggiunto il supporto per il testo del banner dopo aver stabilito una nuova connessione. • Rimossa la possibilità di utilizzare pull-filter in relazione a echo, cioè pull-filter * echo • Miglioramenti e correzioni di bug minori. 	20 gennaio 2022	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.4.0	<ul style="list-style-type: none">• Aggiunto il monitoraggio del server DNS durante la connessione. Se non corrispondono alle impostazioni della VPN le impostazioni verranno riconfigurate.• In alcuni casi è stato corretto il tentativo di connessione di autenticazione federata.• Miglioramenti e correzioni di bug minori.	9 novembre 2021	Non è più supportato.
1.3.5	<ul style="list-style-type: none">• Aggiunto il supporto per i flag OpenVPN: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout.• Miglioramenti e correzioni di bug minori.	20 settembre 2021	Non è più supportato.
1.3.4	<ul style="list-style-type: none">• Aggiunto il supporto per il flag OpenVPN: dhcp-option.• Miglioramenti e correzioni di bug minori.	4 agosto 2021	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.3.3	<ul style="list-style-type: none">• Aggiunto il supporto per i flag OpenVPN: inactive, pull-filter, route.• Risolto un problema legato ai nomi dei file di configurazione con spazi o Unicode.• Risolto un problema che causava un arresto anomalo dell'app durante la disconnessione o l'uscita.• Risolto un problema legato ai nomi utente di Active Directory con barra rovesciata.• Risolto l'arresto anomalo dell'app durante la manipolazione dell'elenco dei profili all'esterno dell'app.• Miglioramenti e correzioni di bug minori.	1 luglio 2021	Non è più supportato.
1.3.2	<ul style="list-style-type: none">• Aggiungere la prevenzione delle perdite IPv6, quando è configurata.• Risolto un potenziale arresto anomalo quando si utilizza l'opzione Show Details (Mostra dettagli) in Connection (Connessione).• Aggiungere la rotazione dei log del daemon.	12 maggio 2021	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.3.1	<ul style="list-style-type: none"> • Aggiunto il supporto per macOS Big Sur (10.16). • Risolto un problema che eliminava le impostazioni DNS configurate da altre applicazioni. • Risolto un problema che si presentava durante l'utilizzo di un certificato non valido per l'autenticazione reciproca che causava problemi di connessione. • Aggiunto il supporto per la direttiva OpenVPN 'route-ipv6'. • Miglioramenti e correzioni di bug minori. 	5 aprile 2021	Non è più supportato.
1.3.0	Sono state aggiunte funzionalità di supporto come la segnalazione degli errori, l'invio di log di diagnostica e l'analisi.	8 marzo 2021	Non è più supportato.
1.2.5	Miglioramenti e correzioni di bug minori.	25 febbraio 2021	Non è più supportato.
1.2.4	Miglioramenti e correzioni di bug minori.	26 ottobre 2020	Non è più supportato.
1.2.3	<ul style="list-style-type: none"> • Aggiunto il supporto per i commenti nella configurazione di OpenVPN. • Aggiunto un messaggio di errore per gli errori di handshake TLS. • Risolto un bug di disinstallazione che interessava alcuni utenti. 	8 ottobre 2020	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.2.2	Miglioramenti e correzioni di bug minori.	12 agosto 2020	Non è più supportato.
1.2.1	<ul style="list-style-type: none"> • Aggiunto il supporto per la disinstallazione dell'applicazione. • Miglioramenti e correzioni di bug minori. 	1 luglio 2020	Non è più supportato.
1.2.0	<ul style="list-style-type: none"> • Aggiunto il supporto per l'autenticazione federata basata su SAML 2.0. • Aggiunto il supporto per macOS Catalina (10.15). 	19 maggio 2020	Non è più supportato.
1.1.2	Miglioramenti e correzioni di bug minori.	21 aprile 2020	Non è più supportato.
1.1.1	<ul style="list-style-type: none"> • Corretto un problema di risoluzione DNS. • Corretto un problema di arresto anomalo dell'app causato da connessioni più lunghe. • Corretto un problema MFA. 	2 aprile 2020	Non è più supportato.
1.1.0	<ul style="list-style-type: none"> • Aggiunto il supporto per la configurazione DNS macOS. • Aggiunto il supporto per la funzionalità OpenVPN static challenge echo per nascondere o mostrare il testo visualizzato nell'interfaccia utente. • Miglioramenti e correzioni di bug minori. 	9 marzo 2020	Non è più supportato.
1.0.0	Versione iniziale.	4 febbraio 2020	Non è più supportato.

AWS Client VPN per Linux

Queste sezioni descrivono l'installazione del client AWS fornito per Linux e quindi la creazione di una connessione VPN utilizzando il client AWS fornito. Il client AWS fornito per Linux non supporta gli aggiornamenti automatici. Per gli aggiornamenti e i download più recenti, consulta [ilthe section called "Note di rilascio"](#).

Requisiti per la connessione a Client VPN con un AWS client fornito per Linux

Per utilizzare il client AWS fornito per Linux, è necessario quanto segue:

- Ubuntu 22.04 LTS (AMD64), Ubuntu 24.04 LTS (solo AMD64) o Ubuntu 26.04 LTS (solo AMD64)

Per gli endpoint Client VPN che utilizzano l'autenticazione SAML-based federata (Single Sign-on), il client riserva le porte TCP 8096-8115 sul computer.

Prima di iniziare assicurati che l'amministratore Client VPN abbia [creato un endpoint Client VPN](#) e fornito il [file di configurazione dell'endpoint Client VPN](#). Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

Argomenti

- [Installa il fornito AWS Client VPN per Linux](#)
- [Connect al provider AWS Client VPN per Linux](#)
- [AWS Client VPN note di rilascio per Linux](#)

Installa il fornito AWS Client VPN per Linux

Esistono diversi metodi che possono essere utilizzati per installare il client AWS fornito per Linux. Utilizza uno dei metodi forniti dalle seguenti opzioni. Prima di iniziare, assicurati di leggere i [requisiti](#).

Opzione 1: installazione tramite repository di pacchetti

1. Aggiungi la chiave pubblica del client AWS VPN al tuo sistema operativo Ubuntu.

```
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
```

2. Usa il seguente comando per aggiungere il repository al tuo sistema operativo Ubuntu (versione 22.04 e successive):

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

3. Utilizza il comando riportato di seguito per aggiornare i repository del sistema.

```
sudo apt-get update
```

4. Usa il seguente comando per installare il client AWS fornito per Linux.

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

Opzione 2: Installazione utilizzando il file del pacchetto.deb

1. Scarica il file .deb da [Download di Client VPN AWS](#) o utilizzando il seguente comando.

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

2. Installa il client AWS fornito per Linux utilizzando l'dpkgutilità.

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

Opzione 3: installazione del pacchetto .deb tramite Ubuntu Software Center

1. Scarica il file del pacchetto .deb da [Download di Client VPN AWS](#).
2. Dopo aver scaricato il file del pacchetto .deb, utilizza Ubuntu Software Center per installare il pacchetto. Segui i passaggi per l'installazione da un pacchetto .deb autonomo utilizzando Ubuntu Software Center riportati nel [Wiki Ubuntu](#).

Connect al provider AWS Client VPN per Linux

Il client AWS fornito viene anche chiamato client AWS VPN nei passaggi seguenti.

Per connettersi utilizzando il AWS client fornito per Linux

1. Apri l'app AWS VPN Client.
2. Scegliere File, Manage Profiles (Gestisci profili).
3. Scegliere Add Profile (Aggiungi profilo).
4. In Display Name (Nome visualizzato), immettere un nome per il profilo.
5. Per VPN Configuration File (File di configurazione VPN) seleziona il file di configurazione ricevuto dall'amministratore Client VPN. Seleziona Apri.
6. Scegliere Add Profile (Aggiungi profilo).
7. Se desideri creare più connessioni, ripeti i passaggi Aggiungi profilo per ogni file di configurazione che desideri aggiungere. Puoi aggiungere tutti i profili che desideri, ma puoi avere solo fino a cinque connessioni aperte.
8. Nella finestra Client AWS VPN, scegli il profilo a cui desideri connetterti, quindi scegli Connetti. Se l'endpoint Client VPN è stato configurato per utilizzare l'autenticazione basata su credenziali, ti verrà richiesto di immettere un nome utente e una password. Ripeti questo passaggio per ogni connessione al profilo che desideri avviare, collegando fino a cinque endpoint simultanei.

Note

Se un profilo a cui ti connetti è in conflitto con una sessione attualmente aperta, non sarai in grado di effettuare la connessione. Scegli una nuova connessione o disconnettiti dalla sessione che causa il conflitto.

9. Per visualizzare le statistiche relative a una connessione, scegli Connessione nella finestra del client AWS VPN, scegli Mostra dettagli, quindi scegli la connessione di cui desideri visualizzare i dettagli.
10. Per disconnettere una connessione, scegli una connessione nella finestra del client AWS VPN, quindi scegli Disconnetti. Se hai più connessioni aperte, devi chiudere ogni connessione singolarmente.

AWS Client VPN note di rilascio per Linux

La tabella seguente contiene le note di rilascio e i link per il download delle versioni correnti e precedenti di AWS Client VPN for Linux.

Note

Continuiamo a fornire correzioni di usabilità e sicurezza con ogni versione. Ti consigliamo vivamente di utilizzare la versione più recente per ogni piattaforma. Le versioni precedenti potrebbero essere influenzate da problemi di and/or sicurezza relativi all'usabilità. Per informazioni dettagliate, consulta le note di rilascio.

Versione	Modifiche	Data	Collegamento per il download
5.3.3	<ul style="list-style-type: none"> Miglioramenti e correzioni di bug minori. Assetto di sicurezza migliorato 	18 maggio 2026	Scarica la versione 5.3.3 sha256: d0096c934 b36122c24 5d8c2243d 4146cdac6 7125c7421 c4e1e6ad4 30eb3adfcf
5.3.2	<ul style="list-style-type: none"> Miglioramenti e correzioni di bug minori. Posizione di sicurezza migliorata. 	17 dicembre 2025	Non è più supportato.
5.3.1	<ul style="list-style-type: none"> Miglioramenti minori. 	25 settembre 2025	Non è più supportato.
5.3.0	<ul style="list-style-type: none"> Miglioramenti minori. È stato aggiunto il supporto per le connessioni IPv6. 	14 agosto 2025	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
5.2.0	<ul style="list-style-type: none"> Miglioramenti minori. È stato aggiunto il supporto per Client Route Enforcement. 	8 aprile 2025	Non è più supportato.
5.1.0	<ul style="list-style-type: none"> È stato risolto un problema che causava la riconnessione automatica della AWS Client VPN versione 5.0.x alla VPN dopo una disconnessione per timeout di inattività. Miglioramenti e correzioni di bug minori. 	17 marzo 2025	Non è più supportato.
5.0.0	<ul style="list-style-type: none"> È stato aggiunto il supporto per più connessioni simultanee. È stata aggiornata l'interfaccia utente grafica. Miglioramenti e correzioni di bug minori. 	21 gennaio 2025	Non è più supportato.
4.1.0	<ul style="list-style-type: none"> Aggiunto il supporto per Ubuntu 22.04 e 24.04. Correzioni di bug. 	12 novembre 2024	Non è più supportato.
4.0.0	Miglioramenti minori.	25 settembre 2024	Non è più supportato.
3.15.1	Aggiunto il supporto per il <code>mssfix</code> flag OpenVPN.	4 settembre 2024	Non è più supportato.
3.15.0	<ul style="list-style-type: none"> Aggiunto il supporto per il <code>tap-sleep</code> flag OpenVPN. Aggiornate le librerie OpenVPN e OpenSSL. 	12 agosto 2024	Non è più supportato.
3.14.0	<ul style="list-style-type: none"> Aggiornate le librerie OpenVPN e OpenSSL. 	29 luglio 2024	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
3.13.0	<ul style="list-style-type: none"> Riconnettiti automaticamente quando gli intervalli della rete locale cambiano. 	21 maggio 2024	Non è più supportato.
3.12.2	<ul style="list-style-type: none"> Risolto un problema di autenticazione SAML con Chromium-based i browser a partire dalla versione 123. 	11 aprile 2024	Non è più supportato.
3.12.1	<ul style="list-style-type: none"> Risolta un'azione di buffer overflow che poteva potenzialmente consentire a un attore locale di eseguire comandi arbitrari con autorizzazioni elevate. Posizione di sicurezza migliorata. 	16 febbraio 2024	Non è più supportato.
3.12.0	<ul style="list-style-type: none"> Problemi di connettività risolti per alcune configurazioni LAN. 	19 dicembre 2023	Non è più supportato.
3.11.0	<ul style="list-style-type: none"> Rollback per "Problemi di connettività risolti per alcune configurazioni LAN". Accessibilità migliorata. 	6 dicembre 2023	Non è più supportato.
3.10.0	<ul style="list-style-type: none"> Problemi di connettività risolti per alcune configurazioni LAN. Accessibilità migliorata. 	6 dicembre 2023	Non è più supportato.
3.9.0	<ul style="list-style-type: none"> È stato risolto un problema di connettività quando NAT64 è abilitato nella rete client. Miglioramenti e correzioni di bug minori. 	24 agosto 2023	Non è più supportato.
3.8.0	<ul style="list-style-type: none"> Posizione di sicurezza migliorata. 	3 agosto 2023	Non è più supportato.
3.7.0	<ul style="list-style-type: none"> Posizione di sicurezza migliorata. 	15 luglio 2023	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
3.6.0	<ul style="list-style-type: none"> • Sono state ripristinate le modifiche rispetto alla versione 3.5.0. 	15 luglio 2023	Non è più supportato.
3.5.0	<ul style="list-style-type: none"> • Posizione di sicurezza migliorata. 	14 luglio 2023	Non è più supportato.
3.4.0	<ul style="list-style-type: none"> • È stato aggiunto il supporto per il flag OpenVPN «verify-x509-name». 	14 febbraio 2023	Non è più supportato.
3.1.0	<ul style="list-style-type: none"> • Risolto il problema di rilevamento del tipo di unità. • È stata migliorata la posizione di sicurezza. 	23 maggio 2022	Non è più supportato.
3.0.0	<ul style="list-style-type: none"> • Risolto il problema del messaggio del banner che non veniva visualizzato quando si utilizza l'autenticazione federata. • Corretta la visualizzazione del testo del banner per testo più lungo e sequenze di caratteri specifiche. • Posizione di sicurezza migliorata. 	3 marzo 2022	Non è più supportato.
2.0.0	<ul style="list-style-type: none"> • Aggiunto il supporto per il testo del banner dopo aver stabilito una nuova connessione. • Rimossa la possibilità di utilizzare pull-filter in relazione a echo, cioè pull-filter * echo • Miglioramenti e correzioni di bug minori. 	20 gennaio 2022	Non è più supportato.

Versione	Modifiche	Data	Collegamento per il download
1.0.3	<ul style="list-style-type: none">• In alcuni casi è stato corretto il tentativo di connessione di autenticazione federata.• Miglioramenti e correzioni di bug minori.	8 novembre 2021	Non è più supportato.
1.0.2	<ul style="list-style-type: none">• Aggiunto il supporto per i flag OpenVPN: connect-retry-max, dev-type, keepalive, ping, ping-restart, pull, rcvbuf, server-poll-timeout.• Miglioramenti e correzioni di bug minori.	28 settembre 2021	Non è più supportato.
1.0.1	<ul style="list-style-type: none">• Abilitata l'opzione per uscire dalla barra dell'applicazione Ubuntu.• Aggiunto il supporto per i flag OpenVPN: inactive, pull-filter, route.• Miglioramenti e correzioni di bug minori.	4 agosto 2021	Non è più supportato.
1.0.0	Versione iniziale.	11 giugno 2021	Non è più supportato.

Connect a AWS Client VPN endpoint che utilizza un client OpenVPN

È possibile stabilire una connessione a un endpoint Client VPN utilizzando le comuni applicazioni client Open VPN. Client VPN è supportato sui seguenti sistemi operativi:

- Windows

Usa un certificato e una chiave privata da Windows Certificate Store. Dopo aver generato il certificato e la chiave, puoi stabilire una connessione AWS Client utilizzando l'applicazione client OpenVPN GUI o OpenVPN GUI Connect Client. Per i passaggi per creare il certificato e la chiave, vedi [Stabilisci una connessione VPN utilizzando un certificato su Windows](#)

- macOS


Stabilisci una connessione VPN utilizzando un file di configurazione per mac OS-based Tunnelblick o per Client VPN AWS . Per ulteriori informazioni, consulta [Stabilisci una connessione VPN su macOS](#).

- Linux

Stabilisci una connessione VPN su Linux utilizzando l'interfaccia OpenVPN - Network Manager o l'applicazione OpenVPN. Per utilizzare l'interfaccia OpenVPN - Network Manager devi prima installare il modulo di gestione della rete se non è già installato. Per ulteriori informazioni, consulta [Stabilire una connessione VPN su Linux](#).

- Android e iOS

Stabilisci una connessione VPN utilizzando l'applicazione client OpenVPN su un dispositivo Android o iOS. Per ulteriori informazioni, consulta [Connessioni Client VPN su Android e iOS](#).

 Important

Se l'endpoint Client VPN è stato configurato per utilizzare l'[autenticazione SAML-based federata](#), non è possibile utilizzare il client OpenVPN-based VPN per connettersi a un endpoint Client VPN. Ciò include tutte le architetture ARM-based. Se utilizzi un dispositivo con un processore ARM (come Mac Apple Silicon o dispositivi ARM-based Windows), devi utilizzare gli endpoint SAML-based VPN con il client AWS fornito anziché i client OpenVPN.

Applicazioni client

- [Connect a AWS Client VPN dispositivo che utilizza un'applicazione client Windows](#)
- [Connect a AWS Client VPN endpoint che utilizza un'applicazione client macOS](#)
- [Connect a AWS Client VPN endpoint che utilizza un'applicazione client OpenVPN](#)
- [AWS Client VPN connessioni su applicazioni Android e iOS](#)

Connect a AWS Client VPN dispositivo che utilizza un'applicazione client Windows

Queste sezioni descrivono come stabilire una connessione VPN utilizzando i client Windows-based VPN.

Prima di iniziare assicurati che l'amministratore Client VPN abbia [creato un endpoint Client VPN](#) e fornito il [file di configurazione dell'endpoint Client VPN](#). Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

Per informazioni sulla risoluzione dei problemi, consulta [Risoluzione dei problemi AWS Connessioni Client VPN con Windows-based client](#).

Important

Se l'endpoint Client VPN è stato configurato per utilizzare l'[autenticazione SAML-based federata](#), non è possibile utilizzare il client OpenVPN-based VPN per connettersi a un endpoint Client VPN. Ciò include tutte le architetture ARM-based. Se utilizzi un dispositivo con un processore ARM (come Mac Apple Silicon o dispositivi ARM-based Windows), devi utilizzare gli endpoint SAML-based VPN con il client AWS fornito anziché i client OpenVPN.

Processi

- [Usa un certificato e stabilisci un AWS Connessione Client VPN su Windows](#)

Usa un certificato e stabilisci un AWS Connessione Client VPN su Windows

È possibile configurare il client OpenVPN in modo che utilizzi un certificato e una chiave privata dall'archivio del sistema di certificati di Windows. Questa opzione è utile quando si utilizza una smart

card per la connessione Client VPN. Per informazioni sull'opzione `cryptoapicert` del client OpenVPN, consulta il [Manuale di riferimento per OpenVPN](#) sul sito Web di OpenVPN.

Note

Il certificato deve essere memorizzato nel computer locale.

Per utilizzare un certificato e stabilire una connessione

1. Crea un file con estensione `.pfx` contenente il certificato client e la chiave privata.
2. Importa il file con estensione `.pfx` nell'archivio personale dei certificati, sul computer locale. Per ulteriori informazioni, consulta [Come visualizzare i certificati con lo snap-in MMC](#) sul sito Web di Microsoft.
3. Verifica che l'account disponga delle autorizzazioni per leggere il certificato sul computer locale. È possibile utilizzare la console di gestione di Microsoft per modificare le autorizzazioni. Per ulteriori informazioni, vedere [Diritti di visualizzazione dell'archivio dei certificati del computer locale](#) sul sito Web di Microsoft.
4. Aggiorna il file di configurazione OpenVPN e specifica il certificato utilizzando l'oggetto del certificato o l'identificazione personale del certificato.

Di seguito è riportato un esempio di specifica del certificato utilizzando un oggetto.

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

Di seguito è riportato un esempio di specifica del certificato utilizzando un'identificazione personale. È possibile trovare l'identificazione personale utilizzando la console di gestione di Microsoft. Per ulteriori informazioni, vedere [Procedura: Recuperare l'impronta digitale di un certificato](#) sul sito Web di Microsoft.

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

5. Dopo aver completato la configurazione, usa OpenVPN per stabilire una connessione VPN effettuando una delle seguenti operazioni:
 - Usa l'applicazione client GUI OpenVPN
 1. Avviare l'applicazione client OpenVPN.

2. Nella barra delle applicazioni di Windows, scegli le icone. Show/Hide Right-click OpenVPN GUI, quindi scegli Importa file.
 3. Nella finestra di dialogo di apertura, seleziona il file di configurazione ricevuto dall'amministratore Client VPN e scegli Open (Apri).
 4. Nella barra delle applicazioni di Windows, scegli le icone. Show/Hide Right-click OpenVPN GUI, quindi scegli Connect.
- Usa il client OpenVPN GUI Connect
 1. Avvia l'applicazione OpenVPN e scegli Importa, Da file locale... .
 2. Passa al file di configurazione ricevuto dall'amministratore VPN e seleziona Apri.

Connect a AWS Client VPN endpoint che utilizza un'applicazione client macOS

Queste sezioni descrivono come stabilire una connessione VPN utilizzando il client OS-based VPN mac, Tunnelblick o Client VPN AWS .

Prima di iniziare assicurati che l'amministratore Client VPN abbia [creato un endpoint Client VPN](#) e fornito il [file di configurazione dell'endpoint Client VPN](#). Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

Per informazioni sulla risoluzione dei problemi, consulta [Risoluzione dei problemi AWS Connessioni Client VPN con client macOS](#).

Important

Se l'endpoint Client VPN è stato configurato per utilizzare l'[autenticazione SAML-based federata](#), non è possibile utilizzare il client OpenVPN-based VPN per connettersi a un endpoint Client VPN. Ciò include tutte le architetture ARM-based. Se utilizzi un dispositivo con un processore ARM (come Mac Apple Silicon o dispositivi ARM-based Windows), devi utilizzare gli endpoint SAML-based VPN con il client AWS fornito anziché i client OpenVPN.

Argomenti

- [Stabilisci un AWS Client VPN connessione su macOS](#)

Stabilisci un AWS Client VPN connessione su macOS

È possibile stabilire una connessione VPN utilizzando l'applicazione client Tunnelblick su un computer macOS.

Note

Per ulteriori informazioni sull'applicazione client Tunnelblick per macOS, consulta la [documentazione di Tunnelblick](#) sul sito Web Tunnelblick.

Per stabilire una connessione VPN utilizzando Tunnelblick

1. Avviare l'applicazione client Tunnelblick e scegliere I have configuration files (Ho i file di configurazione).
2. Trascinare il file di configurazione ricevuto dall'amministratore VPN nel riquadro Configurations (Configurazioni).
3. Selezionare il file di configurazione nel riquadro Configurazioni e scegliere Connetti.

Per stabilire una connessione VPN utilizzando AWS Client VPN.

1. Avvia l'applicazione OpenVPN e scegli Importa, Dal file locale....
2. Passa al file di configurazione ricevuto dall'amministratore VPN e seleziona Apri.

Connect a AWS Client VPN endpoint che utilizza un'applicazione client OpenVPN

Queste sezioni descrivono come stabilire una connessione VPN utilizzando OpenVPN - Network Manager o OpenVPN.

Prima di iniziare assicurati che l'amministratore Client VPN abbia [creato un endpoint Client VPN](#) e fornito il [file di configurazione dell'endpoint Client VPN](#). Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

Per informazioni sulla risoluzione dei problemi, consulta [Risoluzione dei problemi AWS Connessioni Client VPN con Linux-based client](#).

⚠ Important

Se l'endpoint Client VPN è stato configurato per utilizzare l'[autenticazione SAML-based federata](#), non è possibile utilizzare il client OpenVPN-based VPN per connettersi a un endpoint Client VPN. Ciò include tutte le architetture ARM-based. Se utilizzi un dispositivo con un processore ARM (come Mac Apple Silicon o dispositivi ARM-based Windows), devi utilizzare gli endpoint SAML-based VPN con il client AWS fornito anziché i client OpenVPN.

Argomenti

- [Stabilisci un AWS Client VPN connessione su Linux](#)

Stabilisci un AWS Client VPN connessione su Linux

Stabilisci una connessione VPN utilizzando la GUI di Network Manager su un computer Ubuntu o l'applicazione OpenVPN.

Per stabilire una connessione VPN utilizzando OpenVPN - Network Manager

1. Installare il modulo Network Manager utilizzando il seguente comando.

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

2. Passare a Settings (Impostazioni), Network (Rete).
3. Scegliere il simbolo più (+) accanto a VPN, quindi selezionare Import from file... (Importa da file...).
4. Passare al file di configurazione ricevuto dall'amministratore VPN e scegliere Open (Apri).
5. Nella finestra Aggiungi VPN scegli Aggiungi.
6. Avviare la connessione abilitando l'interruttore accanto al profilo VPN aggiunto.

Per stabilire una connessione VPN utilizzando OpenVPN

1. Installare OpenVPN usando il seguente comando.

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

2. Avviare la connessione caricando il file di configurazione ricevuto dall'amministratore VPN.

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

AWS Client VPN connessioni su applicazioni Android e iOS

Important

Se l'endpoint Client VPN è stato configurato per utilizzare l'[autenticazione SAML-based federata](#), non è possibile utilizzare il client OpenVPN-based VPN per connettersi a un endpoint Client VPN. Ciò include tutte le architetture ARM-based. Se utilizzi un dispositivo con un processore ARM (come Mac Apple Silicon o dispositivi ARM-based Windows), devi utilizzare gli endpoint SAML-based VPN con il client AWS fornito anziché i client OpenVPN.

La procedura seguente mostra come stabilire una connessione VPN utilizzando l'applicazione client OpenVPN su un dispositivo mobile Android o iOS. I passaggi per Android e iOS sono uguali.

Note

Per ulteriori informazioni sul download e sull'utilizzo dell'applicazione client OpenVPN per iOS o Android, consulta la Guida per l'[utente di OpenVPN Connect sul](#) sito Web di OpenVPN.

Prima di iniziare assicurati che l'amministratore Client VPN abbia [creato un endpoint Client VPN](#) e fornito il [file di configurazione dell'endpoint Client VPN](#). Se desideri connetterti a più profili contemporaneamente, avrai bisogno di un file di configurazione per ogni profilo.

Per stabilire la connessione, avvia l'applicazione client OpenVPN, quindi importa il file ricevuto dall'amministratore Client VPN.

Risoluzione dei problemi AWS Connessioni Client VPN

Utilizza gli argomenti seguenti per risolvere i problemi che si potrebbero verificare durante l'utilizzo di un'applicazione client per connettersi a un endpoint Client VPN.

Argomenti

- [Risoluzione dei problemi degli endpoint Client VPN per gli amministratori](#)
- [Invia i registri di diagnostica a Supporto AWS nel AWS Client fornito da](#)
- [Risoluzione dei problemi AWS Connessioni Client VPN con Windows-based client](#)
- [Risoluzione dei problemi AWS Connessioni Client VPN con client macOS](#)
- [Risoluzione dei problemi AWS Connessioni Client VPN con Linux-based client](#)
- [Risoluzione dei problemi comuni AWS Problemi relativi alla Client VPN](#)

Risoluzione dei problemi degli endpoint Client VPN per gli amministratori

Alcune delle fasi in questa guida possono essere eseguite dall'utente. Altre fasi devono essere eseguite dall'amministratore Client VPN sull'endpoint Client VPN stesso. Nelle sezioni seguenti viene descritto quando è necessario contattare l'amministratore.

Per ulteriori informazioni sulla risoluzione dei problemi relativi agli endpoint Client VPN, consulta [Risoluzione dei problemi di Client VPN](#) nella Guida per l'amministratore di AWS Client VPN .

Invia i registri di diagnostica a Supporto AWS nel AWS Client fornito da

Se hai problemi con il client AWS fornito e hai bisogno di contattarci per aiutarti Supporto AWS a risolverli, il client AWS fornito ha la possibilità di inviare i log di diagnostica a Supporto AWS. L'opzione è disponibile per le applicazioni client Windows, macOS e Linux.

Prima di inviare i file, devi accettare di consentire l'accesso Supporto AWS ai registri di diagnostica. Dopo aver accettato, ti forniremo un numero di riferimento a cui puoi fornire Supporto AWS in modo che possano accedere immediatamente ai file.

Inviare registri di diagnostica

Il client AWS fornito viene anche chiamato client AWS VPN nei passaggi seguenti.

Per inviare i registri di diagnostica utilizzando il AWS client fornito per Windows

1. Apri l'app AWS VPN Client.
2. Scegli Help (Aiuto), Send Diagnostic Logs (Invia log di diagnostica).
3. Nella finestra Send Diagnostic Logs (Invia log di diagnostica), scegli Yes (Sì).
4. Nella finestra Send Diagnostic Logs (Invia log di diagnostica), esegui una delle seguenti operazioni:
 - Per copiare il numero di riferimento negli Appunti, scegli Sì, quindi scegli OK.
 - Per tenere traccia manualmente del numero di riferimento, seleziona No.

Quando contatti Supporto AWS, dovrai fornire loro il numero di riferimento.

Per inviare i registri di diagnostica utilizzando il AWS client fornito per macOS

1. Apri l'app AWS VPN Client.
2. Scegli Help (Aiuto), Send Diagnostic Logs (Invia log di diagnostica).
3. Nella finestra Send Diagnostic Logs (Invia log di diagnostica), scegli Yes (Sì).
4. Prendi nota del numero di riferimento dalla finestra di conferma, quindi scegli OK.

Quando contatti Supporto AWS, dovrai fornire loro il numero di riferimento.

Per inviare i registri di diagnostica utilizzando il AWS client fornito per Ubuntu

1. Apri l'app AWS VPN Client.
2. Scegli Help (Aiuto), Send Diagnostic Logs (Invia log di diagnostica).
3. Nella finestra Invia log di diagnostica, scegli Sì.
4. Prendi nota del numero di riferimento dalla finestra di conferma. Ti viene data la possibilità di copiare le informazioni negli appunti.

Quando contattate Supporto AWS, dovrete fornire loro il numero di riferimento.

Risoluzione dei problemi AWS Connessioni Client VPN con Windows-based client

Le seguenti sezioni contengono informazioni sui problemi che potresti riscontrare quando utilizzi Windows-based i client per connetterti a un endpoint Client VPN.

AWS ha fornito i registri degli eventi dei client

Il client AWS fornito crea i registri degli eventi e li archivia nella seguente posizione sul computer.

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

Sono disponibili i seguenti tipi di log:

- Log applicazioni: contengono informazioni sull'applicazione. Questi log sono preceduti da 'aws_vpn_client_'.
- Log di OpenVPN: contengono informazioni sui processi OpenVPN. Questi log sono preceduti da 'ovpn_aws_vpn_client_'.

Il client AWS fornito utilizza il servizio Windows per eseguire operazioni root. I log dei servizi Windows vengono archiviati nel seguente percorso nel computer.

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

Argomenti sulla risoluzione dei problemi

- [Il client non è in grado di connettersi](#)
- [Il client non può connettersi con il messaggio di registro «nessun TAP-Windows adattatore»](#)
- [Il client è bloccato in uno stato di riconnessione](#)
- [Il processo di connessione VPN si chiude in maniera imprevista](#)
- [Impossibile avviare l'applicazione](#)
- [Il client non è in grado di creare un profilo](#)
- [La VPN si disconnette con un messaggio pop-up](#)
- [Si verifica un arresto anomalo del client su PC Dell che utilizzano Windows 10 o 11](#)
- [OpenVPN GUI](#)
- [Client OpenVPN Connect](#)

- [Impossibile risolvere il DNS](#)
- [Alias PKI mancante](#)

Il client non è in grado di connettersi

Problema

Il client AWS fornito non può connettersi all'endpoint Client VPN.

Causa

La causa del problema può essere una delle seguenti:

- Sul computer è già in esecuzione un altro processo OpenVPN che impedisce al client di connettersi.
- Il file di configurazione (.ovpn) non è valido.

Soluzione

Controlla che nessun'altra applicazione OpenVPN sia in esecuzione sul computer. In caso contrario, interrompi o chiudi questi processi e prova di nuovo a connetterti all'endpoint Client VPN. Controlla la presenza di errori nei log OpenVPN e chiedi all'amministratore Client VPN di verificare le seguenti informazioni:

- Il file di configurazione contiene la chiave e il certificato client corretti. Per ulteriori informazioni, consulta [Esportazione della configurazione client](#) nella Guida per l'amministratore di AWS Client VPN .
- Il CRL è ancora valido. Per ulteriori informazioni, consulta [Il client non è in grado di connettersi a un endpoint Client VPN](#) nella Guida per l'amministratore di AWS Client VPN .

Il client non può connettersi con il messaggio di registro «nessun TAP-Windows adattatore»

Problema

Il client AWS fornito non può connettersi all'endpoint Client VPN e nei registri dell'applicazione viene visualizzato il seguente messaggio di errore: «Non ci sono TAP-Windows adattatori su questo

sistema. Dovresti essere in grado di creare un TAP-Windows adattatore andando su Start -> Tutti i programmi -> Utilità TAP-Windows -> Aggiungi un nuovo adattatore ethernet TAP-Windows virtuale».

Soluzione

È possibile risolvere questo problema eseguendo una o più delle seguenti azioni:

- Riavvia l' TAP-Windows adattatore.
- Reinstallare il TAP-Windows driver.
- Crea un nuovo TAP-Windows adattatore.

Il client è bloccato in uno stato di riconnessione

Problema

Il client AWS fornito sta tentando di connettersi all'endpoint Client VPN, ma è bloccato in uno stato di riconnessione.

Causa

La causa del problema può essere una delle seguenti:

- Il computer non è connesso a Internet.
- Il nome host DNS non viene risolto in un indirizzo IP.
- Un processo OpenVPN sta tentando indefinitamente di connettersi all'endpoint.

Soluzione

Verifica che il computer sia connesso a Internet. Chiedi all'amministratore Client VPN di verificare che la direttiva `remote` nel file di configurazione venga risolta in un indirizzo IP valido. Puoi anche disconnettere la sessione VPN selezionando `Disconnetti` nella finestra del client AWS VPN e riprova a connetterti.

Il processo di connessione VPN si chiude in maniera imprevista

Problema

Durante la connessione a un endpoint Client VPN, il client si chiude in maniera imprevista.

Causa

TAP-Windows non è installato sul tuo computer. Questo software è obbligatorio per eseguire il client.

Soluzione

Esegui nuovamente il programma di installazione del client AWS fornito per installare tutte le dipendenze richieste.

Impossibile avviare l'applicazione

Problema

In Windows 7, il client AWS fornito non si avvia quando si tenta di aprirlo.

Causa

.NET Framework 4.7.2 o versione successiva non è installato nel computer. Questo è obbligatorio per eseguire il client.

Soluzione

Esegui nuovamente il programma di installazione del client AWS fornito per installare tutte le dipendenze richieste.

Il client non è in grado di creare un profilo

Problema

Quando provi a creare un profilo utilizzando il client fornito da AWS viene visualizzato il seguente errore:

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

Causa

Se l'endpoint Client VPN utilizza l'autenticazione reciproca, il file di configurazione (.ovpn) non contiene il certificato e la chiave client.

Soluzione

Assicurati che l'amministratore Client VPN aggiunga il certificato e la chiave client al file di configurazione. Per ulteriori informazioni, consulta [Esportazione della configurazione client](#) nella Guida per l'amministratore di AWS Client VPN .

La VPN si disconnette con un messaggio pop-up

Problema

La VPN si disconnette con un messaggio pop-up che dice: «La connessione VPN viene interrotta perché lo spazio degli indirizzi della rete locale a cui è connesso il dispositivo è cambiato. Stabilisci una nuova connessione VPN».

Causa

TAP-Windows l'adattatore non contiene la descrizione richiesta.

Soluzione

Se il `Description` campo non corrisponde a quello riportato di seguito, rimuovi prima l' TAP-Windows adattatore, quindi esegui nuovamente il programma di installazione del client AWS fornito per installare tutte le dipendenze richieste.

```
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
```

Si verifica un arresto anomalo del client su PC Dell che utilizzano Windows 10 o 11

Problema

Su alcuni PC Dell (desktop e laptop) che eseguono Windows 10 o 11, è possibile che si verifichi un arresto anomalo durante la navigazione del file system per importare un file di configurazione

VPN. Se si verifica questo problema, nei log del client fornito verranno visualizzati messaggi come i seguenti: AWS

```
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.DBROverlayIcon.initComponent()
```

Causa

Il sistema di backup e ripristino Dell in Windows 10 e 11 potrebbe causare conflitti con il client AWS fornito, in particolare con le seguenti tre DLL:

- DBRShellExtension.dll
- DBROverlayIconBackupid.dll
- DBROverlayIconNotBackupid.dll

Soluzione

Per evitare questo problema, assicurati innanzitutto che il client sia aggiornato con l'ultima versione del client AWS fornito. Vai su [Download Client VPN AWS](#) e se è disponibile una versione più recente, esegui l'aggiornamento alla versione più recente.

Devi inoltre eseguire una delle seguenti operazioni:

- Se utilizzi l'applicazione Dell Backup and Recovery, verifica che sia aggiornata. Un [post del forum Dell](#) afferma che questo problema è stato risolto nelle versioni più recenti dell'applicazione.
- Se non utilizzi l'applicazione Dell Backup and Recovery, è comunque necessario intraprendere alcune operazioni se si verifica questo problema. Se non desideri aggiornare l'applicazione, in alternativa, è possibile eliminare o rinominare i file DLL. Tuttavia, ricorda che ciò impedirà il funzionamento completo dell'applicazione Dell Backup and Recovery.

Elimina o rinomina i file DLL

1. Accedi a Esplora risorse e individua la posizione in cui è installato Dell Backup and Recovery. In genere è installato nella posizione seguente, ma potrebbe essere necessario cercare per trovarlo.

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

2. Elimina manualmente i seguenti file DLL dalla directory di installazione o rinominali. Eseguendo entrambe queste operazioni si evita il caricamento.
 - DBRShellExtension.dll
 - DBROverlayIconBackupped.dll
 - DBROverlayIconNotBackupped.dll

Puoi rinominare i file aggiungendo «.bak» alla fine del nome del file, ad esempio.
DBROverlayIconBackupped.dll.bak

OpenVPN GUI

Le seguenti informazioni sulla risoluzione dei problemi sono state verificate sulle versioni 11.10.0.0 e 11.11.0.0 del software OpenVPN GUI in Windows 10 Home (a 64 bit) e Windows Server 2016 (a 64 bit).

Il file di configurazione viene archiviato nel seguente percorso del computer.

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

I log di connessione vengono archiviati nel seguente percorso del computer.

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

Client OpenVPN Connect

Le seguenti informazioni sulla risoluzione dei problemi sono state verificate sulle versioni 2.6.0.100 e 2.7.1.101 del software OpenVPN Connect Client in Windows 10 Home (64 bit) e Windows Server 2016 (a 64 bit).

Il file di configurazione viene archiviato nel seguente percorso del computer.

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

I log di connessione vengono archiviati nel seguente percorso del computer.

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

Impossibile risolvere il DNS

Problema

La connessione non riesce e viene restituito il seguente errore.

```
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.
```

Causa

Impossibile risolvere il nome DNS. Il client deve anteporre una stringa casuale al nome DNS per impedire la memorizzazione nella cache DNS; tuttavia, alcuni client non lo fanno.

Soluzione

Consulta la soluzione [Impossibile risolvere il nome DNS dell'endpoint Client VPN](#) nella Guida per l'amministratore di AWS Client VPN .

Alias PKI mancante

Problema

Una connessione a un endpoint Client VPN che non utilizza l'autenticazione reciproca non va a buon fine con il seguente errore.

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

Causa

Il software OpenVPN Connect Client presenta un problema noto in cui tenta di eseguire l'autenticazione utilizzando l'autenticazione reciproca. Se il file di configurazione non contiene una chiave e un certificato client, l'autenticazione non va a buon fine.

Soluzione

Specifica una chiave e un certificato client casuali nel file di configurazione Client VPN e importa la nuova configurazione nel software OpenVPN Connect Client. In alternativa, utilizzare un client diverso, ad esempio il client GUI OpenVPN (v11.12.0.0) o il client Viscosity (v.1.7.14).

Risoluzione dei problemi AWS Connessioni Client VPN con client macOS

Le sezioni seguenti contengono informazioni sulla registrazione e sui problemi che potrebbero verificarsi durante l'utilizzo dei client macOS. Verifica di eseguire la versione più recente di questi client.

AWS ha fornito i registri degli eventi del client

Il client AWS fornito crea i registri degli eventi e li archivia nella seguente posizione sul computer.

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

Sono disponibili i seguenti tipi di log:

- Log applicazioni: contengono informazioni sull'applicazione. Questi log sono preceduti da 'aws_vpn_client_'.
- Log di OpenVPN: contengono informazioni sui processi OpenVPN. Questi log sono preceduti da 'ovpn_aws_vpn_client_'.

Il client AWS fornito utilizza il demone client per eseguire operazioni root. I log del daemon vengono archiviati nei seguenti percorsi del computer.

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

Il client AWS fornito memorizza i file di configurazione nella seguente posizione sul computer.

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

Argomenti sulla risoluzione dei problemi

- [Il client non è in grado di connettersi](#)
- [Il client è bloccato in uno stato di riconnessione](#)
- [Il client non è in grado di creare un profilo](#)
- [Lo strumento di supporto è un errore obbligatorio](#)
- [Tunnelblick](#)
- [Algoritmo di cifratura " AES-256-GCM non trovato](#)
- [La connessione smette di rispondere e si ripristina](#)
- [Utilizzo chiave esteso \(EKU\)](#)
- [Certificato scaduto](#)
- [OpenVPN](#)
- [Impossibile risolvere DNS](#)

Il client non è in grado di connettersi

Problema

Il client AWS fornito non può connettersi all'endpoint Client VPN.

Causa

La causa del problema può essere una delle seguenti:

- Sul computer è già in esecuzione un altro processo OpenVPN che impedisce al client di connettersi.
- Il file di configurazione (.ovpn) non è valido.

Soluzione

Controlla che nessun'altra applicazione OpenVPN sia in esecuzione sul computer. In caso contrario, interrompi o chiudi questi processi e prova di nuovo a connetterti all'endpoint Client VPN. Controlla la presenza di errori nei log OpenVPN e chiedi all'amministratore Client VPN di verificare le seguenti informazioni:

- Il file di configurazione contiene la chiave e il certificato client corretti. Per ulteriori informazioni, consulta [Esportazione della configurazione client](#) nella Guida per l'amministratore di AWS Client VPN .
- Il CRL è ancora valido. Per ulteriori informazioni, consulta [Il client non è in grado di connettersi a un endpoint Client VPN](#) nella Guida per l'amministratore di AWS Client VPN .

Il client è bloccato in uno stato di riconnessione

Problema

Il client AWS fornito sta tentando di connettersi all'endpoint Client VPN, ma è bloccato in uno stato di riconnessione.

Causa

La causa del problema può essere una delle seguenti:

- Il computer non è connesso a Internet.
- Il nome host DNS non viene risolto in un indirizzo IP.
- Un processo OpenVPN sta tentando indefinitamente di connettersi all'endpoint.

Soluzione

Verifica che il computer sia connesso a Internet. Chiedi all'amministratore Client VPN di verificare che la direttiva `remote` nel file di configurazione venga risolta in un indirizzo IP valido. Puoi anche disconnettere la sessione VPN selezionando **Disconnetti** nella finestra del client AWS VPN e riprova a connetterti.

Il client non è in grado di creare un profilo

Problema

Quando provi a creare un profilo utilizzando il client fornito da AWS viene visualizzato il seguente errore:

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

Causa

Se l'endpoint Client VPN utilizza l'autenticazione reciproca, il file di configurazione (.ovpn) non contiene il certificato e la chiave client.

Soluzione

Assicurati che l'amministratore Client VPN aggiunga il certificato e la chiave client al file di configurazione. Per ulteriori informazioni, consulta [Esportazione della configurazione client](#) nella Guida per l'amministratore di AWS Client VPN .

Lo strumento di supporto è un errore obbligatorio

Problema

Quando tenti di connettere la VPN, viene visualizzato il seguente errore.

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

Soluzione

Vedi il seguente articolo su AWS re:POST. [Client AWS VPN: lo strumento di supporto è un errore obbligatorio](#)

Tunnelblick

Le seguenti informazioni sulla risoluzione dei problemi sono state verificate sulla versione 3.7.8 (build 5180) del software Tunnelblick su macOS High Sierra 10.13.6.

Il file di configurazione per le configurazioni private viene archiviato nel seguente percorso del computer.

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

Il file di configurazione per le configurazioni condivise viene archiviato nel seguente percorso del computer.

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

I log di connessione vengono archiviati nel seguente percorso del computer.

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

Per aumentare il dettaglio dei log, aprire l'applicazione Tunnelblick, scegliere Settings (Impostazioni) e regolare il valore per VPN log level (Livello di log VPN).

Algoritmo di cifratura " AES-256-GCM non trovato

Problema

La connessione non riesce e restituisce il seguente errore nei 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
```

Causa

L'applicazione utilizza una versione OpenVPN che non supporta l'algoritmo di cifratura. AES-256-GCM

Soluzione

Scegliere una versione di OpenVPN compatibile nel modo seguente:

1. Aprire l'applicazione Tunnelblick.
2. Seleziona Impostazioni.
3. Per OpenVPN version (Versione di OpenVPN), scegliere 2.4.6 - OpenSSL version is v1.0.2q (2.4.6 - la versione OpenSSL è v1.0.2q).

La connessione smette di rispondere e si ripristina

Problema

La connessione non riesce e restituisce il seguente errore nei 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
```

Causa

Il certificato client è stato revocato. La connessione smette di rispondere dopo aver tentato di autenticarsi e alla fine viene ripristinata dal lato server.

Soluzione

Richiedi un nuovo file di configurazione dall'amministratore Client VPN.

Utilizzo chiave esteso (EKU)

Problema

La connessione non riesce e restituisce il seguente errore nei 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,,,,,
```

Causa

L'autenticazione del server è stata completata. Tuttavia, l'autenticazione client non va a buon fine perché il campo Utilizzo chiave esteso (EKU) del certificato client è abilitato per l'autenticazione del server.

Soluzione

Verifica di utilizzare il certificato e la chiave client corretti. Se necessario, verifica con l'amministratore VPN Client. Questo errore può verificarsi se usi il certificato server e non il certificato client per connetterti all'endpoint Client VPN.

Certificato scaduto

Problema

L'autenticazione del server va a buon fine ma l'autenticazione client non riesce con il seguente errore.

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

Causa

La validità del certificato client è scaduta.

Soluzione

Richiedi un nuovo certificato client all'amministratore Client VPN.

OpenVPN

Le seguenti informazioni sulla risoluzione dei problemi sono state verificate sulla versione 2.7.1.100 del software OpenVPN Connect Client su macOS High Sierra 10.13.6.

Il file di configurazione viene archiviato nel seguente percorso del computer.

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

I log di connessione vengono archiviati nel seguente percorso del computer.

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

Impossibile risolvere DNS

Problema

La connessione non riesce e viene restituito il seguente errore.

```
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
```

Causa

OpenVPN Connect non è in grado di risolvere il nome DNS Client VPN.

Soluzione

Consulta la soluzione [Impossibile risolvere il nome DNS dell'endpoint Client VPN](#) nella Guida per l'amministratore di AWS Client VPN .

Risoluzione dei problemi AWS Connessioni Client VPN con Linux-based client

Le sezioni seguenti contengono informazioni sulla registrazione e sui problemi che potrebbero verificarsi durante l'utilizzo Linux-based dei client. Verifica di eseguire la versione più recente di questi client.

Argomenti

- [AWS ha fornito i registri degli eventi dei client](#)
- [Le query DNS vanno a un nameserver predefinito](#)
- [OpenVPN \(riga di comando\)](#)
- [OpenVPN tramite Network Manager \(GUI\)](#)

AWS ha fornito i registri degli eventi dei client

Il client AWS fornito archivia i file di registro e i file di configurazione nella seguente posizione sul sistema:

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

Il processo daemon client AWS fornito archivia i file di registro nella seguente posizione sul sistema:

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

Ad esempio, è possibile controllare i seguenti file di registro per trovare errori negli up/down script DNS che causano l'interruzione della connessione:

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

Le query DNS vanno a un nameserver predefinito

Problema

In alcuni casi, dopo aver stabilito una connessione VPN, le query DNS continueranno a passare al server dei nomi di sistema predefinito anziché ai server dei nomi configurati per l'endpoint Client VPN.

Causa

Il Client interagisce con `systemd-resolved`, un servizio disponibile sui sistemi Linux, che funge da elemento centrale della gestione DNS. Viene utilizzato per configurare i server DNS che vengono spinti dall'endpoint Client VPN. Il problema si verifica perché `systemd-resolved` non imposta la priorità più alta per i server DNS forniti dall'endpoint Client VPN. Al contrario, i server vengono aggiunti all'elenco esistente dei server DNS configurati nel sistema locale. Di conseguenza, i server DNS originali potrebbero ancora avere la priorità più alta e quindi essere utilizzati per risolvere le query DNS.

Soluzione

1. Aggiungi la seguente direttiva nel file di configurazione di OpenVPN per essere certo che tutte le query DNS vengano inviate nel tunnel VPN.

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

2. Utilizza il resolver stub fornito da `systemd-resolved`. Per far ciò, collegare simbolicamente `/etc/resolv.conf` a `/run/systemd/resolve/stub-resolv.conf` emettendo il seguente comando sul sistema.

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

3. (Facoltativo) Se non vuoi che `systemd-resolved` utilizzi un proxy per le query DNS ma desideri che le query vengano inviate direttamente ai server dei nomi DNS reali, stabilisci un collegamento simbolico da `/etc/resolv.conf` a `/run/systemd/resolve/resolv.conf`.

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

Questa procedura può essere necessaria per bypassare `systemd-resolved`, ad esempio per la memorizzazione nella cache delle risposte DNS, la configurazione DNS per interfaccia, l'imposizione DNSSEC e così via. Questa opzione è particolarmente utile quando è necessario sovrascrivere un record DNS pubblico con un record privato quando si è connessi a VPN. Ad esempio, è possibile che nel VPC privato sia presente un resolver DNS privato con un record per `www.example.com`, che viene risolto in un IP privato. Questa opzione può essere utilizzata per sovrascrivere il record pubblico di `www.example.com`, che si risolve in un IP pubblico.

OpenVPN (riga di comando)

Problema

La connessione non funziona correttamente perché la risoluzione DNS non funziona.

Causa

Il server DNS non è configurato nell'endpoint Client VPN o non viene accettato dal software client.

Soluzione

Utilizzare le fasi seguenti per verificare che il server DNS sia configurato e funzioni correttamente.

1. Accertarsi che una voce del server DNS sia presente nei log. Nell'esempio seguente, il server DNS `192.168.0.2` (configurato nell'endpoint Client VPN) viene restituito nell'ultima riga.

```
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
```

Se non è specificato alcun server DNS, chiedi all'amministratore Client VPN di modificare l'endpoint Client VPN assicurandosi che per l'endpoint Client VPN sia specificato un server DNS

(ad esempio il server DNS VPC). Per ulteriori informazioni, consulta [Endpoint Client VPN](#) nella Guida per l'amministratore di AWS Client VPN .

2. Per accertarsi che il pacchetto `resolvconf` sia installato, eseguire il comando seguente.

```
sudo apt list resolvconf
```

Viene restituito l'output seguente.

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

Se non è installato, installarlo utilizzando il seguente comando.

```
sudo apt install resolvconf
```

3. Apri il file di configurazione Client VPN (il file `ovpn`) in un editor di testo e aggiungi le seguenti righe.

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

Controllare i log per verificare che lo script `resolvconf` sia stato richiamato. I log devono contenere una riga simile alla seguente.

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

OpenVPN tramite Network Manager (GUI)

Problema

Quando si utilizza il client Network Manager OpenVPN, la connessione non riesce con il seguente errore.

```
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
```

Causa

Il flag `remote-random-hostname` non è rispettato e il client non può connettersi utilizzando il pacchetto `network-manager-gnome`.

Soluzione

Consulta la soluzione [Impossibile risolvere il nome DNS dell'endpoint Client VPN](#) nella Guida per l'amministratore di AWS Client VPN .

Risoluzione dei problemi comuni AWS Problemi relativi alla Client VPN

Di seguito sono riportati i problemi comuni che possono verificarsi quando utilizzi un client per connetterti a un endpoint Client VPN.

Negoziazione chiave TLS non riuscita

Problema

La negoziazione TLS non va a buon fine con il seguente errore.

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

Causa

La causa del problema può essere una delle seguenti:

- Le regole del firewall bloccano il traffico UDP o TCP.
- La chiave e il certificato client utilizzati nel file di configurazione (`.ovpn`) sono errati.
- L'elenco di revoche di certificati (CRL) del client è scaduto.

Soluzione

Verifica che le regole del firewall sul computer non blocchino il traffico TCP o UDP in ingresso o in uscita sulle porte 443 o 1194. Chiedi all'amministratore Client VPN di verificare le seguenti informazioni:

- Le regole del firewall per l'endpoint Client VPN non blocchino il traffico TCP o UDP sulle porte 443 o 1194.
- Il file di configurazione contiene la chiave e il certificato client corretti. Per ulteriori informazioni, consulta [Esportazione della configurazione client](#) nella Guida per l'amministratore di AWS Client VPN .
- Il CRL è ancora valido. Per ulteriori informazioni, consulta [Il client non è in grado di connettersi a un endpoint Client VPN](#) nella Guida per l'amministratore di AWS Client VPN .

Cronologia dei documenti

La tabella seguente descrive gli aggiornamenti della AWS Client VPN User Guide.

Modifica	Descrizione	Data
AWS rilasciato il client fornito (5.3.7) per Windows ARM64 e x64	Per informazioni dettagliate, consulta le note di rilascio.	15 giugno 2026
AWS rilasciato il client fornito (5.3.6) per Windows ARM64 e x64	Per informazioni dettagliate, consulta le note di rilascio.	28 maggio 2026
AWS rilasciato il client fornito (5.3.5) per Windows ARM64 e x64	Per informazioni dettagliate, consulta le note di rilascio.	27 maggio 2026
AWS rilasciato il client fornito (5.3.3) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	18 maggio 2026
AWS rilasciato il client fornito (5.3.5) per macOS ARM64 e x64	Per informazioni dettagliate, consulta le note di rilascio.	14 maggio 2026
AWS rilasciato il client fornito (5.3.4) per Windows ARM64 e x64	Per informazioni dettagliate, consulta le note di rilascio.	26 marzo 2026
AWS rilasciato il client fornito (5.3.3) per Windows ARM64 e x64	Per informazioni dettagliate, consulta le note di rilascio.	28 febbraio 2026
AWS rilasciato il client fornito (5.3.4) per macOS ARM64 e x64	Per informazioni dettagliate, consulta le note di rilascio.	17 febbraio 2026

AWS rilasciato il client fornito (5.3.2) per Windows ARM64 e x64	Per informazioni dettagliate, consulta le note di rilascio.	17 febbraio 2026
AWS rilasciato il client fornito (5.3.3) per macOS ARM64 e x64	Per informazioni dettagliate, consulta le note di rilascio.	26 dicembre 2025
AWS rilasciato il client fornito (5.3.2) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	17 dicembre 2025
AWS rilasciato il client fornito (5.3.2) per macOS x64	Per informazioni dettagliate, consulta le note di rilascio.	27 ottobre 2025
AWS rilasciato il client fornito (5.3.2) per i sistemi macOS ARM64	Il supporto è ora aggiunto per i ARM64-based sistemi operativi macOS. Ciò include un download della nuova AWS Client VPN versione 5.3.2 specifico per i sistemi macOS ARM64. Consulta i requisiti di Client VPN per macOS per maggiori dettagli e le note di rilascio per AWS Client VPN macOS per il link per il download .	27 ottobre 2025
AWS rilasciato il client fornito (5.3.1) per Windows x64 e Arm64	Per informazioni dettagliate, consulta le note di rilascio.	30 settembre 2025
AWS il client fornito per macOS ora supporta Tahoe (26.0)	Vedi Requisiti per i dettagli.	25 settembre 2025
AWS rilasciato il client fornito (5.3.1) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	25 settembre 2025

AWS rilasciato il client fornito (5.3.1) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	9 settembre 2025
AWS rilasciato il client fornito (5.3.0) per i sistemi Windows Arm64	Il supporto è ora aggiunto per i sistemi Arm64-based operativi Windows. Ciò include un download della nuova AWS Client VPN versione 5.3.0 specifico per i sistemi Windows Arm64. Consulta i requisiti di Client VPN per Windows per maggiori dettagli e le note di rilascio AWS Client VPN per Windows per il link per il download.	26 agosto 2025
AWS rilasciato il client fornito (5.3.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	14 agosto 2025
AWS rilasciato il client fornito (5.3.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	14 agosto 2025
AWS rilasciato il client fornito (5.3.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	14 agosto 2025
AWS rilasciato il client fornito (5.2.1) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	18 giugno 2025
AWS rilasciato il client fornito (5.2.2) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	2 giugno 2025
AWS rilasciato il client fornito (5.2.1) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	21 aprile 2025
AWS rilasciato il client fornito (5.2.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	8 aprile 2025
AWS rilasciato il client fornito (5.2.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	8 aprile 2025

AWS rilasciato il client fornito (5.2.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	8 aprile 2025
AWS rilasciato il client fornito (5.1.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	17 marzo 2025
AWS rilasciato il client fornito (5.1.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	17 marzo 2025
AWS rilasciato il client fornito (5.1.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	17 marzo 2025
È stato rimosso il supporto per macOS Monterey e aggiunto il supporto per macOS Sonoma (14.0)	Per i dettagli, consulta i requisiti di Client VPN per macOS .	12 marzo 2025
È stato rimosso il supporto per Ubuntu 18.0.4 (LTS) e Ubuntu 20.04 LTS (solo AMD64)	Per ulteriori informazioni, consulta Client VPN for Linux Requisiti .	12 marzo 2025
AWS rilasciato il client fornito (5.0.3) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	6 marzo 2025
AWS rilasciato il client fornito (5.0.2) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	24 febbraio 2025
AWS rilasciato il client fornito (5.0.2) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	17 febbraio 2025
AWS rilasciato il client fornito (5.0.1) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	30 gennaio 2025
AWS rilasciato il client fornito (5.0.1) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	22 gennaio 2025

Il client AWS fornito ora supporta fino a cinque connessioni simultanee	Vedi Support per connessioni simultanee utilizzando un client AWS fornito per i dettagli.	21 gennaio 2025
AWS rilasciato il client fornito (5.0.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	21 gennaio 2025
AWS rilasciato il client fornito (5.0.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	21 gennaio 2025
AWS rilasciato il client fornito (5.0.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	12 novembre 2024
AWS rilasciato il client fornito (4.1.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	12 novembre 2024
AWS rilasciato il client fornito (4.1.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	12 novembre 2024
AWS rilasciato il client fornito (4.1.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	12 novembre 2024
AWS rilasciato il client fornito (4.0.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	25 settembre 2024
AWS rilasciato il client fornito (4.0.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	25 settembre 2024
AWS rilasciato il client fornito (4.0.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	25 settembre 2024
AWS rilasciato il client fornito (3.15.1) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	4 settembre 2024
AWS rilasciato il client fornito (3.14.2) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	4 settembre 2024
AWS rilasciato il client fornito (3.12.1) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	4 settembre 2024

AWS rilasciato il client fornito (3.14.1) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	22 agosto 2024
AWS rilasciato il client fornito (3.15.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	12 agosto 2024
AWS rilasciato il client fornito (3.14.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	12 agosto 2024
AWS rilasciato il client fornito (3.12.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	12 agosto 2024
AWS rilasciato il client fornito (3.14.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	29 luglio 2024
AWS rilasciato il client fornito (3.13.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	29 luglio 2024
AWS rilasciato il client fornito (3.11.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	29 luglio 2024
AWS rilasciato il client fornito (3.12.1) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	18 luglio 2024
AWS rilasciato il client fornito (3.13.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	21 maggio 2024
AWS rilasciato il client fornito (3.12.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	21 maggio 2024
AWS rilasciato il client fornito (3.10.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	21 maggio 2024
AWS rilasciato il client fornito (3.9.2) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	11 aprile 2024
AWS rilasciato il client fornito (3.12.2) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	11 aprile 2024

AWS rilasciato il client fornito (3.11.2) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	11 aprile 2024
AWS rilasciato il client fornito (3.9.1) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	16 febbraio 2024
AWS rilasciato il client fornito (3.12.1) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	16 febbraio 2024
AWS rilasciato il client fornito (3.11.1) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	16 febbraio 2024
AWS rilasciato il client fornito (3.12.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	19 dicembre 2023
AWS rilasciato il client fornito (3.9.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	6 dicembre 2023
AWS rilasciato il client fornito (3.11.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	6 dicembre 2023
AWS rilasciato il client fornito (3.11.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	6 dicembre 2023
AWS rilasciato il client fornito (3.10.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	6 dicembre 2023
AWS rilasciato il client fornito (3.9.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	24 agosto 2023
AWS rilasciato il client fornito (3.8.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	24 agosto 2023
AWS rilasciato il client fornito (3.10.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	24 agosto 2023
AWS rilasciato il client fornito (3.9.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	3 agosto 2023

AWS rilasciato il client fornito (3.8.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	3 agosto 2023
AWS rilasciato il client fornito (3.7.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	3 agosto 2023
AWS rilasciato il client fornito (3.8.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.7.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.7.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.6.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.6.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.5.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	15 luglio 2023
AWS rilasciato il client fornito (3.6.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	14 luglio 2023
AWS rilasciato il client fornito (3.5.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	14 luglio 2023
AWS rilasciato il client fornito (3.4.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	14 luglio 2023
AWS rilasciato il client fornito (3.3.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	27 aprile 2023
AWS rilasciato il client fornito (3.5.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	3 aprile 2023

AWS rilasciato il client fornito (3.4.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	28 marzo 2023
AWS rilasciato il client fornito (3.3.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	17 marzo 2023
AWS rilasciato il client fornito (3.4.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	14 febbraio 2023
AWS rilasciato il client fornito (3.2.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	23 gennaio 2023
AWS rilasciato il client fornito (3.2.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	23 gennaio 2023
AWS rilasciato il client fornito (3.1.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	23 maggio 2022
AWS rilasciato il client fornito (3.1.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	23 maggio 2022
AWS rilasciato il client fornito (3.1.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	23 maggio 2022
AWS rilasciato il client fornito (3.0.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	3 marzo 2022
AWS rilasciato il client fornito (3.0.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	3 marzo 2022
AWS rilasciato il client fornito (3.0.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	3 marzo 2022
AWS rilasciato il client fornito (2.0.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	20 gennaio 2022
AWS rilasciato il client fornito (2.0.0) per Windows	Per informazioni dettagliate, consulta le note di rilascio.	20 gennaio 2022

AWS rilasciato il client fornito (2.0.0) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	20 gennaio 2022
AWS rilasciato il client fornito (1.4.0) per macOS	Per informazioni dettagliate, consulta le note di rilascio.	9 novembre 2021
AWS rilasciato il client fornito per Windows (1.3.7)	Per informazioni dettagliate, consulta le note di rilascio.	8 novembre 2021
AWS rilasciato il client fornito (1.0.3) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	8 novembre 2021
AWS rilasciato il client fornito (1.0.2) per Ubuntu	Per informazioni dettagliate, consulta le note di rilascio.	28 settembre 2021
AWS rilasciato il client fornito per Windows (1.3.6) e macOS (1.3.5)	Per informazioni dettagliate, consulta le note di rilascio.	20 settembre 2021
AWS rilasciato il client fornito per Ubuntu 18.04 LTS e Ubuntu 20.04 LTS	È possibile utilizzare il AWS client fornito su Ubuntu 18.04 LTS e Ubuntu 20.04 LTS.	11 giugno 2021
Supporto per OpenVPN tramite un certificato dall'archivio del sistema di certificati di Windows	Puoi utilizzare OpenVPN con un certificato dall'archivio del sistema di certificati di Windows	25 febbraio 2021
Self-service portale	È possibile accedere a un portale self-service per ottenere il client e il file di configurazione più recenti AWS forniti.	29 ottobre 2020
AWS cliente fornito	È possibile utilizzare il client AWS fornito per connettersi a un endpoint Client VPN.	4 febbraio 2020

[Versione iniziale](#)

Questa versione introduce
AWS Client VPN.

18 dicembre 2018

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.