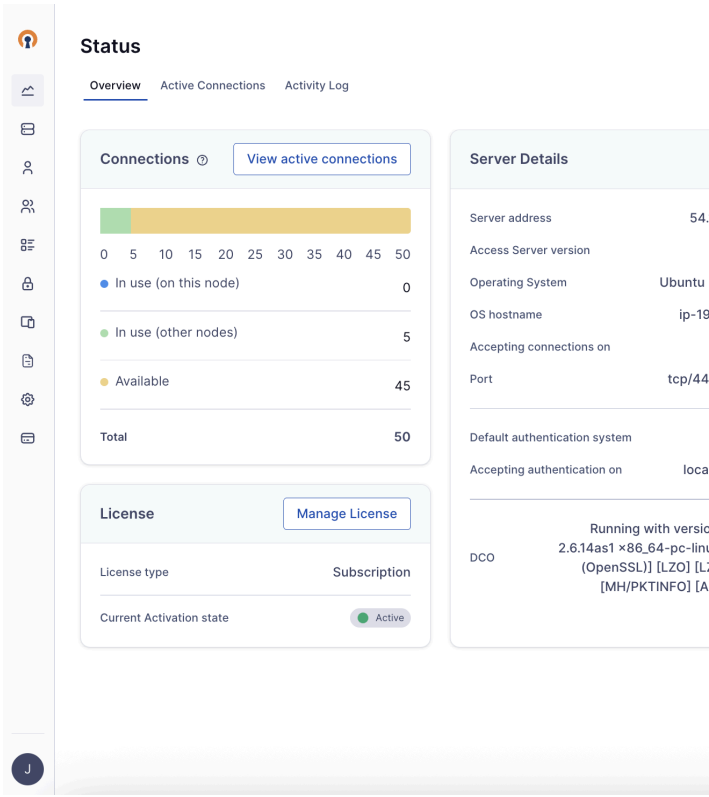
Access Server / Datasheet – February 2026

Access Server

The reliable, self-hosted VPN software solution — rapidly deployable in the cloud or on-premise — that delivers secure remote access to your business network and resources with essential zero trust network access (ZTNA) capabilities.

Access Server lets your remote, hybrid, or in-person workforce securely work from anywhere, giving your business greater flexibility without added risk. You can provide secure remote access to your corporate network with granular permissions and zero-trust enforcement, ensuring least-privilege access and that connections come from trusted devices and locations. Access Server can also protect your sensitive data by isolating your essential SaaS applications from the internet, making them accessible only after connecting to your VPN. This effectively reduces your attack surface and renders stolen or leaked credentials useless. To strengthen security against unauthorized access, Access Server includes support for multiple authentication methods, a built-in X.509 PKI for certificate provisioning, and more for comprehensive identity verification.

Unlike legacy hardware VPN solutions, Access Server takes the cost and complexity out of secure networking with popular deployment options, economical licensing models, and intuitive web-based interfaces for both users and administrators. With high scalability and ZTNA functionality support, Access Server is the network security solution that can meet your business needs at every stage, letting your organization run safely and efficiently.



How does Access Server work?

Access Server is a VPN server software that can be deployed in the cloud or on premise on general computing hardware or virtual machines. You can install multiple Access Servers to form a high-availability cluster setup to load-balance connections and data communications across multiple nodes. Plus, using the latest software developments, Access Server can handle encryption in the kernel to maximize data speeds. You can easily enable remote access to your applications and resources by installing Access Server on your corporate network. Your organization's workforce can then securely access your assets by installing the OpenVPN Connect app and connecting to your Access Server. We support client devices running on Windows, macOS, Linux, ChromeOS, iOS, and Android.

Features	What is it?
Simple Administration & Flexible Installation Options	
Administrative Web UI	Intuitive interface for managing your network configurations, access controls, users and groups, authentication settings, and more. Supports SAML for optional SSO login
Command-line interface	Exhaustive command line tools for managing every aspect of your Access Server
Offline / airgapped installation	Flexibility to install an Access Server on an airgapped LAN (Contact OpenVPN Support for an offline activation using your fixed license key.)
Cloud availability	Pre-configured images for Amazon Web Services, Google Cloud, DigitalOcean, Microsoft Azure, Oracle Cloud, and IBM Cloud marketplaces for rapid deployment and scalability
Virtualization support	Pre-configured images available for Docker, Microsoft Hyper-V, and VMWare ESXI for rapid deployment and scalability
Linux OS support	Compatibility with Red Hat Enterprise Linux, Debian, and Ubuntu
Database support	Compatibility with MySQL (defaults to SQLite database)
OpenVPN Connect client OS support	OpenVPN Connect clients are available for Android, iOS, Windows, and macOS.
Easy Onboarding	
Client Web UI	Simple interface for your users to download the Connect client bundled with their connection profile, manage their profiles, and edit their passwords
OpenVPN Connect bundled installer	Setup files that will install OpenVPN Connect v3 and preload your connection profile (You can create these files with the CLI and distribute to your macOS and Windows OS users.)
Connection profile distribution via URL	Lets your users get their profiles by simply entering the server URL in the Connect app or clicking a custom token URL (You can create token URLs in the Admin Web UI or CLI.)
Global configuration file support	Single file that automatically configures your users' Connect app with your preferred settings, profiles, and proxies to help simplify and streamline mobile device management
Connectivity	
Data Channel Offload (DCO)	Increases the speed and performance of your VPN connections by relocating data channel encryption and decryption to the kernel space
OpenVPN protocol support	Uses the OpenVPN protocol, which is widely supported across networking equipment (This protocol is firewall-friendly and works in both TCP and UDP modes. Its open-source nature means that it is open to scrutiny and auditing.)
Full application support TCP, UDP, IP	Supports any application that communicates using TCP and UDP, ensuring Access Server can secure all network traffic for the services your organization depends on
High Availability & Redundancy	
Server Clustering	Increases availability and load capacity by distributing data traffic load across multiple Access Servers nodes, which enables horizontal scaling and allows you to meet the needs of your growing workforce
Failover mode	Runs a second server on standby that can automatically take over if the primary server fails, helping to minimize downtime. Both must run on a local area network

Features	What is it?
Authentication	
SAML support	Centralizes user management and provides secure, easy access through Single Sign-On (SSO), reducing the need for multiple credentials and improving the user experience
LDAP, RADIUS, and PAM support	Manages and enforces consistent user authentication across systems and services, from local devices to your corporate network, for secure access to your private resources
Post-authentication (post-auth) script support	Extends Access Server's built-in capabilities using Python3 to include custom MFA and ZTNA checks, automated group assignments (via LDAP, SAML, or RADIUS), and more
Built-in X.509 certificate authority and PKI	Issues, manages, and inspects X.509 certificates for both your Access Server and clients to verify their identities before establishing a connection
External PKI support	Allows for integration with other X.509 PKI management software, such as OpenSSL and Microsoft AD CS, to create and distribute certificate/key pairs for your server and clients
Multi-factor authentication	Adds an extra layer of security with MFA via an authenticator app (e.g., Google Authenticator, Duo) or other TOTP generator plug-ins
Multiple authentication methods	Enables different authentication systems based on group or user, letting you enforce stricter validation for users in critical roles that access highly sensitive data
Security	
Device posture check* (via post-auth script)	Blocks connections from devices with an unregistered MAC address or UUID or any non-compliant application (including version) to help enforce approved device posture
Location context check* (via post-auth script)	Blocks connection attempts from unregistered IP addresses to help enforce location-based access policies and reduce the impact of compromised login credentials
Control channel security	Supports TLS-Crypt v2 by default to offer TLS-level post-quantum attack resistance
Data Channel Cryptography	Supports AES-256-GCM as the default for data channel encryption and can be configured to include other cipher suites (e.g., Chacha20-Poly1305) in order of priority
FIPS compliance	Complies with FIPS under default settings and supports FIPS mode (Red Hat, Ubuntu)
Access control	Defines which users and groups have access to what, including networks, IP services, and other users and groups
Automatic CA certificate renewal	Automatically generates a new CA certificate for your Access Server every year so that newly-downloaded user profiles can avoid disruptions resulting from expired certificates
Multiple user profiles per user account	Prevents connection disruptions by allowing users to have additional user profiles, at least one of which must match the most up-to-date CA certificate
Authentication failure lockout policy	Prevents brute-force attacks by automatically locking a user out after repeated failed authentication attempts. The attempt threshold and timeout duration are customizable
Web services encryption	Secures Client and Admin Web UI traffic out-of-the-box with self-signed web certificates (You can install a valid SSL certificate to avoid browser warnings and enhance security.)
Client-side script support (Windows and macOS)	Unlocks the ability for certain tasks to run automatically when the user connects (e.g., opening their web browser or running a program)

Features	What is it?
Simplified Routing	
Split-tunneling	Allows traffic bound for public internet destinations to bypass the VPN, which helps to improve network speed and latency — and reduce your Access Server load
Least privilege access (ZTNA)	Defines which IP subnets or specific IP addresses a user can access to secure your sensitive server-side resources (You can even narrow access to a specific port.)
NAT and routing	Requires all connections with Access Server (set to NAT) to be initiated by clients or lets both your clients and Access Server (set to Routing) initiate connections
Site-to-site & point-to-site routing	Supports connecting a router (used as a gateway) at one site with your Access Server at another, extending your business network to your remote offices
Domain name-based routing	Uses domain names instead of IP address subnets to simplify network routing, allowing you to easily define and configure access to your resources
Automation & Logs	
Log reports	Shows past connections made to your Access Server, along with relevant metadata, including user identity, IP address, connection duration, and more
Remote logging	Writes and stores your Access Server log data to the local syslog daemon or an external syslog server for centralized log management, simplified audits, and easier compliance
XML-RPC & REST API	Integrates with other systems to manage your Access Server programmatically, automate workflows, and more

*More features and enhancements coming soon**

Hear from our customers

“I have a use case where we are running two parallel VPNs. OpenVPN blows our other VPN server out of the water in terms of speed.” — Thomas A., President

“Access Server combines power, versatility, and security in an affordable package, solving key challenges such as remote productivity, sensitive data protection, and scalability.” — Richard V., CTO

“We migrated VPN solutions around 4 years ago and identified OpenVPN as the ideal solution for us. It ticked a lot of boxes for us, particularly with regards to 2FA and a zero trust approach to user's access with profiles. Pricing is very competitive too. Customer support is very good too.” — Daniel C., IT Manager

See what others are saying about Access Server on G2.