

VPN Client-to-Site



Overview

JioCloud VPN Client-to-Site gives users secure access to your private cloud environment – from anywhere, on any device. Each connection runs through an encrypted tunnel, with policies that control who gets access to what. Whether it's a developer reaching a test server or a contractor logging into internal tools, access stays limited, logged, and easy to manage.

Key Features

- Encrypted IPsec and SSL tunnels**
Secure all user connections over public networks using industry-standard encryption protocols.
- Multi-platform client support**
Connect securely from Windows, macOS, Linux, and mobile devices – without any special hardware.
- Always-on and split tunnel support**
Enforce a persistent VPN or tunnel only what's needed – for a performance and security balance.
- Session logging and auditing**
Track who connected, when, and to what – supporting full compliance and traceability.
- Instant, scalable deployment**
Onboard or revoke users in minutes via the JioCloud console – no manual setup required.

Benefits

- Secure remote access for employees, contractors, and third-party users.
- Identity-based controls aligned with zero-trust architecture.
- Compliance-ready logging and audit trails for every session.
- Reduced IT overhead with centralised, cloud-native management.
- No hardware, no licensing hassle, and no infrastructure sprawl.

Use Case

- **Connect teams securely**

Enable developers, support staff, and vendors to access private cloud services – without public exposure.

- **Implement zero trust**

Control access based on user identity and policy – not static credentials or IP ranges.

- **Replace legacy VPN**

Eliminate costly, complex on-premise VPN appliances with a cloud-native, scalable alternative.

- **Audit with confidence**

Log every session with context-rich metadata for compliance, audits, and investigations.