Trimble Connect Security Overview

Data Center Physical Security

Connect's infrastructure runs on Amazon Web Services (AWS). AWS provides state of the art physical protection for the infrastructure on which Connect is built. Access to AWS data centers is strictly controlled and data centers are constantly monitored to ensure systems are functioning properly.

Data Security

All communication with Trimble Connect occurs over HTTPS, ensuring communication is encrypted with TLS (SSL). All customer data is stored for high-availability and durability. Data generated within Trimble Connect is stored in secure databases which are backed-up daily.

Trimble Connect's application security model prevents customer data cross-over and ensures complete customer data segregation and privacy.

Software Security

All code developed in-house or by third-parties is checked for security defects with a source code analysis tool. Production servers are regularly scanned for vulnerabilities.

Access Controls

Within Trimble Connect, only authorized employees have access to servers and application data. Trimble Connect servers can only be accessed through secure encrypted channel connections using a VPN operated by Trimble Connect.

Account Security

Accounts for Trimble Connect are managed in a secure database stored outside of the Connect application.

Additionally, passwords are stored as salted one-way hashes. Passwords themselves are never stored and never transmitted in plain text. Users have the ability to generate and revoke unique access tokens for accessing Trimble Connect via APIs.

Privacy

Use of Trimble Connect is governed by Trimble’s corporate privacy policy which clearly outlines how Trimble collects and transfers personal data.