Security Whitepaper

Disclaimer

This document summarizes relevant topics for customer data and application security in Trimble Connect. The content is subject to change without notice. By using Trimble Connect the customer agrees that Trimble Connect services and related products are subject to the Trimble Connect Terms of Service. The content of this document is informational only and does not supercede the Terms of Service in any part.

Last updated: 19 October 2021

Table of contents

Trimble Connect overview

Trimble Connect enables cloud-based collaboration for engineering and construction projects. Accessible via Desktop, Mobile, Web and even on Mixed Reality (MR) devices, Trimble Connect allows users to view, share, and access project information from anywhere, at anytime. Our mission is to create scalable, cloud-based systems that enable our customers to become more productive, efficient and environmentally conscious by enabling digital construction workflows.

Scope

This document discusses some of the security, privacy and software development topics that we value as important to us as well as to our customers. The scope of this document is limited to Trimble Connect core services and software.

Out of Scope
Trimble Connect services are powered by the following Trimble Cloud Core Services:

- **Trimble Identity service (TID)**
  - Centralized authentication service that manages user authentication. Trimble Identity provides single sign-on capability and handles the responsibility of authenticating the identity of the users across multiple applications, products, and APIs.
- **Trimble User Profile service**
  - Centralized service for managing user profiles.
- **Trimble Data Ocean service**
  - Centralized service that provides secure, reliable, and flexible file management capabilities.
- **Trimble Processing Framework service**
  - Centralized service for managing processing workflows such as file conversions.
- **Trimble Entitlement Management Service (EMS)**
  - Centralized service for entitlement management.
- **Tekla Online Licensing**
  - Centralized service for entitlement management (Tekla users). Whitepaper here.

Trimble Connect Security

Security Standards Compliance

Trimble Connect is 3rd-party certified compliant with the following security standard:

- ISO/IEC 27001:2013. The certificate is available here.

Trimble Connect does **not** have any other 3rd-party certifications, including:

- FedRAMP Authorization
- SOC 2
- ISO 19650

TSDLC (Trimble Secure Development Life Cycle)

Trimble's approach to security includes focused efforts on everything from product development to managing and monitoring our infrastructure as well as our environments. We utilize industry standards where possible to ensure consistency and best practices across the organization.

As a customer-focused organization, Trimble ensures that security is embedded and operationalized continuously throughout the development lifecycle aligned to an enterprise framework that ensures all products have consistent security levels. This allows us to monitor and address any potential issues with our products before customers begin using them in the field.

Equally important, we monitor the infrastructure and the environments in which our solutions are deployed. Many different approaches and techniques are used, including managing identity and access, vulnerability management, and intrusion detection solutions on networks and systems. All of these approaches, together with appropriate incident response, work together to ensure security for our customer solutions.

Specific activities that Trimble Connect executes within TSDLC guidelines include:

- Cloud service access controls (following Least Privilege principles)
- Static code analysis
- Vulnerability scanning
- Intrusion detection
- Open source analysis

Data Center and Cloud Security

The Trimble Connect service is operating on Amazon Web Services (AWS) platform. Data Center security is managed by AWS. We ensure infrastructure security by following AWS security best practices defined by TSDLC, and maintaining a 24x7 Security Operations Team

monitoring system alerts. Production and development environments are separated and production environment access is limited to dedicated engineering resources.

Service and Software Security

Trimble Connect user authentication and credential management are managed by Trimble Identity service which follows industry standards for storing and protecting such information. Access to the Trimble Connect services is protected by token-based authentication and all network communication is secured in transit by using industry standard encryption protocols.

Workflow:

- User signs in with Trimble Identity by using industry standard authentication protocol
- Successful sign in will result in receiving an access token which is used for secure and authorized access to Trimble Connect services. This process is transparent for the application user.

Data Storage and Security

Trimble Connect takes seriously the protection of user information and follows best practices to comply with data protection legislation guidelines, including GDPR and CCPA. One of these practices is to limit the storage of user Personally Identifiable Information (PII) to a centralized Trimble user profile management service which serves multiple Trimble applications. The following PII is collected by Trimble Connect and stored in the Trimble user profile service:

Email address	Required
First Name	Required
Last Name	Required
Company Name	Required
Job Title	Optional
Country	Required
Street address	Optional
City	Optional
State	Required
Zip code	Optional

Telephone	Optional
Photo	Optional

All user information is stored and managed in centralized Trimble services which are hosted in North America.

User PII (including any optional fields which the user has completed) is visible to other members of all projects to which a user belongs.

Trimble Connect uses the Trimble File Management service for secure file storage. File data persistence is secured by standard AWS file storage data durability practices and encrypted. Project data storage location is defined by the user upon project creation. Currently the regional options include North America (USA), Europe (Ireland) and Asia (Singapore). Project databases are backed up daily.

By default, all users in a project can access all data in the project. Project admins can restrict data access to certain data for specific users or groups via Trimble Connect team management capabilities.

A limited number of Trimble staff have access to customer projects and user data, for the sole purpose of providing customer support.

Information about the Trimble Privacy Policy can be found here.

Continuity and Disaster Recovery

Trimble Connect service data resiliency and physical data center disaster recovery capabilities are powered by AWS Availability Zones (AZ). Deployments to multiple Availability Zones ensures service continuation in case of physical data center disaster.

Software Development

Source Code Protection

Ensuring that source code cannot be altered from outside Trimble is critical for the security of our software. To guarantee this, various measures are in place. All code is stored using version control systems, deployed within Trimble's own centralized repository. Access is strictly limited to development teams and named stakeholders.

Secure Development Environment

Code for Trimble Connect software is developed either locally at Trimble premises, or at the premises of our partners. Trimble's own premises are secure and require access permissions for all staff members and visitors. Similar requirements are in place for partners to ensure that they follow equally strict guidelines.

Development and testing is performed either locally on workstations, or within specially set up development environments. Remote development and testing environments are designed to protect the software and other data in a similar manner as in production. Customer-owned data from the production environment is not used in testing.

Code Review

Even the best software development professionals can make mistakes. One effective way and industry standard practice to catch such mistakes and learn from them is code review done within the development teams. Trimble Connect teams perform code review in the form of both peer review and formal code review. This allows us to ensure that the code is of high quality, and to spread the best practices within the teams.

Trimble Connect Software is based on a wide range of technologies. Different teams use and follow industry guidelines and best practices when developing. Code review processes aim to identify deviations from guidelines or best practices. The deviations can then be addressed before deploying the code in production.

Testing and Quality

At Trimble, we want to ensure that our software and services are of the highest quality. To achieve this goal, all systems go through rigorous testing before deployed into production.

All new Trimble Connect software versions and service updates are tested and validated according to our quality assurance processes. The processes consist of various test levels and test types, for example unit, functional, system, performance, and load testing. Updates or changes are usually tested using both automated and manual test methods. Any regressions in the testing are addressed before the changes are deployed or released.

Test cases and other test assets are continuously improved to cover new development. Testing processes and tools are continuously developed by testing professionals following the industry best practices. Various types of metrics, monitoring, and checkpoints are in place to know the testing coverage and to ensure high quality level.

Various quality assurance activities are in place during development as well as after releasing. Continuous issue and defect management is in place and when needed, new production updates are made to ensure our customers and end users can work efficiently without interruptions.

Conclusion

Trimble recognizes the value of our customers and their data. With Trimble Connect software and services, we have taken the steps necessary to protect both your privacy and the designs that are at the core of your business. While using the software and services, you can be assured that your data is protected.

We will continue to work on maintaining and improving the security of our software and services by taking advantage of new developments in industry best practices. Our efforts allow you to focus on your core business without letting security concerns stop you.

If you have any questions or concerns regarding Trimble Connect services and/or software security, privacy, or quality, do not hesitate to contact connect-support@trimble.com.