AUTODESK CONSTRUCTION CLOUD™

Security Whitepaper

Table of Contents

Introduction

Autodesk Construction Cloud ® is a cloud-based design and construction project management platform designed to improve performance across a project's lifecycle. As a secure, cloud-based platform, Autodesk Construction Cloud offers the benefits of collaboration in the design and construction space while safeguarding customer data. Autodesk Construction Cloud is designed and built using best-in-class cloud software practices and powered by Amazon Web Services (AWS), the world's leader in cloud infrastructure. We have designed our services to be scalable and secure, thus providing our customers with a resilient and safe application. We know our customers' business is relying on us and we take that responsibility seriously.

Document Purpose and Scope

The purpose of this document is to outline Autodesk Construction Cloud operations, software development, and security measures implemented in the environment.

WHAT IS INCLUDED:

The scope of this whitepaper includes all modules and services in Autodesk Docs, Autodesk Build (including PlanGrid Build), Autodesk Takeoff, Autodesk BIM Collaborate and Autodesk BIM Collaborate Pro (including Revit® Cloud Worksharing, Collaboration for Civil 3D®, and Collaboration for Plant 3D®).

WHAT IS EXCLUDED:

The scope of this whitepaper excludes the following: Assemble, BuildingConnected, Pype, ACC Connect, BIM 360 Field, BIM 360 Glue, BIM 360 Plan, BIM 360 Ops, and BIM 360 Team. For more information on security practices for Autodesk products, visit the [Autodesk Trust Center](#).

Cloud Services

The Cloud Services* team is responsible for defining and executing procedures for application release management, hardware and operating system upgrades, system health monitoring, and other activities required for the maintenance of Autodesk Construction Cloud.

*The terms "cloud service team", "cloud infrastructure team", and "cloud operations team" all denote the same team at Autodesk.

High Availability

Our commitment to high availability enables customers to enjoy the full power of Autodesk Construction Cloud. To achieve high availability, Autodesk Construction Cloud employs redundant systems in its supporting infrastructure and distributes the load across a scalable fleet of instances. The Autodesk Construction Cloud system consists of several web/application servers, background job processing systems, report execution systems, and data stores and file storage.

- Each Autodesk Data Center is spread across multiple AWS regions and Availability Zones (AZ). Each AZ is an independent physical data center within a territory, so the use of multiple AZs shields Autodesk Construction Cloud applications from outages.

- Customers using in scope Autodesk Construction Cloud products may choose to primarily store their Autodesk Construction Cloud project data in either US or Europe Data Centers. The primary storage location for project data (sometimes referred to as "Covered Content") is the Data Center that hosts your account. Project data includes project files, models, drawings, data sets, images, documents or similar materials submitted or uploaded to our service by the Customer or the

Customer's authorized users and the specific output generated from the Service based on the Customer's own raw data or information, plus the associated metadata of the project file that is not binary or in the design object itself, for example, personal data (e.g., author name, emails), time stamp and activity stream.

Business Continuity & Data Center Redundancy

Autodesk has a Business Continuity Plan and a disaster recovery process that relies on AWS Availability Zones (AZ). To support the process, Autodesk Construction Cloud is deployed across multiple AWS Availability Zones (AZ). Each AWS AZ is in a separate physical data center, and data is replicated between them. As part of deployment across multiple AWS AZs, redundant electrical power systems are installed to maintain 24/7 operations, with uninterrupted power supply (UPS) and generators for long-term backup power if an outage occurs. A redundant, multi-vendor system is used to maintain Internet connectivity to each of AWS's data centers.

Data Replication

Customer data is replicated between data centers in separate locations. Replication prevents the possibility of data loss or delay in service if failover to a backup data center is required. Data is usually replicated within 15 minutes. In addition, separate database backups are taken at least daily.

Physical Infrastructure Security

Autodesk Construction Cloud applications run in secure data centers owned and powered by Amazon AWS. AWS data centers are protected from unauthorized physical access and

environmental hazards by a range of security controls.

- **Facilities access control.** Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access AWS data centers. Entrances to server rooms are secured with devices that sound alarms to initiate an incident response if the door is forced or held open.

- **Video surveillance.** Physical access points to AWS server rooms are recorded by Closed Circuit Television Camera (CCTV). Images are retained according to legal and compliance requirements.

- **Fire prevention.** AWS data centers are equipped with automatic fire detection and suppression equipment. Fire detection systems utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas are also protected by suppression systems.

- **Climate controls.** AWS data centers use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Operations Incident Management

Autodesk Construction Cloud has an incident management policy that defines best practices for driving incident resolution. The operations incident management process is guided by the Information Technology Infrastructure Library (ITIL) Version 3 framework. The Autodesk Construction Cloud incident management policy emphasizes logging incident remediation steps and performing root cause analysis to build a knowledge base

of actionable procedures. The goal of the policy is not only to quickly and effectively close incidents, but also to collect and distribute incident information so that processes are continuously improved and future responses are driven by accumulated knowledge. Please visit the Autodesk Trust Center for more details.

Patch Management

The Cloud Services team follows the Autodesk patch management policy to help ensure effective patch deployment. Where possible, automation is in place to check for new patches and prepare deployment lists that are approved by authorized Cloud Services personnel. The Autodesk Construction Cloud patching policy also defines criteria for determining the impact of a patch on systems stability. If a patch is identified as having a possibly high impact, Cloud Services personnel complete thorough regression testing before deploying the patch. The Cloud Services team tracks the deployment of patches to production systems. Quality Assurance includes automated and manual testing that spans the entire development and deployment process.

Change Management

The Cloud Services team has a change management policy, which includes the following processes and procedures:

- **Request For Change (RFC)**. All changes made to systems supporting the application follow a formalized change management process (evidence is available through a change ticket/RFC with appropriate sign-offs)

- **Backout plans**. The Cloud Services team creates detailed backout plans prior to deploying a change so that they can restore system state if a change causes a service disruption. Backout plans include executable instructions, defined in scripts, that restore system state with minimal manual steps.

- **Defined maintenance windows**. The Cloud Services team specifies scheduled, emergency, and extended maintenance windows. They schedule planned maintenance during off-peak hours.

- **Test plan**. The Cloud Services team defines a set of tests to verify that functionality is accessible after the deployment of a change.

- **Staging environment.** A staging environment, that mirrors the layout of the production system, is maintained. All changes to the production environment are first deployed to the staging environment. Extensive testing, including functional testing, is performed prior to promoting changes from the staging to the production environment.

- **Test execution**. Once deployment is complete, the Cloud Services and Product QA teams execute the tests to check that at-risk functionality remains available.

Capacity Management

Over the course of time, Autodesk Construction Cloud resource needs may change based upon customer demand. Autodesk engineers carefully assess Autodesk Construction Cloud needs for Cloud resources and leverage resource usage instrumentation and Cloud Infrastructure elasticity. Autodesk Construction Cloud resource usage is collected at frequent intervals across a range of infrastructure components, including virtual instances, virtual storage volumes, and virtual network devices. Usage statistics are stored for analysis and may also be used to proactively scale the virtual instances up or down based upon customer demand.

Performance & Scalability

To provide a high level of availability, performance and load tests are executed throughout the software development lifecycle. [Current and historic availability together with upcoming scheduled maintenance are reported on the Autodesk Health Dashboard (https://health.autodesk.com/)](https://health.autodesk.com/)

Autodesk Construction Cloud Operational Security Controls

Autodesk has several security controls on Autodesk Construction Cloud products to prevent unauthorized access to customer accounts and data.

- **Background checks.** Autodesk requires background checks (where applicable) for employees before they are granted access to the computing resources and support systems used by Autodesk Construction Cloud.

- **Access Management.** Autodesk has defined access management policies and processes. These policies and processes address the provisioning of accounts, limiting access to Autodesk information and systems only to the extent necessary to perform assigned job responsibilities, and timely termination of access. The Autodesk Access Management policies are reviewed at least annually by the Autodesk Security team.

- **Test execution**. Once deployment is complete, the Cloud Services and Product QA teams execute tests to check that functionality identified as at-risk remains available.

- **Administrative functionality.** Autodesk Construction Cloud administrative tools provide a flexible way for administrators to manage users, role-based permissions, and other access controls for end users.

- **Redundant technologies.** Redundant technologies such as load balancers and clustered databases limit single points of failure.

Autodesk Construction Cloud Engineering

The Autodesk Construction Cloud Engineering team is responsible for designing, implementing, and testing Autodesk Construction Cloud applications. The design, coding, testing, and maintenance of Autodesk Construction Cloud is based on a software development process that includes security processes as needed.

During the design stage, detailed design documents of user stories are produced and are reviewed by architects to assess functionality and scalability of the design. The design phase uses a joint application design process where architects and software engineers assess the functionality, scalability, and performance characteristics of the user stories.

During implementation, engineers and architects conduct peer code reviews in order to detect deviations from Autodesk Construction Cloud application development practices.

All code produced during the process includes unit testing, integration, and QA verification. No new release is complete until quality assurance personnel verify the acceptance criteria.

As part of the development lifecycle, Autodesk Construction Cloud's performance team conducts load tests throughout the development sprints to catch changes that negatively affect performance as early in the process as possible.

Employee Training

Autodesk makes available general information security policy and awareness training to all its employees and contingent workers on a periodic basis.

Additionally, employees are required to read, understand, and take a training course on the company's Code of Conduct. The code requires every employee to conduct business lawfully, ethically, with integrity, and with respect for each other and the company's users, partners, and competitors.

Autodesk employees are required to follow the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. New employees must sign a confidentiality agreement. New employee orientation emphasizes the confidentiality and privacy of customer data.

To implement security best practices, each development team works closely with a dedicated Security Champion. Specialized training is mandatory for Security Champions. In addition, Autodesk provides all engineers access to Secure Development Life Cycle training. Engineers can work towards the [(ISC)² Software Security Practitioner Certification](#).

In addition, Autodesk provides various training exercises and brown bag meetings regularly for its employees including regular mock phishing exercises.

Autodesk Construction Cloud Product Security Controls

Autodesk Construction Cloud has built-in security features that allow customers to create detailed identity and access management policies. The Customer's administrators and users can use Autodesk Construction Cloud's security tools to manage ownership of their workspace, documents, and set sharing permissions.

Authentication and Encryption in Transit

Credentials consisting of user ID and password are required to access Autodesk Construction Cloud. Credentials are secured during network transmission and stored only as a salted hash.

Communication between clients and backend services is over an encrypted channel to provide communication security. The services are scanned regularly by industry-leading tools to ensure that they continue to meet the highest standards. The services support TLS v1.2 connections with secure cipher suites.

Encryption at Rest

All Autodesk Construction Cloud customer uploaded files are stored in the cloud on encrypted storage. The storage solution uses 256-bit advanced encryption (AES-256), one of the strongest block ciphers available. The entire encryption, key management, and decryption process is inspected and verified internally on a regular basis as part of our existing audit process.

Administrative Controls

Autodesk Construction Cloud provides customer administrators with security features for creating identity and access management policies.

- **Provisioning user**s. Administrators can create and deactivate users.

- **Using role-based security.** Autodesk Construction Cloud roles allow administrators to customize access control levels, to provide fine grained controls to restrict access. A role is a collection of permissions to data and functionality that relate to a job function.

By providing a flexible way of assigning permissions-based on roles, Autodesk Construction Cloud adheres to the principle of least privilege, which requires that each user's access to data and functionality be limited to what they need to complete their assigned tasks.

User Control

Users can control access to the items, reports, and files they own with exception to administrative restrictions. Users can also use file versioning to restore previous versions of files they have attached to workspace items.

Identity Federation Standards

Autodesk Construction Cloud supports Single Sign On (SSO) with customer systems for all users.

Cloud Security

Our dedicated Autodesk Security team is focused on identifying and enforcing security within the Autodesk Construction Cloud environment. Their responsibilities include:

- Reviewing the security posture of Autodesk's cloud infrastructure design and implementation.

- Defining and ensuring implementation of security policies, including identity and access management, password management, and vulnerability management.

- Driving compliance with established security procedures by conducting internal

reviews and audits.

- Identifying and implementing technologies that secure customer information.

- Engaging third-party security experts to conduct security assessments as needed.

- Monitoring cloud services for possible security issues and responding to incidents as needed.

Vulnerability Scans, Penetration Testing, and External Audits

Autodesk's Security team conducts regular security scans and penetration testing of Autodesk Construction Cloud services that are in scope for SOC2 certification. Security scans and penetration testing cover a wide range of vulnerabilities defined by the Open Web Application Security Project (OWASP) and SANS Top 25 as a part of SOC2 certifications.

Network Security

Network security is enforced using a combination of physical and logical controls, including encryption, firewalls (physical or logical), and hardening procedures. Stand-alone hardware firewalls are deployed at the perimeter of Autodesk's cloud environment. All ports are blocked, except those required to serve customer requests.

Security Standards and Compliance

- Autodesk Construction Cloud has selected industry standard – SSAE-16 AT 101 SOC 2 attestation to validate our security posture. Autodesk Construction Cloud is scheduled to be included in Autodesk's next annual SOC2 audit.

- Once audited and certified, Autodesk Construction Cloud will join BIM 360 modules and services as ISO 27001, ISO 27017 and ISO 27018 certified.

For more information on the latest attestation status of Autodesk Construction Cloud and related services, please review the "Compliance" section on Autodesk Trust Center.

Privacy

Autodesk is transparent on how customers' personal data is collected and used. Read the Autodesk Privacy Statement to learn more. You can also reference the Privacy section of the Autodesk Trust Center.

Resources

The following resources provide general information about Autodesk and additional information on topics referenced in this document.

- To learn more about Autodesk, please visit: http://www.autodesk.com.

- For more information on our comprehensive security framework, please visit: https://www.autodesk.com/trust/security.

- Autodesk Construction Cloud applications are hosted in AWS. As such, security and infrastructure are a shared responsibility between Autodesk and Amazon. For more information about Amazon security, please review these resources

    - AWS Compliance

    - AWS Data Center Controls

    - AWS Shared Responsibility Model

United States
+1 (866) 475-3802
autodesk.com/construction

Australia & APAC
AUS +61 1800 314 435
acs.apac@autodesk.com
construction.autodesk.com/au

UK & EMEA
+44 808 1892 253
acs.emea@autodesk.com
construction.autodesk.com/gb