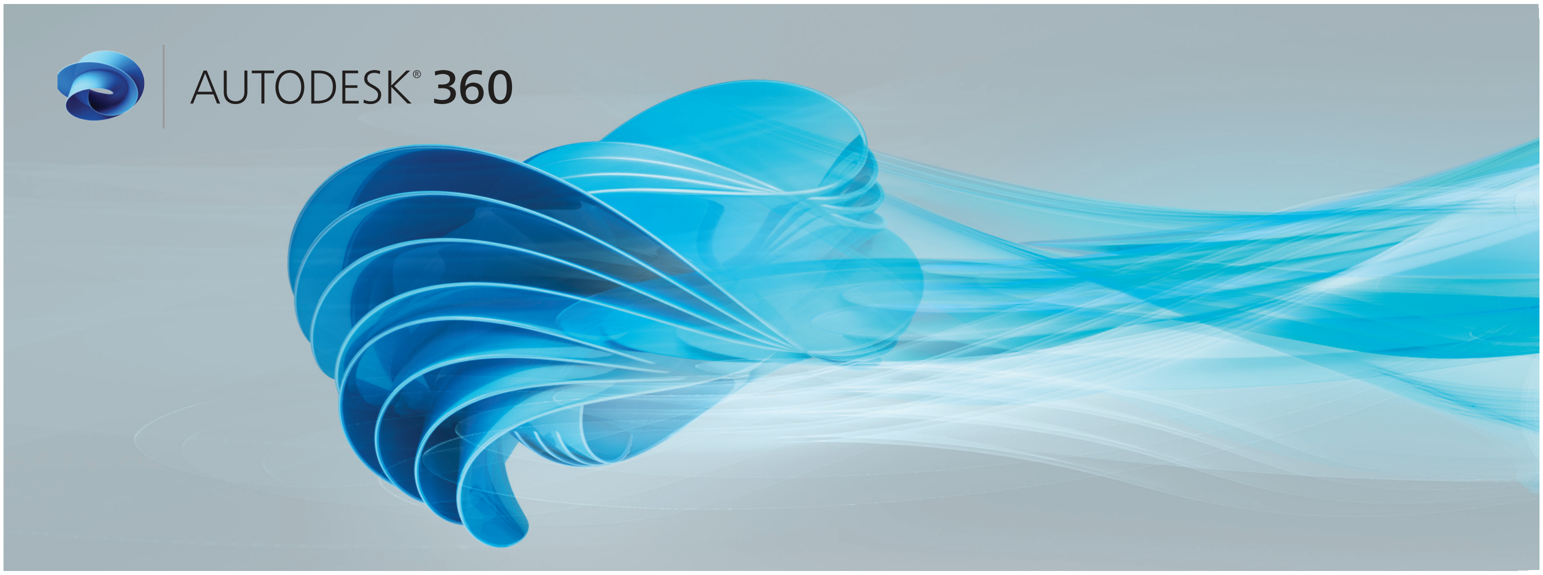


Work Securely in the Cloud

Autodesk 360

Autodesk 360 is an integrated cloud-based destination that provides a powerful and secure set of tools that can dramatically improve the way you design, visualize, simulate and share your work. Autodesk has been a trusted provider of secure cloud technology for more than a decade. Autodesk 360 uses industry-standard practices and mechanisms to uphold that trust at the forefront of all our cloud products.

Cloud Security Operations

Qualified Services

Autodesk has a dedicated team of cloud operations and security professionals who are experts in information, application and network security, as well as product delivery and management. Members of our cloud operations team hold CISSP (Certified Information Systems Security Professional), CISA (Certified Information Systems Auditor) or CISM (Certified Information Security Manager) certifications.

The Autodesk 360 Operations team oversees the cloud platform infrastructure and implements strategies to mitigate risks and operational failures. The team studies the data and systems of the security community, develops security review processes and build customized infrastructure and appropriate security responses for Autodesk 360 services.

Audits and Compliance

Autodesk performs semiannual audits of the Autodesk 360 managed services in accordance with the AT101 Soc2 Type II[1] to adhere to the highest standards for SaaS operations and applications.

The Autodesk host data centers protects data by adhering to strict internal polices in accordance with internationally accepted data protection legislation.

Finally, Autodesk conducts as needed or at least annual security policy audits and has been performing independent security reviews since 2005. A recent summary can be obtained upon request[2].

Technology and Infrastructure Overview

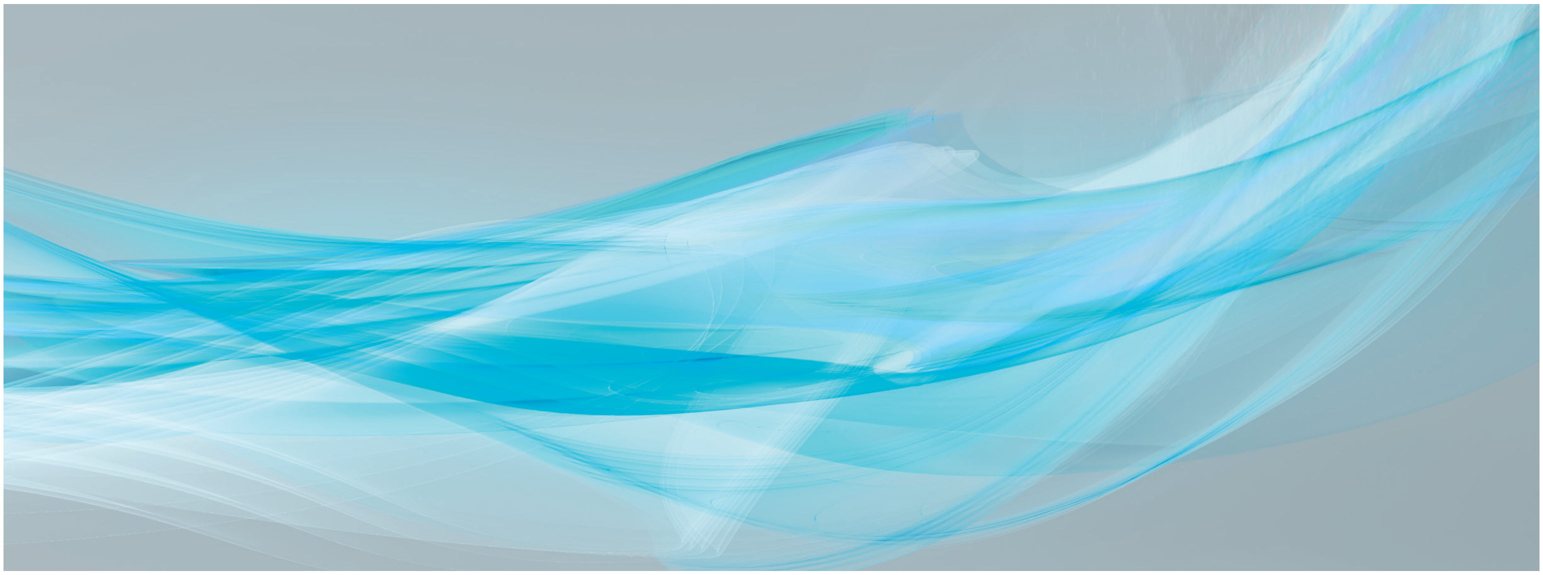
Physical Architecture

All the production systems necessary to operate Autodesk 360 are physically located in a secure data center with 24/7 security staffing and formalized security-access procedures. Advanced technologies and formalized procedures exist to control physical access to the data center. Entrance to the data center is limited to one person at a time and required an active electronic key card, biometric finger scans and PIN. Video monitoring of facilities hosting the Autodesk 360 happen via closed-circuit TV in operation both inside and outside the data centers.

Industry Best Practices

Autodesk 360 is built on industry-standard best practices for data center operations.

Autodesk 360 uses 256-bit SSL encryption (industry standard) for all communication. Data centers deploy firewall products in high-availability pairs to offer protection through system redundancy.



Uptime and Data Reliability

Data Center

The data center runs Autodesk 360 services in a clustered database environment to mitigate downtime caused by single-point failures. In addition, an identical infrastructure exists on standby, in the event the primary data center fails. Autodesk 360 actively replicates data into the secondary data centers located in the same geographic regions. This allows for near continuous operations in the event of a data center outage.

Access to Content and User Privacy

Customers own the content they create. Customers can also share their content to collaborate or for other purposes. The Autodesk 360 Terms and Services and Privacy Statement further describe the access Autodesk has to your content as part of providing you the services. The use of Autodesk's cloud services involves access to your digital content and information. Without this access, these cloud services could not function.

Encrypted Communications

Transactions between the Autodesk 360 server and customers' devices are encrypted to protect data during transit. Data stored in the Autodesk 360 service is backed up automatically to maintain reliability and availability. The data center also segregates server hardware on a private VLAN (Virtual Local Area Network) to ensure all communications remain private and confidential, and separate from other servers.

Autodesk employs several layers of software application security to ensure only authorized users may perform the actions granted by each customer's administrators.

Decommissioning of Data and File Protections

Customers control access to their files and how long their files are stored on Autodesk 360. Previous versions are never deleted and stored in a recycle bin until a customer empties the bin to permanently delete the files Our Terms of Service explains the specific commitments we make to make our users' content available even if they decide to terminate their Autodesk 360 service contract.

Autodesk adheres to the NIST[4] guidelines for proper data destruction as part of its decommissioning procedures for Autodesk 360.

For more information about Autodesk 360, Autodesk Terms of Service and the Autodesk Privacy Statement, go to *www.autodesk.com/autodesk360*. To learn more about Autodesk's commitment to security, data protection and operational excellence, go to the Autodesk 360 Trust Center. *www.autodesk.com/trust/overview*.

[1] Service organization controls relevant to Security and Availability

[2] Contact Autodesk via email at *trust@autodesk.com*

[3] Copies may persist in backup copies

[4] National Institute of Standards and Technology

AUTODESK.