Autodesk Collaboration for Revit Security Overview

August 19, 2016

Contents

Introduction

Autodesk® Collaboration for Revit® is a cloud product that works with Revit® software to connect building project teams with centralized access to cloud workshared Revit models. Integrated with Autodesk® BIM 360™ Team, a cloud-based platform for design collaboration, Collaboration for Revit enables an extended project team to edit, view, comment and share building information models.

The purpose of this document is to explain the policies and processes for Collaboration for Revit product security and Collaboration for Revit software development process, Autodesk Cloud Operations and Cloud security relating to and the cloud worksharing service in Collaboration for Revit.

Collaboration for Revit Product Security

Communications Security

Communication between Collaboration for Revit and cloud services requires secure HTTPS connections. The versions of TLS and specific cipher suites are routinely adjusted to respond to announcements about new security developments.

Encryption & Ciphers

Communication between Collaboration for Revit and backend services and within the backend services is over the encrypted channel to provide communication security. The services are scanned weekly by industry-leading tools to ensure that they continue to meet the highest standards. The services support TLS v1.2 connections with 256-bit AES encryption.

Authentication

Credentials, consisting of an Autodesk ID, user ID, and password, are required to access Collaboration for Revit. Credentials are secured during network transmission and stored only as a salted hash generated by the SHA-2 cryptographic hash function.

Data Security

Data is encrypted using 256-bit AES encryption, also known as 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. A small amount of metadata containing project attributes such as filenames, are stored unencrypted to facilitate searching of projects and other management operations.

Design Item Versioning

Every version of a cloud workshared model is saved in the cloud worksharing service, providing a record of the time and responsible team member for each Sync with Central (SWC) operation. For disaster recovery scenarios, project teams can restore previous versions of cloud workshared models from within Revit.

Permissions

Collaboration for Revit projects operate on a high-trust model. All Project Members with a Collaboration for Revit subscription can view, modify, delete, and carry out administrative operations on any cloud workshared Revit model in the Project.

Team Members are invited by the moderator of the BIM 360 project from the BIM 360 Team web or mobile experiences. A Team Member can view and interact with other Team Members and create projects within that Team hub. If allowed by a Team Administrator, a Team Member can invite other people to join the Team hub. A Team Member can join any Open project on the Team hub without invitation.

A Project Contributor can access only the projects to which the person was invited. For example, a person invited to the project from outside your organization is considered a Project Contributor. Project Contributors may include contractors, vendors, or customers, for example. After joining the project, the Project Contributor can collaborate fully on that project, creating, uploading, and commenting on items. A Project Contributor must have their own Subscription to Collaboration for Revit in order to participate in collaboration.

Collaboration for Revit Development Processes

Security is a fundamental concept of the entire development process. Annually, each engineer must repeat their security training tailored to each individual's job role.

Source code is maintained in access-controlled source management systems that maintain a history of any changes. Engineers are trained in secure development. Prior to committing a change, engineers routinely perform a security scan and evaluate and resolve issues as appropriate. A change to the source code initiates a series of automated tests that validate the security and correctness of the change. Failures to these tests are further evaluated and resolved. Further automated security testing, performed on a weekly basis, includes static analysis of source code.

A software bill of materials containing detailed information about third-party components is generated during the build and deploy process of Collaboration for Revit. A combination of automated and manual processes exists to monitor external components for security flaws so that patches can be applied in a timely manner.

Cloud Operations

Autodesk's Cloud Operations 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 Collaboration for Revit. All employees who will have access to customer data or deployment systems undergo a rigorous background check prior to being granted such access.

Autodesk uses Amazon Web Services (AWS) to host Collaboration for Revit instances. Autodesk utilizes AWS across multiple Availability Zones to provide redundancy for power, network, and server infrastructure with no single point of failure. Currently Collaboration for Revit is using the AWS us-east-1 region, please refer to AWS for location. The application infrastructure is hosted in AWS which has strict controls that meet ISO 27001 controls that are audited with AT101 SOC 2 Type 2 assessments.

Deployment Staging

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 automated testing, including functional testing, is performed prior to promoting changes from the staging to the production environment.

Power System Redundancy

Redundant electrical power systems are installed in data centers to maintain operations 24 hours a day, 7 days a week. Uninterruptible Power Supplies (UPSs) automatically provide backup to primary electrical systems in the event of a failure. Generators at each data center provide long-term backup power if an outage occurs.

Internet connectivity redundancy

A redundant multi-vendor system is used to maintain Internet connectivity to each of the data centers.

Physical Infrastructure Security

The Collaboration for Revit service hosts models in secure data centers that are protected from unauthorized physical access and environmental hazards by a range of security controls.

Facilities Access Control

Data centers are guarded 24 hours a day, 7 days a week by professional physical security staff. The perimeter of each data center, as well as rooms that contain computing and support equipment are protected by video surveillance. Video surveillance is preserved on digital media that allows recent activity to be viewed on demand. Data center entrances are guarded by mantraps that restrict access to a single person at a time. All visitors and contractors must present identification to be admitted and are escorted by authorized personnel at all times. Only employees with a legitimate business need are provided with data center access and all visits are logged electronically.

Fire prevention

Fire detection and suppression systems, such as smoke alarms and heat-activated wet pipes, are installed throughout each data center to guard rooms containing equipment and support systems. Fire detection sensors are installed in the ceiling and under a raised floor.

Climate control

Data center climate controls protect servers, routers, and other equipment subject to failure if strict environmental ranges are violated. Monitoring by both systems and personnel is in place to prevent dangerous conditions, such as overheating, from occurring. Adjustments that keep temperature and other environmental measurements within acceptable ranges are made automatically by control systems.

Operations Incident Management

Autodesk has an incident management policy which defines best practices for driving incident resolution. The Autodesk incident management policy emphasizes logging of remediation steps and the use of root cause analysis to build a knowledge base of actionable procedures. The goal of the Autodesk incident management 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.

Patch Management

Where possible, automation is in place to check for new patches and prepare deployment lists that can be approved by authorized Cloud Operations personnel. 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, regression testing is completed before the patch is deployed. Change Management tracks deployment of patches to production systems.

Weekly scanning of production machines is performed to ensure that systems are appropriately patched.

Change Management

The Cloud Operations team has a change management policy which includes the following activities:

- Requiring the submission of a Request for Change (RFC) form, that includes the name of the change initiator, the change priority, the business justification for the change, and a requested change implementation date.
- The Cloud Operations team creates detailed back out plans prior to deployment so that system state can be restored if a change causes a service disruption. Back out plans include executable instructions defined in scripts that restore system state with a minimum of manual steps.
- Maintenance is performed by Cloud Operations in a rolling manner during lower traffic periods to minimize or avoid impact to production functionality.
- Defining tests to verify that functionality is accessible after the deployment of a change.
- Once deployment is complete, the Cloud Operations and Autodesk Collaboration for Revit QA teams execute the tests to check that functionality identified as at-risk remains available.

Capacity Management

Because customer access to cloud services is provisioned on-demand through a self-service model, traffic patterns are highly variable and subject to usage spikes. When a spike occurs, the availability of a service can be negatively impacted if the pool of computing resources powering the service is exhausted. To maintain a high level of availability, the Cloud Operations team implements a capacity management policy. These practices include:

- Frequent recording of resource usage – Collaboration for Revit usage is automatically recorded by AWS and is reviewed on a weekly basis to determine if changes are needed in capacity. Also, if there is an urgent need for capacity changes, a change can be made quickly. Usage statistics are stored in a capacity management repository.

- Building a capacity plan documenting current resource use and forecasting future requirements – the capacity management repository is used by the Cloud Operations team to generate a detailed capacity plan that documents current levels of use and models future levels on statistical analysis and the impact of upcoming enhancements to business functionality. The capacity plan is updated as needed or if significant changes to usage patterns are detected.
- Collaboration for Revit has "Auto-Scaling" policies in place that trigger the automatic startup of machines in order to meet demand (to a maximum). Conversely, if demand decreases, the machines are shut down (to a minimum).

Collaboration for Revit Operational Controls

Collaboration for Revit provides protection of sensitive customer data from unauthorized access.

- Physical restrictions to data centers – Physical restrictions to data centers prevent unauthorized parties from accessing the hardware and support systems used by Collaboration for Revit.
- Background checks –Background checks are required, where permitted by law, for employees with physical and/or logical access to the computing resources and support systems used by Collaboration for Revit and BIM 360 Team.
- Redundant technologies – Redundant technologies such as load balancers and clustered databases limit single points of failure.

Cloud Security

The Cloud Security team is a dedicated group of information security specialists focused on identifying and enforcing security within Collaboration for Revit cloud environment.

The Cloud Security team's responsibilities include:

- Reviewing the security of 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 expert to conduct information security assessments.
- Monitoring cloud services for possible security issues and responding to incidents as needed.
- Conducting annual reviews of security policy.

Vulnerability scans and penetration testing

The Cloud Security team conducts scans and penetration testing of Collaboration for Revit and BIM 360 Team services. Security scans and penetration-testing cover a wide range of vulnerabilities defined by the Open Web Application Security Project (OWASP) and SANS top 25.

Network Security

Only ports except those required to serve customer requests are allowed.

Encryption

Network traffic containing sensitive information, such as credentials, application session information, access tokens and user profiles, in transmitted securely over the Internet to the perimeter of our environment.

Host Security

Automated scans are performed to validate host security.

Security Standards and Attestations

Collaboration for Revit security controls are aligned and certified for ISO 27001 and will be reviewed by an independent auditor and listed in the AT Section 101 SOC 2 audit report in the future.

Resources

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

- Autodesk
- Autodesk® Collaboration for Revit®
- Autodesk® BIM 360™ Team

The information contained in this document represents the current view of Autodesk, Inc. as of the date of publication, and Autodesk assumes no responsibility for updating this information. Autodesk occasionally makes improvements and other changes to its products or services, so the information within applies only to the version of Autodesk® Collaboration for Revit® offered as of the date of publication. This white paper is for informational purposes only. Autodesk makes no warranties, express or implied, in this document, and the information in this white paper does not create any binding obligation or commitment on the part of Autodesk.

Without limiting or modifying the foregoing, Collaboration for Revit services are provided subject to the applicable terms of service located at http://www.autodesk.com/company/legal-notices-trademarks/terms-of-service-autodesk360-web-services.