



AUTODESK
CONSTRUCTION
CLOUD™

Livre blanc sur la sécurité



mensch  **maschine**

CAD as CAD can

Mensch Maschine Suisse SA

Route du Simplon 16 - 1094 Paudex- Lausanne

021 793 20 32 – info.fr@mum.ch - www.fr.mum.ch





Mise en route de la plateforme ACC

Notre offre en 3 modules

A - Configuration et mise en service Plateforme-HUB

Phase 1 - Identification utilisateurs	1 jour
Phase 2 - Gabarits de projet ACC	2 jours
Phase 3 - Structure des dossiers	2 jours
Phase 4 - Groupes utilisateurs (Rôles)	1 jours
Phase 5 - Gestion des droits et des utilisateurs	2 jours
Phase 6 - Equipes de conception	1 jour
Phase 7 - Convention de nommage	2 jours
Phase 8 – Interopérabilité	1 jour

B - Formations et coaching

Phase 9 – Formations	7 jours
Phase 10 – Accompagnement	2 jours

C - Adaptations futures

Phase 11 - Développements spécifiques	2 à 5 jours
---------------------------------------	-------------

Une offre adaptée au besoin spécifique de l'entreprise, sera à préparer et présentée, après à une séance de travail (workshop).



Table des matières

INTRODUCTION	3
OBJECTIF ET PORTÉE DU DOCUMENT	3
SERVICES CLOUD.....	4
HAUTE DISPONIBILITÉ	4
CONTINUITÉ DE L'ACTIVITÉ ET REDONDANCE DES CENTRES DE DONNÉES	5
RÉPLICATION DES DONNÉES	5
SÉCURITÉ DE L'INFRASTRUCTURE PHYSIQUE	5
GESTION DES INCIDENTS D'EXPLOITATION	6
GESTION DES CORRECTIFS	7
GESTION DES MODIFICATIONS	7
GESTION DE LA CAPACITÉ	8
PERFORMANCES ET ÉVOLUTIVITÉ	9
CONTRÔLES DE LA SÉCURITÉ OPÉRATIONNELLE D'AUTODESK CONSTRUCTION CLOUD	9
INGÉNIERIE D'AUTODESK CONSTRUCTION CLOUD	10
FORMATION DES EMPLOYÉS	11
CONTRÔLES DE LA SÉCURITÉ OPÉRATIONNELLE D'AUTODESK CONSTRUCTION CLOUD	11
AUTHENTIFICATION ET CHIFFREMENT EN TRANSIT	12
CHIFFREMENT AU REPOS	12
CONTRÔLES ADMINISTRATIFS	12
CONTRÔLE UTILISATEUR	13
NORMES DE FÉDÉRATION DES IDENTITÉS	13
SÉCURITÉ CLOUD	13
ANALYSES DE VULNÉRABILITÉ, TESTS D'INTRUSION ET AUDITS EXTERNES	14
SÉCURITÉ RÉSEAU	14
NORMES DE SÉCURITÉ ET CONFORMITÉ	14
CONFIDENTIALITÉ	15
RESSOURCES	16

mens  **maschine**

CAD as CAD can

Mensch Maschine Suisse SA

Route du Simplon 16 - 1094 Paudex- Lausanne
021 793 20 32 – info.fr@mum.ch - www.fr.mum.ch

Introduction

Autodesk Construction Cloud[®] est une plate-forme de conception et de gestion de projets de construction basée sur le cloud. Elle est conçue pour améliorer les performances tout au long du cycle de vie d'un projet. Il s'agit d'une plate-forme cloud sécurisée qui permet la collaboration dans l'espace de conception et de construction tout en protégeant les données des clients. Autodesk Construction Cloud a été conçu et créé sur la base de pratiques logicielles cloud d'excellence et optimisé par Amazon Web Services (AWS), le leader mondial de l'infrastructure cloud. Nous avons conçu nos services afin qu'ils soient évolutifs et sécurisés, ce qui nous permet de proposer à nos clients une application résiliente et sûre. Nous sommes conscients que nos clients comptent sur nous pour assurer la bonne conduite de leur activité et nous prenons cette responsabilité très au sérieux.

Objectif et portée du document

Ce document vise à décrire les mesures relatives au fonctionnement, au développement logiciel et à la sécurité mises en œuvre dans l'environnement pour Autodesk Construction Cloud.

CONTENUS INCLUS :

Ce livre blanc aborde tous les modules et services offerts dans Autodesk Docs, Autodesk Build (notamment PlanGrid Build), Autodesk Takeoff, Autodesk BIM Collaborate et Autodesk BIM Collaborate Pro (notamment Revit[®] Cloud Worksharing, Collaboration for Civil 3D[®] et Collaboration for Plant 3D[®]).

CONTENUS EXCLUS :

En revanche, il ne traite pas les contenus suivants : Assemble, BuildingConnected, Pype, ACC Connect, BIM 360 Field, BIM 360 Glue, BIM 360 Plan, BIM 360 Ops et BIM 360 Team. Pour en savoir plus sur les pratiques en matière de sécurité relatives aux produits Autodesk, consultez le [Centre de confiance Autodesk](#).

Services cloud

L'équipe des services cloud* est chargée de définir et d'exécuter les procédures relatives à la gestion des versions des applications, aux mises à niveau du matériel et du système d'exploitation, à la surveillance de l'intégrité des systèmes et aux autres activités nécessaires dans le cadre de la maintenance d'Autodesk Construction Cloud.

* Les expressions « équipe des services cloud », « équipe de l'infrastructure cloud » et « équipe des opérations cloud » désignent toutes la même équipe chez Autodesk.

Haute disponibilité

Notre engagement en faveur d'une haute disponibilité permet à nos clients de tirer parti de toute la puissance d'Autodesk Construction Cloud. Pour atteindre une haute disponibilité, l'infrastructure de support d'Autodesk Construction Cloud a recours à des systèmes redondants et répartit la charge dans une flotte évolutive d'instances. Le système Autodesk Construction Cloud se compose de plusieurs serveurs Web et d'applications, de systèmes de traitement des tâches en arrière-plan, de systèmes d'exécution de rapports, ainsi que de banques de données et d'un système de stockage de fichiers.

- Chaque centre de données Autodesk couvre plusieurs régions et zones de disponibilité AWS. Chaque zone de disponibilité représente un centre de données physique indépendant au sein d'un territoire. Ainsi, l'existence de plusieurs zones de disponibilité protège les applications Autodesk Construction Cloud contre les pannes.
- Les clients qui utilisent les produits Autodesk Construction Cloud concernés peuvent choisir de stocker essentiellement leurs données de projet Autodesk Construction Cloud dans des centres de données situés aux États-Unis ou en Europe. L'emplacement principal de stockage des données du projet (parfois appelé « Contenu couvert ») est le centre de données qui héberge votre compte. Les données de projet comprennent les fichiers, les modèles, les dessins, les ensembles de données, les images, les documents ou éléments similaires du projet qui sont soumis ou chargés par le client ou les utilisateurs autorisés du client sur notre service. Elles comprennent également la sortie

spécifique générée par le service à partir des propres données ou informations brutes du client, ainsi que les métadonnées associées du fichier de projet qui ne sont pas binaires ou qui sont situées dans l'objet de conception lui-même, par exemple, les données personnelles (notamment, le nom de l'auteur, les e-mails), l'horodatage et le flux d'activité.

Continuité de l'activité et redondance des centres de données

Autodesk a mis en place un plan de continuité de l'activité et un processus de reprise sur sinistre qui repose sur des zones de disponibilité AWS.

Autodesk Construction Cloud est déployé dans plusieurs de ces zones afin de garantir la prise en charge de ce processus. Chaque zone de disponibilité AWS se situe dans un centre de données physique différent et les données sont répliquées dans plusieurs centres. Dans le cadre du déploiement dans plusieurs zones de disponibilité AWS, l'installation de systèmes d'alimentation électrique redondants permet le maintien des opérations 24 h/24 et 7 j/7 grâce à des onduleurs et à des générateurs qui offrent une alimentation de secours à long terme en cas de panne. Un système redondant avec plusieurs fournisseurs est utilisé pour maintenir la connectivité Internet à chacun des centres de données AWS.

Réplication des données

Les données des clients sont répliquées entre les centres de données dans des emplacements distincts. La réplication empêche le risque de perte de données ou de retard du service en cas de basculement vers un centre de données de sauvegarde. Les données sont généralement répliquées sous 15 minutes. De plus, des sauvegardes de bases de données distinctes sont effectuées au moins quotidiennement.

Sécurité de l'infrastructure physique

Les applications Autodesk Construction Cloud s'exécutent dans des centres de données sécurisés détenus et alimentés par Amazon AWS. Les centres de données AWS sont protégés contre les accès physiques non autorisés et les risques liés à l'environnement par un large éventail de contrôles de sécurité.

- **Contrôle d'accès aux installations.** L'accès physique est contrôlé aux points d'entrée du bâtiment par du personnel de sécurité professionnel qui utilise des systèmes de surveillance et de détection ainsi que d'autres moyens électroniques. Le personnel autorisé a recours à des mécanismes d'authentification à plusieurs facteurs pour accéder aux centres de données AWS. Les entrées des salles de serveurs sont sécurisées à l'aide d'appareils à alarmes qui se déclenchent et entraînent une procédure d'incident dans le cas où une porte est forcée ou maintenue ouverte.
- **Surveillance vidéo.** Les points d'accès physiques aux salles de serveurs AWS sont enregistrés par un système de vidéosurveillance. Les images sont conservées conformément aux exigences légales et de conformité.
- **Prévention des incendies.** Les centres de données AWS sont dotés d'équipements automatiques de détection et d'extinction d'incendie. Les systèmes de détection d'incendie utilisent des capteurs de détection de fumée dans les espaces de mise en réseau, mécaniques et d'infrastructure. Des systèmes d'extinction protègent ces zones.
- **Contrôles climatiques.** Les centres de données AWS utilisent des mécanismes de contrôle climatique et maintiennent une température de fonctionnement appropriée pour les serveurs et les autres équipements informatiques afin d'éviter la surchauffe et de réduire le risque de pannes de service potentielles. Le personnel et les systèmes surveillent et maintiennent la température et l'humidité à des niveaux appropriés.

Gestion des incidents d'exploitation

Autodesk Construction Cloud comprend une politique de gestion des incidents qui définit les meilleures pratiques de résolution des incidents. Le processus de gestion des incidents d'exploitation est guidé par le document cadre ITIL (Information Technology Infrastructure Library) version 3. La politique de gestion des incidents d'Autodesk Construction Cloud met l'accent sur la consignation des étapes de résolution des incidents et l'analyse des causes principales afin de créer une base de connaissances de procédures à mettre en œuvre. Cette politique vise non seulement à résoudre rapidement et efficacement les incidents, mais également

à collecter et à diffuser des informations sur les incidents afin que les processus soient constamment améliorés et que les réponses futures soient fondées sur les connaissances acquises. Consultez le [Centre de confiance Autodesk](#) pour plus d'informations.

Gestion des correctifs

L'équipe des services cloud respecte la politique de gestion des correctifs d'Autodesk afin de garantir le déploiement efficace de ces derniers. Lorsque cela est possible, l'automatisation est mise en œuvre pour vérifier la présence de nouveaux correctifs et préparer des listes de déploiement approuvées par le personnel agréé des services cloud. La politique de correctifs d'Autodesk Construction Cloud définit également des critères pour déterminer l'impact d'un correctif sur la stabilité des systèmes. Si un correctif semble avoir un impact potentiellement élevé, le personnel des services cloud effectue des tests de régression approfondis avant de déployer le correctif. L'équipe des services cloud suit le déploiement des correctifs dans les systèmes de production. L'assurance qualité comprend des tests automatisés et manuels qui s'étendent sur l'ensemble du processus de développement et de déploiement.

Gestion des modifications

L'équipe des services cloud applique une politique de gestion des modifications qui comprend les procédures et processus suivants :

- **Demande de modification.** Toutes les modifications apportées aux systèmes prenant en charge l'application s'inscrivent dans un processus formalisé de gestion des modifications (des preuves sont disponibles via un ticket de modification, avec les approbations appropriées).
- **Plans d'annulation.** L'équipe des services cloud crée des plans d'annulation détaillés avant le déploiement d'une modification afin de pouvoir restaurer l'état du système dans le cas où des modifications entraîneraient une interruption de service. Les plans d'annulation incluent des instructions exécutables, définies dans des scripts, qui restaurent l'état du système avec un minimum d'étapes manuelles.

- **Fenêtres de maintenance définies.** L'équipe des services cloud indique les fenêtres de maintenance planifiées, d'urgence et prolongées. Elle programme la maintenance planifiée pendant les heures creuses.
- **Planification de tests.** L'équipe des services cloud définit un ensemble de tests pour vérifier que la fonctionnalité est accessible après le déploiement d'une modification.
- **Environnement intermédiaire.** Un environnement intermédiaire, qui reflète la disposition du système de production, est maintenu. Toutes les modifications apportées à l'environnement de production sont déployées au préalable dans l'environnement intermédiaire. Des tests approfondis, notamment des tests fonctionnels, sont mis en œuvre avant d'appliquer les modifications de l'environnement intermédiaire dans l'environnement de production.
- **Exécution de tests.** Une fois le déploiement terminé, les équipes des services cloud et d'assurance qualité des produits exécutent les tests afin de vérifier que les fonctionnalités à risque restent disponibles.

Gestion de la capacité

Les besoins en ressources d'Autodesk Construction Cloud peuvent évoluer au fil du temps, en fonction de la demande du client. Les ingénieurs d'Autodesk évaluent soigneusement les besoins d'Autodesk Construction Cloud en ressources cloud et tirent parti de l'instrumentation de l'utilisation des ressources et de l'élasticité de l'infrastructure cloud. L'utilisation des ressources d'Autodesk Construction Cloud est collectée à intervalles fréquents pour une gamme de composants d'infrastructure, notamment les instances virtuelles, les volumes de stockage virtuels et les périphériques de réseau virtuel. Les statistiques d'utilisation sont stockées pour analyse et peuvent également être utilisées pour augmenter ou réduire de manière proactive les instances virtuelles en fonction de la demande des clients.

Performances et évolutivité

Pour fournir un haut niveau de disponibilité, des tests de performance et de charge sont exécutés tout au long du cycle de vie du développement logiciel. [La disponibilité actuelle et historique ainsi que la maintenance planifiée à venir sont signalées sur Autodesk Health Dashboard \(<https://health.autodesk.com/>\)](#)

Contrôles de la sécurité opérationnelle d'Autodesk Construction Cloud

Autodesk a mis en place plusieurs contrôles de sécurité sur les produits Autodesk Construction Cloud pour empêcher l'accès non autorisé aux comptes et aux données des clients.

- **Vérification des antécédents.** Autodesk exige la vérification des antécédents (le cas échéant) des employés avant qu'ils n'aient accès aux ressources informatiques et aux systèmes de support utilisés par Autodesk Construction Cloud.
- **Gestion des accès.** Autodesk a défini des politiques et des processus de gestion des accès. Ces politiques et processus traitent de l'approvisionnement des comptes, en limitant l'accès aux informations et aux systèmes Autodesk dans la seule portée nécessaire pour s'acquitter des responsabilités professionnelles assignées, et de la résiliation de l'accès en temps opportun. Les politiques de gestion des accès d'Autodesk sont révisées au moins une fois par an par l'équipe de sécurité d'Autodesk.
- **Exécution de tests.** Une fois le déploiement terminé, les équipes des services cloud et de l'assurance qualité des produits exécutent des tests afin de vérifier la disponibilité de la fonctionnalité identifiée comme étant à risque.
- **Fonctionnalité d'administration.** Les outils d'administration Autodesk Construction Cloud offrent aux administrateurs un moyen flexible de gérer les utilisateurs, les autorisations basées sur les rôles, et d'autres contrôles d'accès pour les utilisateurs finaux.

- **Technologies redondantes.** Les technologies redondantes telles que les modules d'équilibrage de charge et les bases de données en cluster limitent les points de défaillance uniques.

Ingénierie d'Autodesk Construction Cloud

L'équipe d'ingénierie d'Autodesk Construction Cloud est responsable de la conception, de la mise en œuvre et du test des applications Autodesk Construction Cloud. La conception, le codage, les tests et la maintenance d'Autodesk Construction Cloud reposent sur un processus de développement logiciel qui inclut des processus de sécurité selon les besoins.

Au cours de la phase de conception, des documents de conception détaillés de récits utilisateurs sont produits et examinés par des architectes afin d'évaluer la fonctionnalité et l'évolutivité de la conception. La phase de conception utilise un processus de conception d'applications conjoint dans lequel les architectes et les ingénieurs logiciels évaluent la fonctionnalité, l'évolutivité et les caractéristiques de performance des récits utilisateurs.

Au cours de la mise en œuvre, les ingénieurs et les architectes procèdent à des examens de code par les pairs afin de détecter les écarts par rapport aux pratiques de développement d'applications Autodesk Construction Cloud.

L'ensemble du code produit au cours du processus comprend les tests d'unité, l'intégration et la vérification de l'assurance qualité. Aucune nouvelle version n'est terminée tant que le personnel chargé de l'assurance qualité n'a pas vérifié les critères d'acceptation.

Dans le cadre du cycle de vie du développement, l'équipe des performances d'Autodesk Construction Cloud effectue des tests de charge tout au long des sprints de développement afin de détecter, le plus tôt possible dans le processus, les modifications susceptibles d'entraîner des conséquences néfastes sur les performances.

Formation des employés

Afin de sensibiliser l'ensemble de ses employés et travailleurs intérimaires, Autodesk offre régulièrement une formation sur la politique générale de sécurité des informations. De plus, les employés sont tenus de lire et de comprendre le Code de conduite de l'entreprise et d'assister à une formation le concernant. Ce code exige que chaque employé travaille de manière légale et éthique, avec intégrité en respectant ses collègues et les utilisateurs, les partenaires et les concurrents de l'entreprise.

Les employés d'Autodesk sont tenus de suivre les directives de l'entreprise concernant la confidentialité, l'éthique professionnelle, l'utilisation appropriée et les normes professionnelles. Les nouveaux employés doivent signer un accord de confidentialité. L'orientation des nouveaux employés met l'accent sur la confidentialité des données des clients.

Pour mettre en œuvre les meilleures pratiques de sécurité, chaque équipe de développement travaille en étroite collaboration avec un champion de la sécurité dédié. Une formation spécialisée est obligatoire pour les champions de la sécurité. De plus, Autodesk fournit à tous les ingénieurs un accès à la formation sur le cycle de vie de développement sécurisé. Les ingénieurs peuvent préparer la [Certification \(ISC\)² pour les experts en sécurité logicielle](#).

En outre, Autodesk propose régulièrement à ses employés divers exercices d'entraînement et des réunions informelles de formation à l'heure du déjeuner, y compris des exercices réguliers de simulation d'hameçonnage.

Contrôles de la sécurité opérationnelle d'Autodesk Construction Cloud

Autodesk Construction Cloud comprend des fonctionnalités de sécurité intégrées qui permettent aux clients de créer des politiques détaillées de gestion des identités et des accès. Les administrateurs et les utilisateurs du client peuvent se servir des outils de sécurité d'Autodesk Construction Cloud pour gérer la propriété de leurs espaces de travail et de leurs documents, et définir des autorisations de partage.

Authentification et chiffrement en transit

Pour accéder à Autodesk Construction Cloud, il convient de disposer d'informations d'identification comprenant un ID utilisateur et un mot de passe. Les informations d'identification sont sécurisées lors de la transmission sur le réseau et stockées uniquement en tant que hash salé.

Les communications entre les clients et les services backend s'effectuent sur un canal chiffré afin d'en renforcer la sécurité. Les meilleurs outils du secteur analysent régulièrement les services afin de s'assurer qu'ils répondent en permanence aux normes les plus strictes. Les services prennent en charge des connexions TLS v1.2 avec des suites de chiffrement sécurisées.

Chiffrement au repos

Tous les fichiers téléchargés par les clients d'Autodesk Construction Cloud sont stockés dans le cloud dans des systèmes de stockage chiffré. La solution de stockage utilise une méthode de chiffrement avancé à 256 bits (AES-256), qui fait partie des méthodes de chiffrement par blocs les plus puissantes. L'ensemble du processus de chiffrement, de gestion des clés et de déchiffrement est régulièrement inspecté et vérifié en interne dans le cadre de notre processus d'audit en place.

Contrôles administratifs

Autodesk Construction Cloud fournit aux administrateurs des clients des fonctionnalités de sécurité pour créer des politiques de gestion des identités et des accès.

- **Provisionnement des utilisateurs.** Les administrateurs peuvent créer et désactiver des utilisateurs.
- **Utilisation de la sécurité basée sur les rôles.** Avec les rôles Autodesk Construction Cloud, les administrateurs peuvent personnaliser les niveaux de contrôle d'accès afin de fournir des contrôles granulaires de restriction des accès. Un rôle est un ensemble d'autorisations sur des données et des fonctionnalités qui sont liées à une fonction professionnelle.

En offrant un moyen flexible d'attribuer des autorisations en fonction des rôles, Autodesk Construction Cloud adhère au principe du moindre privilège. Ce principe énonce que l'accès aux données et aux fonctionnalités de chaque utilisateur est limité à ce dont ce dernier a besoin pour effectuer les tâches qui lui sont assignées.

Contrôle utilisateur

Les utilisateurs sont libres de contrôler les accès aux ressources, rapports et fichiers dont ils sont propriétaires, à l'exception des restrictions d'administration. Les utilisateurs peuvent également recourir à la gestion des versions pour restaurer les versions précédentes des fichiers qu'ils ont joints aux éléments de l'espace de travail.

Normes de fédération des identités

Autodesk Construction Cloud prend en charge l'authentification unique (SSO, Single Sign On) sur les systèmes des clients pour tous les utilisateurs.

Sécurité cloud

Notre équipe dédiée à la sécurité d'Autodesk axe ses efforts sur l'identification et l'application des règles de sécurité dans l'environnement Autodesk Construction Cloud. Ses responsabilités comprennent :

- l'examen de la position en matière de sécurité dans la conception et la mise en œuvre de l'infrastructure cloud d'Autodesk ;
- la définition et la garantie de la mise en œuvre des politiques de sécurité, notamment la gestion des identités et des accès, la gestion des mots de passe et la gestion des vulnérabilités ;
- le respect de la conformité dans les procédures de sécurité établies en effectuant des examens et des audits ;

- l'identification et la mise en œuvre de technologies visant à sécuriser les informations des clients ;
- le recrutement d'experts en sécurité tiers pour mener des évaluations de sécurité selon les besoins ;
- la surveillance des services cloud afin de détecter des problèmes de sécurité éventuels et la réponse aux incidents, le cas échéant.

Analyses de vulnérabilité, tests d'intrusion et audits externes

L'équipe de sécurité d'Autodesk effectue régulièrement des analyses de sécurité et des tests d'intrusion des services Autodesk Construction Cloud qui entrent dans le champ d'application de la certification SOC2. Les analyses de sécurité et les tests d'intrusion couvrent un large éventail de vulnérabilités définies par l'OWASP (Open Web Application Security Project) et la liste SANS Top 25 dans le cadre des certifications SOC2.

Sécurité réseau

La sécurité réseau est appliquée à l'aide d'une association de contrôles physiques et logiques, notamment le chiffrement, les pare-feu (physiques ou logiques) et les procédures de renforcement. Des pare-feu matériels autonomes sont déployés dans le périmètre de l'environnement cloud d'Autodesk. Tous les ports sont bloqués, à l'exception de ceux qui sont nécessaires pour répondre aux demandes des clients.

Normes de sécurité et conformité

- Autodesk Construction Cloud a sélectionné l'attestation SSAE-16 AT 101 SOC 2 de la norme du secteur pour attester de sa position en matière de sécurité. Il est prévu qu'Autodesk Construction Cloud soit intégré au prochain audit annuel SOC2 d'Autodesk.
- Une fois audité et certifié, Autodesk Construction Cloud rejoindra les services et les modules BIM 360 certifiés [ISO 27001](#), [ISO 27017](#) et [ISO 27018](#).

Pour en savoir plus sur le dernier statut d'attestation d'Autodesk Construction Cloud et les services connexes, veuillez consulter la [section « Conformité » du Centre de confiance Autodesk](#).

Confidentialité

Autodesk fait preuve de transparence sur la manière dont les données personnelles des clients sont collectées et utilisées. Lisez la [Déclaration de confidentialité](#) d'Autodesk pour en savoir plus. Vous pouvez également consulter la section Conformité du [Centre de confiance Autodesk](#).

mens  **maschine**
CAD as CAD can

Mensch Maschine Suisse SA

Route du Simplon 16 - 1094 Paudex- Lausanne
021 793 20 32 – info.fr@mum.ch - www.fr.mum.ch

Ressources

Les ressources suivantes fournissent des informations générales sur Autodesk et d'autres renseignements sur les thèmes abordés dans ce document.

- Pour en savoir plus sur Autodesk, consultez le site <http://www.autodesk.fr>.
- Pour en savoir plus sur notre cadre de sécurité global, consultez le site <https://www.autodesk.fr/trust/security>.
- Les applications Autodesk Construction Cloud sont hébergées dans AWS. Ainsi, la sécurité et l'infrastructure sont une responsabilité partagée entre Autodesk et Amazon. Pour en savoir plus sur la sécurité d'Amazon, veuillez consulter les ressources suivantes :
 - [Conformité AWS](#)
 - [Contrôles du centre de données AWS](#)
 - [Modèle de responsabilité partagée AWS](#)

Les informations contenues dans ce document représentent la position actuelle d'Autodesk, Inc. à la date de publication et Autodesk n'assume aucune responsabilité quant à la mise à jour de ces informations. Autodesk apporte occasionnellement des améliorations et d'autres modifications à ses produits ou services. Ainsi, les informations contenues dans ce document s'appliquent uniquement à la version d'Autodesk Construction Cloud offerte à la date de publication.

Ce livre blanc est fourni à titre d'information uniquement. Autodesk n'offre aucune garantie, expresse ou implicite, dans ce document. En outre, les informations contenues dans ce livre blanc ne créent aucune obligation ou engagement contraignant pour Autodesk.

Nonobstant ce qui précède, les services Autodesk Construction Cloud sont fournis sous réserve des Conditions générales disponibles à l'adresse <https://www.autodesk.com/company/terms-of-use/fr/general-terms>.

Autodesk, le logo Autodesk, Autodesk Construction Cloud, Civil 3D, Plant 3D et Revit sont des marques déposées d'Autodesk, Inc., et/ou de ses filiales et/ou de ses sociétés affiliées, aux États-Unis et/ou dans d'autres pays. Tous les autres noms de marques, de produits ou marques commerciales appartiennent à leurs propriétaires respectifs. Autodesk se réserve le droit de modifier à tout moment et sans préavis l'offre sur ses produits et ses services, les spécifications de produits, ainsi que ses tarifs. Autodesk ne saurait être tenue responsable des erreurs typographiques ou graphiques susceptibles d'apparaître dans ce document. © 2020 Autodesk, Inc. Tous droits réservés.

États-Unis
+1 (866) 475-3802
autodesk.com/construction

mensch  **maschine**
CAD as CAD can

Mensch Maschine Suisse SA
Route du Simplon 16 - 1094 Paudex - Lausanne
021 793 20 32 – info.fr@mum.ch - www.fr.mum.ch

Royaume-Uni et EMEA
+44 808 1892 253
acs.emea@autodesk.com
construction.autodesk.com/gb