LOGITECH SYNC

LIVRE BLANC – SÉCURITÉ ET CONFIDENTIALITÉ

logitech®

INTRODUCTION

Grâce à Logitech® Sync, la gestion des salles de réunion ainsi que des dispositifs Logitech n'a jamais été aussi simple et intuitive. Avec son architecture sécurisée basée sur le cloud, Sync permet le déploiement et la gestion de vos solutions de visioconférence à l'échelle de votre entreprise. Ce livre blanc explique comment Logitech Sync aborde la sécurité et la confidentialité quant aux données clients, aux versions des micrologiciels et au développement de logiciels.

Leader mondial dans le développement de matériel informatique, de logiciels et de services, Logitech relie les individus aux expériences numériques qui les attirent. Nous proposons un large éventail d'outils collaboratifs faciles à utiliser. Par ailleurs, nos logiciels simples d'utilisation vous permettent de surveiller et de gérer vos solutions de collaboration vidéo, et d'obtenir des informations clés sur celles-ci. Ainsi, vos équipes virtuelles travaillent plus efficacement.

Logitech Sync fait partie intégrante de nos solutions de visioconférence. Sync est une plateforme de gestion des dispositifs basée sur le cloud qui permet aux services informatiques de gérer et de surveiller les dispositifs Logitech des salles de réunion à l'échelle de l'entreprise. Elle fonctionne en liaison avec l'application Logitech Sync, exécutée sur un ordinateur ou un dispositif vidéo dans la salle de réunion.

Sync traite les données ainsi que les informations provenant des dispositifs. La plateforme fournit aux administrateurs informatiques des données exploitables en matière de surveillance et de gestion ainsi que des informations essentielles sur les salles. Les utilisateurs de Sync se connectent facilement au portail Web dédié sur sync.logitech.com afin de gérer leurs dispositifs Logitech.

Cette approche novatrice de la surveillance à distance et de la gestion des dispositifs simplifie des tâches telles que les mises à jour des micrologiciels et l'activation des fonctionnalités, tandis qu'une API et une architecture avant-gardiste constituent une base solide pour de nouvelles idées et intégrations.

La sécurité et la confidentialité constituent évidemment des enjeux majeurs pour les responsables informatiques dans le cadre de la gestion des données et des mises à jour logicielles. C'est pourquoi nous avons élaboré ce livre blanc, qui aborde la gestion par Logitech Sync des données personnelles et la mise à disposition des versions des micrologiciels. Ces données sont utilisées conformément à la Politique de confidentialité Logitech et aux Conditions d'utilisation.

Remarque : La version la plus récente de ce livre blanc est disponible sur le site Web de Logitech.

GESTION DE LA SÉCURITÉ CHEZ LOGITECH

Nos clients peuvent dormir sur leurs deux oreilles : Logitech élabore et met en œuvre des bonnes pratiques en matière de sécurité des données. Tous les protocoles de sécurité concernant le développement de logiciels de visioconférence s'appuient sur les normes NIST 800-53 et ISO/IEC 27001:2013. Nos processus de sécurité sont gérés par un ensemble varié de parties prenantes, de la gestion à l'ingénierie, qui appliquent ces normes comme des principes fondamentaux dans le cadre de notre cycle de vie de développement logiciel sécurisé (SSDLC).

INTÉGRATION ET LIVRAISON CONTINUES

Logitech met en œuvre un solide couloir d'intégration et de livraison continu (CI/CD) qui assure le respect d'exigences d'ingénierie strictes afin de garantir la qualité des logiciels avant le déploiement de tout nouveau changement. Ce processus harmonise la garantie de qualité, y compris, mais pas uniquement, les tests fonctionnels, les tests de sécurité, les tests d'intégration et les approbations de modifications de la part de l'ensemble des parties prenantes. Notre processus assure un déploiement fluide des nouvelles versions des logiciels, sans nuire à la disponibilité du service.

TEST DE SÉCURITÉ APPLICATIVE

Logitech mène des tests de sécurité par le biais d'experts indépendants afin d'identifier d'éventuelles failles. Les tests statiques de sécurité des applications (SAST), les tests dynamiques de sécurité des applications (DAST) ainsi que l'évaluation de la configuration du service cloud portent notamment sur les failles de sécurité courantes énoncées dans le projet Open Web Application Security Project (OWASP) et la liste Common Weakness Enumeration (CWE) de l'organisme MITRE. En cas de détection d'une faille dans le cadre de ces tests, Logitech résoudra tous les problèmes de sécurité identifiés par les experts. Si l'évaluation de sécurité tierce est effectuée sur les versions principales, Logitech réalise également des tests SAST et DAST en interne au cours des cycles de développement.

AUTHENTIFICATION ET AUTORISATION DE L'UTILISATEUR

Afin de gérer leurs dispositifs Logitech, les utilisateurs de Sync se connectent au portail Web, qui utilise des mécanismes d'accès basés sur des jetons et des rôles afin de les authentifier et d'autoriser la portée de l'accès. Les utilisateurs consultent ou modifient les données en fonction des rôles qui leur sont attribués dans le système. Par ailleurs, chaque jeton de sécurité repose sur une session et une période de validité limitée. Afin de sécuriser le système, les utilisateurs doivent actualiser leur accès en renseignant à nouveau leurs identifiants après expiration du jeton.

INTÉGRATIONS À AUTHENTIFICATION UNIQUE (*SINGLE SIGN-ON*, SSO)

Le service d'authentification du portail Sync de Logitech prend en charge l'authentification unique et peut être intégré à des fournisseurs d'identité (IdP) SAML 2.0 standards tels qu'Azure Active Directory et Okta. Ainsi, le portail Sync peut authentifier les utilisateurs via leurs identifiants professionnels sans avoir à gérer des identifiants distincts sur la plateforme Sync.

DONNÉES EN TRANSFERT

Logitech Sync compte deux composantes : l'application de bureau Sync, exécutée sur le matériel informatique présent dans la salle, et le portail Sync dans le cloud. Une fois installée et authentifiée, votre application Sync communique directement avec le portail Sync afin de fournir une gestion à distance, des fonctions de surveillance et diverses informations clés quant à l'utilisation et aux performances.

Toutes les communications[1] entre le portail Sync dans le cloud et votre application Sync utilisent les protocoles de réseau HTTPS et MQTT. Le trafic de ces deux protocoles est authentifié et chiffré via la version 1.2 ou ultérieure du protocole Transport Level Security (TLS) avec les suites cryptographiques AES de 128/256 bits afin de garantir la confidentialité et l'intégrité des données sur Internet.

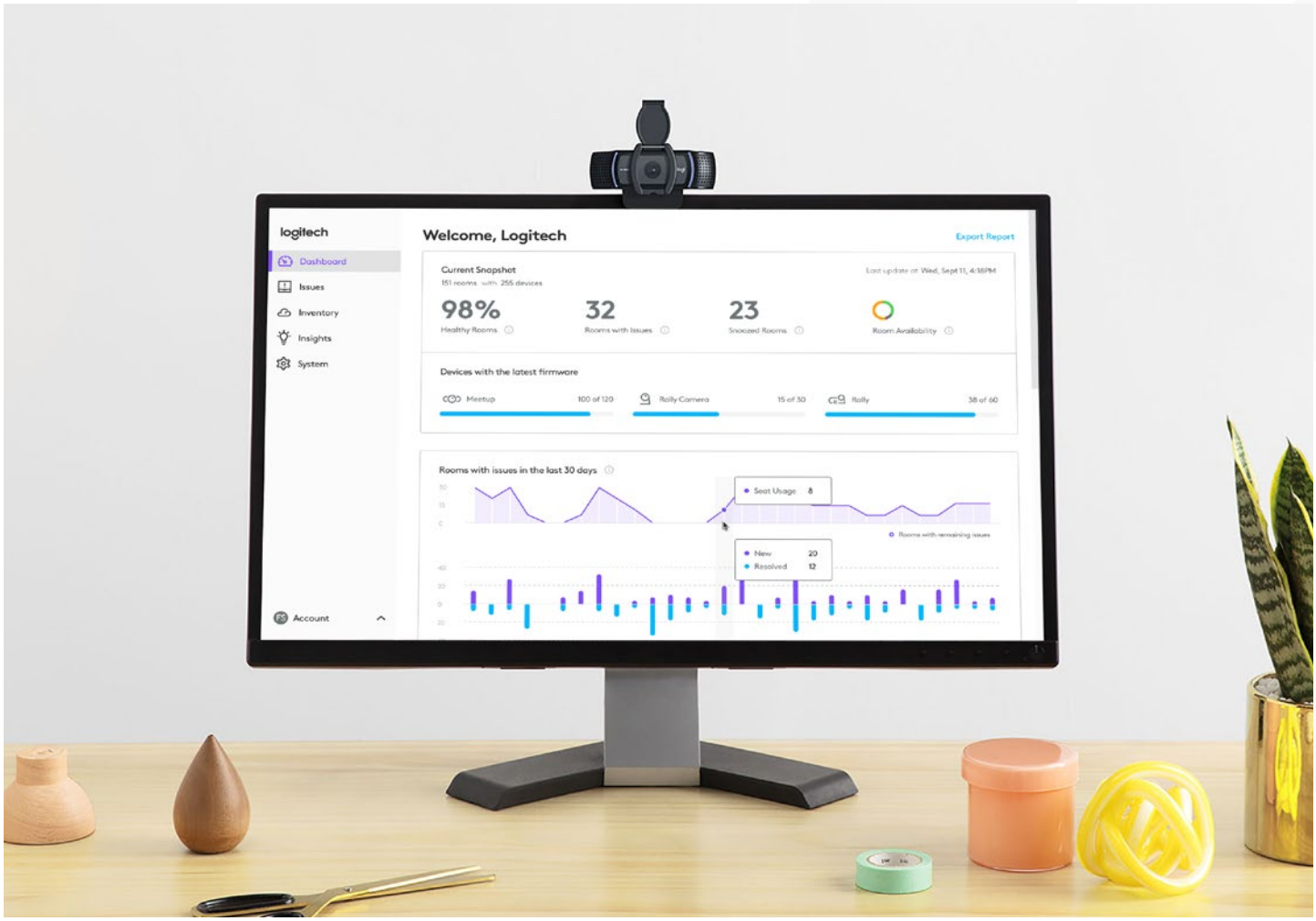
SÉCURITÉ DES DONNÉES

DONNÉES STOCKÉES

Les données clients dans le service dorsal de Sync sont protégées grâce aux chiffrements AES à 256 bits de haut niveau dans la base de données. Par ailleurs, les clés de chiffrement sont à nouveau chiffrées et gérées de façon centralisée par les services de données AWS afin d'éviter les fuites de données clients.

DISPONIBILITÉ DU SERVICE ET RÉCUPÉRATION DES DONNÉES APRÈS INCIDENT

Afin de garantir un service continu, Logitech Sync repose sur une architecture et une infrastructure insensibles aux défaillances pour un service hautement disponible. La grande évolutivité des ressources informatiques et la répartition de la charge permettent d'obtenir un tel niveau de disponibilité. Les données actuelles sont hébergées sur des serveurs situés sur la côte ouest des États-Unis et sauvegardées de façon continue dans le centre de données. En cas d'urgence, Logitech Sync peut effectuer une récupération à tout moment et dans toute zone géographique au cours des 35 derniers jours, et ce sans interruption du service.



COLLECTE ET CONFIDENTIALITÉ DES DONNÉES

La Politique de confidentialité et de sécurité décrit les types de données collectées par Logitech, leur utilisation ainsi que la protection des informations personnelles recueillies par ses produits, services, applications et logiciels. Logitech est un groupe d'entreprises opérant sous une société mère, Logitech International S.A. L'entreprise Logitech qui gère vos données dépend de vos relations à notre égard (client, partenaire, sous-traitant ou autre). Nous ne collectons et ne stockons dans le cloud aucune piste audio, aucun fichier vidéo, ni aucune image provenant d'une salle de réunion. Dans le tableau 1.1 ci-dessous, vous trouverez la liste complète des données que nous collectons ainsi que des utilisations que nous en faisons.

Source de collecte de données	Type de données collectées	Fins de la collecte de données	Stockage des données
Portail Sync (inscription et création de compte)	• Adresse e-mail • Mot de passe • Prénom • Nom • Nom de l'organisation	Authentification des utilisateurs et création de compte.	AWS
Informations supplémentaires fournies par l'utilisateur pour le portail Sync	• Nom de la salle • Nombre d'utilisateurs • Noms de groupe	Identification et regroupement de salles dans Sync. Le nombre d'utilisateurs est utilisé avec des métadonnées relatives à l'occupation des salles dans le but d'évaluer l'utilisation des licences.	AWS
Application Sync (installée sur le PC ou un autre dispositif dans la salle de réunion, tel que Logitech Rally Bar)	• Nom du dispositif • Identifiant unique du dispositif • Version du micrologiciel du dispositif • Numéro de série du dispositif • Version de l'application Sync • Type de système d'exploitation de l'ordinateur • Version du système d'exploitation de l'ordinateur • Adresse IP/MAC • Métadonnées sur les caractéristiques de l'ordinateur • Occupation de la salle de réunion (métadonnées uniquement)	Ces informations sont utilisées pour fournir des fonctions de surveillance, de gestion et d'analyse via le portail Sync.	AWS

CONFIDENTIALITÉ DES DONNÉES

ACCÈS AU SERVICE ET AUX DONNÉES CLIENTS

Logitech collabore avec les plateformes AWS dans le cadre de l'hébergement de ses services logiciels et des données des utilisateurs. AWS met en œuvre des directives opérationnelles strictes, des niveaux de protection et des processus de surveillance afin de garantir que seuls les employés autorisés peuvent accéder à ses centres de données.

Chez Logitech, l'accès à la base de données des clients et aux paramètres du service est limité à un petit groupe de personnes autorisées chargées de la gestion du service.

STOCKAGE ET SUPPRESSION DES DONNÉES

Lorsqu'un client s'inscrit dans le cadre de Logitech Sync, toutes les données sur l'utilisateur et le dispositif collectées de façon régulière sont stockées dans le service jusqu'à la désinscription du client. Pour quitter le service, les clients doivent en faire la demande via le formulaire Web disponible sur support.logitech.com/response-center. Ils seront ensuite guidés par Logitech à travers la procédure de suppression. Une fois le compte supprimé, toutes les données du client, excepté les journaux de produit, seront immédiatement supprimées de façon définitive.

RÉPONSE AUX INCIDENTS DE SÉCURITÉ

Logitech s'engage à fournir des produits ainsi que des services sécurisés à ses clients et accepte volontiers les retours de chercheurs indépendants, d'organismes du secteur, de fournisseurs, de clients et d'autres entités en matière de sécurité. Logitech définit une faille de sécurité comme une fragilité involontaire dont un pirate informatique peut profiter en vue de compromettre l'intégrité, la disponibilité ou la confidentialité d'un produit, d'un logiciel ou d'un service.

Le service de sécurité de Logitech met en œuvre divers indicateurs afin de surveiller la latence de trafic, les seuils et les taux d'erreur concernant des activités suspectes. Il mène également des tests de sécurité réguliers par le biais de prestataires tiers concernant les versions principales afin de veiller à la sécurité du produit. Toute faille est ainsi résolue en conséquence.

En cas de problème, l'équipe de produit, en collaboration avec le service de sécurité de Logitech, mènera une enquête dans les plus brefs délais sur les anomalies et les failles de sécurité signalées à l'échelle de l'entreprise. Vous pouvez faire part de votre problème au service de sécurité de Logitech via nos pages Déclaration de vulnérabilité ou Programme Bug Bounty.

logitech

Contactez votre revendeur ou contactez-nous à l'adresse www.logitech.com/vcsales

Logitech Americas
7700 Gateway Blvd.
Newark, CA 94560 États-Unis

Logitech Europe S.A.
EPFL - Quartier de l'Innovation
Daniel Borel Innovation Center
CH - 1015 Lausanne

Logitech Asia Pacific Ltd.
Tél. : 852-2821-5900
Fax : 852-2520-2230

[1] Une mise à jour du micrologiciel pour Logitech MeetUp, Rally, Rally Cam, Tap et Swytch sera effectuée en 2021 afin de configurer le chiffrement complet pour ces nouveaux dispositifs.

Publié en juin 2021