LOGITECH SYNC

SECURITY & PRIVACY WHITEPAPER

logitech®

INTRODUCTION

Logitech® Sync makes managing meeting rooms and Logitech devices easy and intuitive. Built on secure, cloud-based architecture, Sync helps you deploy and manage video conferencing at scale. This whitepaper explains how Logitech Sync handles security and privacy of customer data, firmware releases, and software development.

A world leader in developing hardware, software, and services solutions, Logitech connects people to the digital experiences they care about. We offer a range of collaboration tools that are easy to use. And we provide simple-to-use software to help you monitor, manage, and receive insights about your video collaboration solutions, enabling virtual teams to work more effectively.

Logitech Sync is an integral part of our video collaboration solutions. Sync is a cloud-based device-management platform that allows IT to manage and monitor Logitech meeting room devices at scale. It works in conjunction with the Logitech Sync App, which runs on a computer or video appliance device in the meeting room.

Sync processes data and information that hardware devices report to it and presents IT admins with actionable data regarding monitoring, management, and room insights. Sync users easily log on to the dedicated web portal at sync.logitech.com to manage their Logitech devices.

This fresh approach to remote monitoring and device management simplifies tasks like firmware updates and feature enablement, while the API and forward-looking architecture establish a robust foundation for new insights and integrations.

Naturally, IT leaders are concerned about security and privacy when it comes to the handling of data and software updates. To address this topic, we created the following whitepaper, which discusses Logitech Sync's handling of personal data and the delivery of firmware releases. We use such data in a manner consistent with the Logitech Privacy Policy and Terms of Service.

Note: The most current version of this white paper may be found on the Logitech website.

SECURITY GOVERNANCE AT LOGITECH

Customers can be confident that Logitech establishes and implements best-practice information security processes. All video collaboration software development security protocols use NIST 800-53 and ISO/IEC 27001:2013 as guiding roadmaps. Our security processes are managed by a diverse set of product stakeholders, ranging from product management to engineering, who apply these security standards as core operating principles in our Secure Software Development Lifecycle (SSDLC).

CONTINUOUS INTEGRATION AND DELIVERY

Logitech implements a well-established Continuous Integration and Delivery (CI/CD) pipeline that enforces strict engineering requirements to ensure the quality of the software before any new changes deploy to production. The process streamlines quality assurance including, but not limited to, functional tests, security tests, integrations tests, and change approvals from all stakeholders. Our deployment process ensures the new software release is seamlessly deployed without impacting service availability.

APPLICATION SECURITY TESTING

Logitech conducts security testing by third-party security consultants to identify vulnerabilities. Such Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), and cloud service configuration assessment align with but are not limited to, common security weaknesses as outlined in the Open Web Application Security Project (OWASP) and MITRE's Common Weakness Enumeration(CWE). Should any vulnerabilities appear within the context of testing, Logitech will remediate all security issues as identified by the vendor. While the third-party security assessment is done on major releases, Logitech also runs in-house SAST and DAST during development cycles.

USER AUTHENTICATION AND AUTHORIZATION

When the Sync users log in to the web portal to manage their Logitech devices, the Sync portal uses token-based and role-based access mechanisms to authenticate them and authorize the scope of access. Users view or modify data based on their assigned role in the system. Each security token is also session-based and valid for a certain time. Once the token expires, users must refresh access by providing their credentials again to maintain a secure system.

SINGLE SIGN-ON (SSO) INTEGRATIONS

The Logitech Sync Portal authentication service supports single sign-on (SSO) and can be integrated with standard SAML2.0 Identity Providers (IdP) such as Azure Active Directory and Okta. These providers allow the Sync Portal to authenticate users using their enterprise credentials without managing separate credentials while in the Sync platform.

DATA IN TRANSIT

Logitech Sync is made up of two parts: the desktop Sync application which runs on your in-room hardware, and the cloud-based Sync Portal. Once installed and authenticated, your Sync application communicates directly with Sync Portal to enable remote management, monitoring capabilities, and various insights regarding room usage and performance.

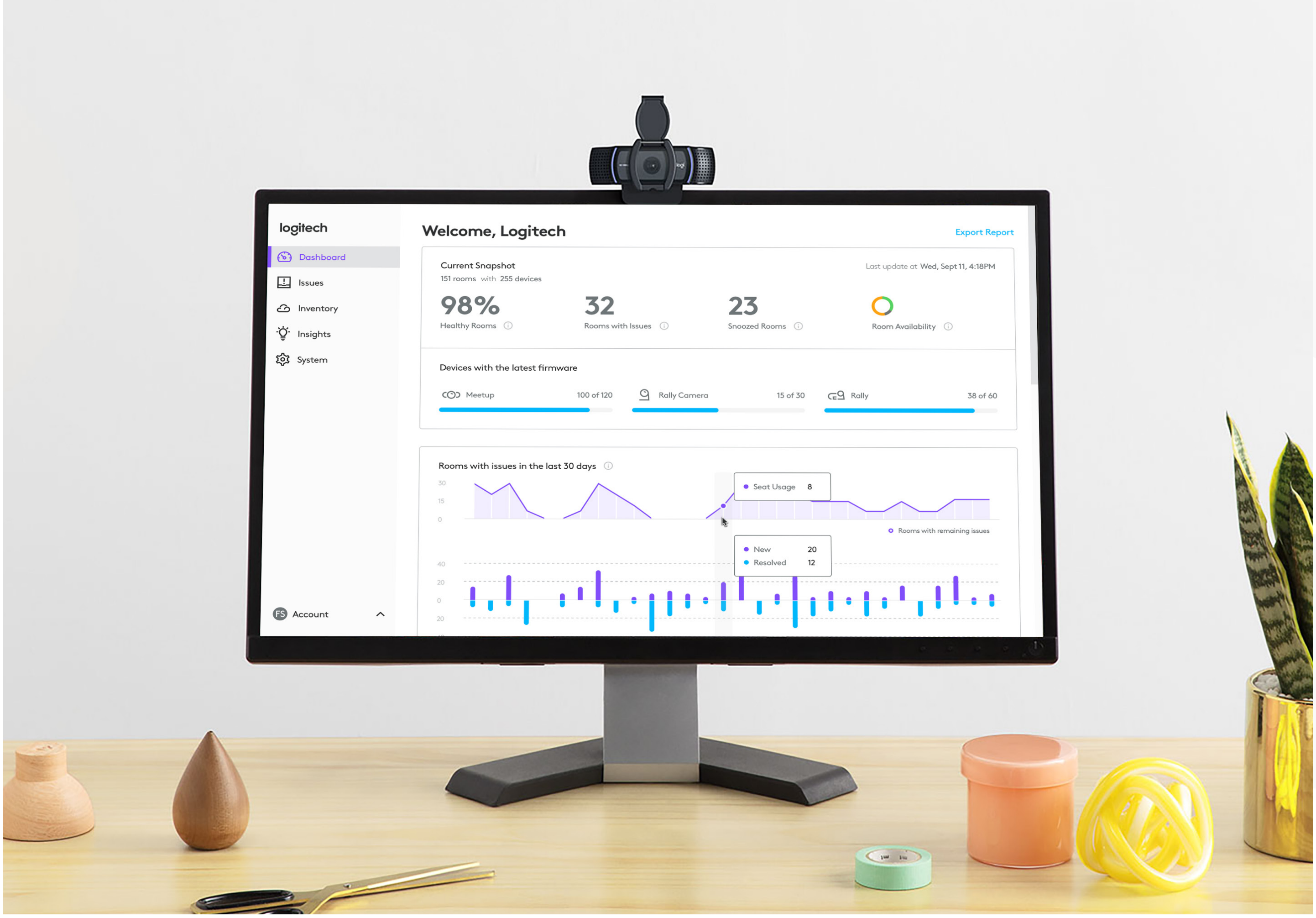
All communication[1] between the Logitech Sync cloud-based portal and your Sync application exists within HTTPS and MQTT network protocols. The traffic from both protocols is authenticated and encrypted using Transport Level Security (TLS) version 1.2 or above with AES-128/256-bit cipher suites support to ensure confidentiality and data integrity over the internet.

DATA AT REST

The customer data in Sync's backend service is protected using the strongest standard AES-256 bit encryptions inside the database. Also, the encryption keys are further encrypted and centrally managed by the AWS data services to safeguard customer data from data breaches.

SERVICE AVAILABILITY AND DISASTER RECOVERY

To ensure 24/7 service, Logitech Sync is designed with fault-tolerant software architecture and infrastructure for a highly available service. To achieve High Availability (HA), computing resources are highly scalable and load distributed. Current data is hosted on servers on the US West Coast, and data is continuously backed up within the data center. In case of an emergency, Logitech Sync can recover at any point and in any region without interruption of service within the past 35 days.



DATA COLLECTION AND PRIVACY

The Privacy & Security Policy outlines what types of data Logitech collects, how we use it, and how we protect personal information collected by our products, services, apps, and software. Logitech is a group of companies working under their parent company; Logitech International S.A. The Logitech company that controls your data will vary depending on your relationship with us (whether it be as a customer, partner, contractor, or any other relevant relationship). We do not capture or store any sound, video, or static images from a meeting room to the cloud at any time. In Chart 1.1 below, we offer a full listing of what data we do collect and its usage.

Data collection source	Type of data collected	Purpose of data collection	Data Store
Sync Portal (registration and account creation)	• Email address • Password • First name • Last name • Organization name	User authentication and account creation for individuals.	AWS
Sync Portal additional user-provided information	• Room name • Seat count • Group names	Identification and grouping of rooms within Sync. Seat count is used to calculate seat usage in combination with room occupancy metadata.	AWS
Sync App (installed on the meeting room PC or appliance, such as Logitech Rally Bar)	• Device name • Device unique ID • Device firmware version • Device serial number • Sync app version • Computer OS type • Computer OS version • IP/MAC address • Computer specification metadata • Meeting room occupancy (metadata only)	Information is used to provide monitoring, management, and analytic capabilities through Sync Portal.	AWS

SERVICE AND CUSTOMER DATA ACCESS

Logitech contracts with AWS platforms to host our software services and the user data. AWS implements strict operation guidelines, layers of protection, and monitoring to ensure its data centers are only accessible by approved employees.

Inside Logitech, access to the customer database and the service settings are restricted to a small group of approved individuals responsible for maintaining and supporting the service.

DATA RETENTION AND DELETION

Once a customer signs up for Logitech Sync, all user and device data regularly collected is retained within the service until the customer decides to opt-out of the service. To exit the service, customers should make their request by completing the webform at support.logitech.com/response-center Logitech will then walk through the deletion process with the customer. Once the account has been marked as deleted, all customer data except product logs will be permanently deleted immediately.

SECURITY INCIDENT RESPONSE

Logitech is committed to providing secure products and services to our customers and welcomes reports from independent researchers, industry organizations, vendors, customers, and other sources concerned with security. Logitech defines a security vulnerability as an unintended weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of a product, software, or service.

Logitech Security deploys various metrics to monitor traffic latency, thresholds, and error rates for suspicious activities. It also conducts regular security tests by third-party vendors on major releases to ensure the product is secure. Any vulnerabilities are addressed accordingly.

Should you encounter an issue, the product team in collaboration with Logitech Security promptly investigates reported anomalies and suspected security breaches on an enterprise-wide level. You may submit your security concern or break with Logitech security by using our Vulnerability Disclosure page or Bug Bounty Program page.

logitech®

Contact your reseller
or contact us at
www.logitech.com/vcsales

Logitech Americas
7700 Gateway Blvd.
Newark, CA 94560 USA

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

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

[1] A firmware update for Logitech Meetup, Rally, Rally Cam, Tap, and Swytch will take place in 2021 to configure full encryption for these newer devices.

This whitepaper is provided for informational purposes only. Logitech makes no warranties, express or implied or statutory as to the information in this whitepaper. This whitepaper is provided "as is" and may be updated by Logitech from time to time. Visit the Logitech website for the latest version.

Published June 2021