Security & Privacy Whitepaper

Logitech Sync & Space Management

logitech®

Logitech Sync is the management platform for your entire workplace, streamlining the management of rooms, desks, and devices. Built on a secure, cloud-based architecture, Sync supports large-scale deployment, configuration, monitoring, and updates across your environment.

Sync also powers space management features such as Logitech Room Booking, Desk Booking, and View, features that help employees easily find and reserve spaces while giving IT teams visibility and control to optimize the workplace.

IT administrators can access everything through the Sync web portal, where they manage devices, apply policies, view activity data, and gain insights across rooms and desks — all within a single, unified platform.

IT leaders often have questions about security and privacy when onboarding a new tool for their teams. This whitepaper outlines how Logitech Sync — including Room Booking, Desk Booking, and View — protects customer data, manages updates, and ensures compliance with the Logitech Privacy Policy and Terms of Service.

Note: The latest version of this whitepaper is available on the Logitech website.

Security governance at Logitech

Customers can be confident that Logitech has established and implemented best-practice information security processes. All space management software development security protocols use 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 are deployed to production. The process streamlines quality assurance, including, but not limited to, functional tests, security tests, integration tests, and change approvals from all stakeholders. Our deployment process ensures that new software releases are seamlessly deployed without impacting service availability.

Application security testing

To demonstrate our dedication to security, Logitech has integrated several application security tools into the development lifecycle, including Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST). Additionally, Logitech has allocated resources to dedicated security teams tasked with identifying security issues and vulnerabilities in our products.

Logitech also conducts security testing through third-party security consultants. These assessments encompass but are not limited to common security weaknesses outlined in the Open Web Application Security Project (OWASP) and MITRE's Common Weakness Enumeration (CWE). If any vulnerabilities are identified during testing, Logitech will promptly address all security issues as identified by the vendor.

User authentication and authorization

When IT team members log in to the Sync web portal to manage their Logitech devices, the Sync portal uses token-based and role-based access mechanisms to authenticate 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 specific timeframe. Once the token expires, users must refresh access by providing their credentials again to maintain a secure system.

Calendar authentication and authorization

When IT team members connect a calendar service to their Logitech Sync Portal account to use with Logitech Room Booking, Desk Booking, or View, they must first sign into the calendar service using a service account for that particular service provider. Once they have successfully signed in, the calendar service provider will show IT users the access Sync requires to carry out Room Booking, space automation, workplace insights, and View functionality.

For calendars connected to Sync, we request the following access rights:

Microsoft 365

- offline_access
- Calendars.ReadWrite.Shared
- Place.Read.All
- User.Read

Google Workspace

- https://www.googleapis.com/auth/userinfo.email
- https://www.googleapis.com/auth/admin.directory.resource.calendar.readonly
- https://www.googleapis.com/auth/calendar.events
- https://www.googleapis.com/auth/admin.directory.user.readonly
- https://www.googleapis.com/auth/calendar.calendarlist.readonly

This allows Logitech Room Booking, Desk Booking, and View to read calendar data, show events, indicate room status, add ad-hoc meetings, edit meetings on the calendar, and carry out space automation like Auto Book and Auto Release.

Auto Book and Auto Release space automations

With calendar access and in-room participant data from Sync it's possible to enable space automation with Auto Book and Auto Release for meeting rooms and spaces. When someone is detected in a space by a supported camera or sensors in the room, that space can be booked automatically; if no one shows up, the space can be released; and, if the meeting ends early, the end time can be adjusted to ensure that in-room usage is accurate.

Single sign-on (SSO) integrations

The Logitech Sync Portal authentication service supports single sign-on (SSO) and can be integrated with standard SAML 2.0 Identity Providers (IdP) such as Microsoft Entra ID and Okta. These providers allow the Sync Portal to authenticate users using their enterprise credentials without managing separate credentials while in the Sync platform. Users can register a domain and set up their single sign-on within Sync.

Data in transit

Logitech Sync is made up of two parts: Sync clients and the cloud-based Sync Portal. Sync clients include the Logitech Sync App running on meeting room PCs and CollabOS devices, and Logitech Tune running on personal devices. Once connected, the Sync client communicates directly with the Sync Portal to enable remote management, monitoring, and various insights regarding room usage and performance.

Similarly, Logitech Room Booking, Desk Booking, View, space automation, and workspace insights are made up of two parts: 1) the Room Booking, Desk Booking, and View apps, and 2) the cloud-based Sync Portal. The Room Booking app runs on Tap Scheduler, a CollabOS device; the Logi Tune app runs on Windows/Mac/iOS/Android; and the View app runs on RoomMate, also a CollabOS device. The Room Booking, Desk Booking, and View apps communicate directly with Sync Portal to receive data on the rooms and desks they are connected to as well as for calendar events.

All communication between Sync Portal and Sync clients, as well as between Sync Portal and the Room Booking, Desk Booking, and View apps, occurs over HTTPS and MQTT network protocols. The traffic from both protocols is authenticated and encrypted using Transport Layer Security (TLS) version 1.2 or above, with AES 128-bit/256-bit cipher suites support, to ensure confidentiality and data integrity over the internet.

Data at rest

Customer data, calendar data, and desk booking data for Logitech Room Booking, Desk Booking, View, space management, and workplace insights are stored in Sync and are protected using the strongest standard AES 256-bit encryption. Additionally, the encryption keys are further encrypted and centrally managed by the AWS Key Management Service to safeguard customer data from data breaches. Logitech only stores 48 hours of data from connected calendar resources.

Service availability and disaster recovery

To ensure 24/7 service, Logitech Sync is built on fault-tolerant software architecture and infrastructure designed for high availability. To achieve high availability, computing resources are highly scalable and load-balanced. The service deployment process is fully automated to enable rapid redeployment in case of emergency, without service interruption.

Customer data, including that used for Room Booking, Desk Booking, View, and other space management features, is continuously backed up within the local data center. Sync provides 35 days of backup coverage, enabling full recovery in any region during service disruptions.

Data collection and privacy

The Privacy & Security Policy outlines the 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 operating under a parent company, Logitech International S.A. The specific Logitech company that controls your data will vary depending on your relationship with us (whether you are a customer, partner, or contractor, or you have another relevant relationship). We do not capture, store, or transfer any audio or video. Below, we provide a full listing of the data we collect and its usage.

Data collection source	Type of data collected	Purpose of data collection	Datastore
Sync Portal	• Room name • Seat count • Room attributes • Room alias • Group names • Room activity log • License status • Room Booking settings • Group device settings • Update channels settings • Background images • Desk name • Desk attributes • Desk activity log • Desk Booking settings • Group desk settings • User name • User email	Identification, grouping, and configuration of rooms and desks within Sync and on Tap Scheduler using Logitech Room Booking; on Logi Dock Flex with Logitech Desk Booking; on Logi Tune; and on RoomMate using Logitech View.	AWS
Sync Portal	• Occupancy data • Map data	Used to carry out Auto Book and Release functionality and to display maps.	AWS
Calendar service provider	• Calendar data: subject, start time, end time, organizer (name only), number of attendees (attendee names and other identifying information are not stored) • Resource data: display name, email address, building, floor, capacity	Room status, ad-hoc bookings, Auto Book and Release, a list of upcoming events.	AWS
Logitech Desk Booking (used through the Logi Tune application)	• Desk name • Desk attributes • Desk Booking settings • Room name • Room alias • License status • Room name • Map data • User name • User email • User profile image	Used to show desk bookings, desk status, room status, and maps.	AWS

Regional data storage

To support data residency/sovereignty and security requirements, Logitech has deployed independent Sync services in multiple regions. If you do not have regional data storage limitations, we recommend using the global instance (sync.logitech.com).

Service supported	Region	URL	AWS region
Logitech Sync Logitech Room Booking Logitech Desk Booking Logitech View	Global	sync.logitech.com	us-west-2
Logitech Sync Logitech Room Booking Logitech View	EU	eu.sync.logitech.com	eu-central-1
Logitech Sync	Canada	ca.sync.logitech.com	ca-central-1
Logitech Sync	France	fr.sync.logitech.com	eu-west-3

Service and customer data access

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

Inside Logitech, access to the customer database and service settings is 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 that is regularly collected is retained within the service until the customer decides to opt out of the service. To exit the service, customers should submit their request by completing the web form at support.logitech.com/response-center. Logitech will then guide the customer through the deletion process. Once the account has been marked as deleted, all customer data, except for 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 with 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 at an enterprise-wide level. You may submit your security concern or report through our Vulnerability Disclosure page or Bug Bounty Program page

logitech

Contact your reseller
Or contact us at
www.logitech.com/business

Logitech Americas
3930 North First St
San Jose, CA 95134 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

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.

©2025 Logitech, Inc. All rights reserved.

Published September 2025