Logitech Sync

Security & privacy whitepaper

JULY 2024

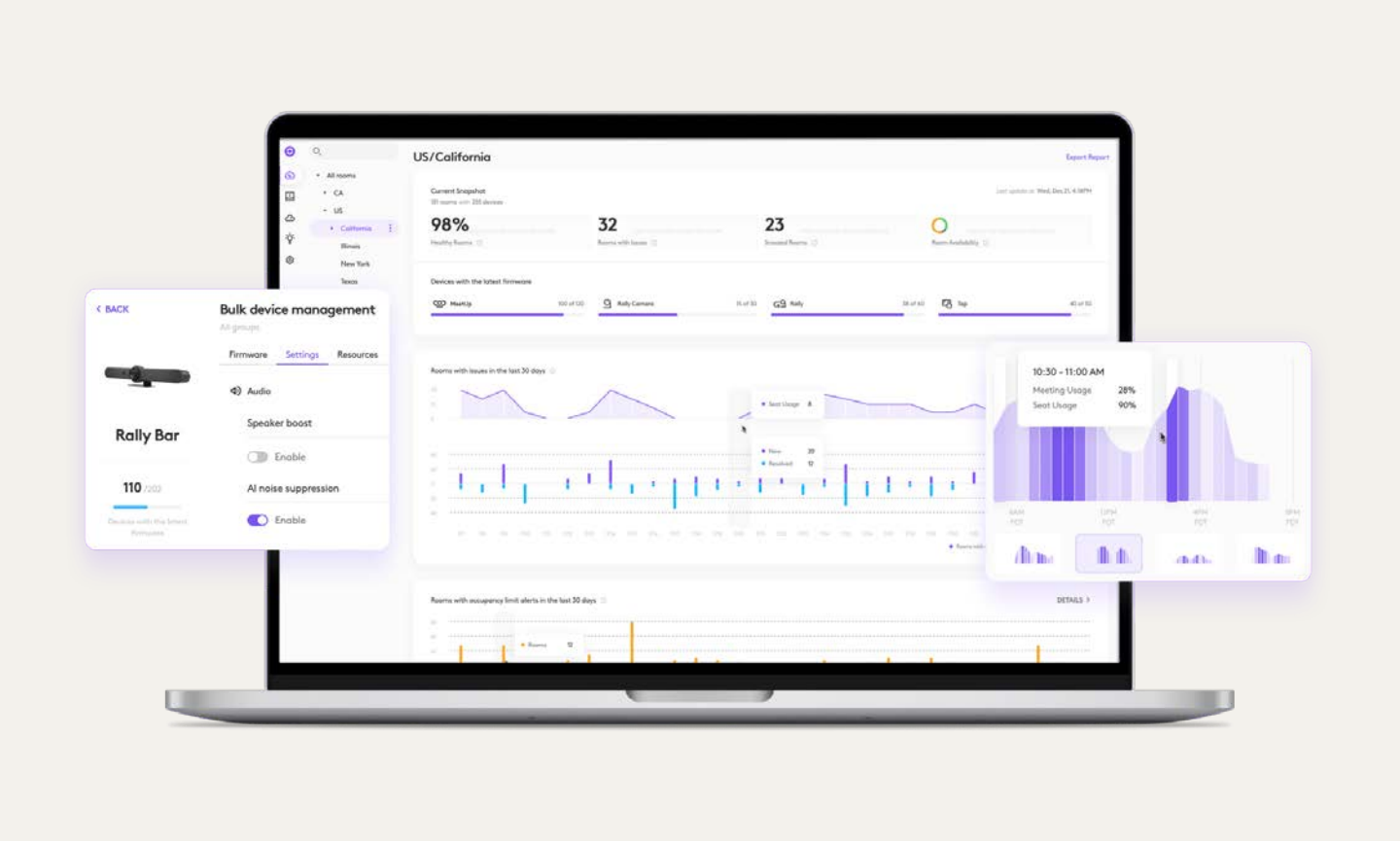
logitech

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 facilitates the deployment and management of devices across the workspace at scale. This whitepaper outlines how Sync ensures the security and privacy of customer data, manages firmware releases, and facilitates software updates.

Logitech Sync is a critical component of our space management ecosystem, offering IT administrators a cloud-based platform to efficiently oversee Logitech devices in various settings. It provides a comprehensive dashboard for monitoring and managing data, tools for device configuration and updates, and insights into device and room usage. IT admins can easily log onto the dedicated web portal at sync.logitech.com to manage Logitech devices.

IT leaders often have questions about security and privacy when onboarding a new tool for their teams. This whitepaper addresses how Logitech Sync manages personal data and firmware releases, consistent with the Logitech Privacy Policy and Terms of Service.

Note: The latest version of this white paper 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 the 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, including Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST), into the development lifecycle. 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.

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.

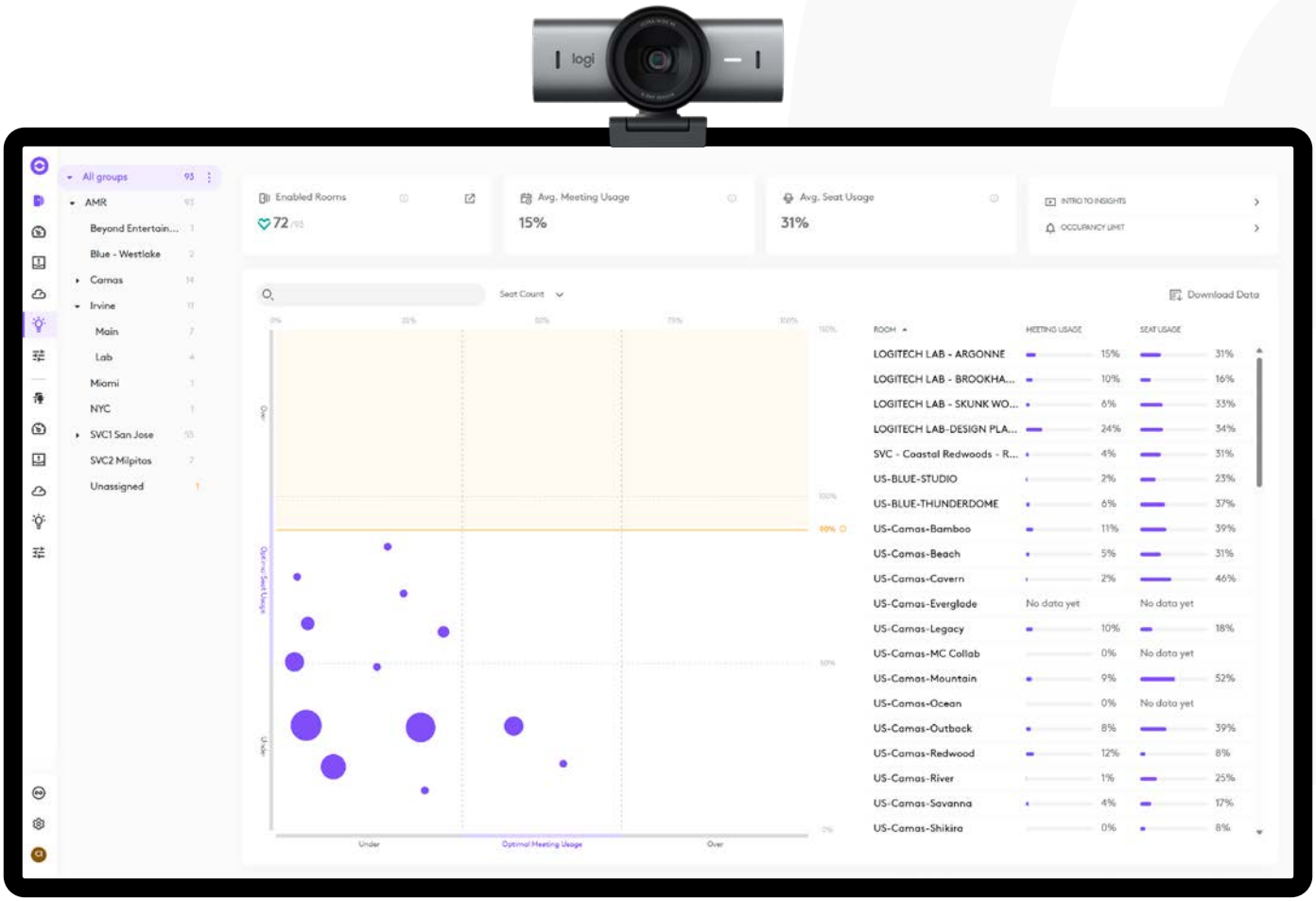
All communication between the Logitech Sync cloud-based portal and the Sync clients occurs over HTTPS and MQTT network protocols. The traffic from both protocols is authenticated and encrypted using Transport Layer Security (TLS) version 1.2 or above, with AES 128-bit/256-bit cipher suites support, to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

Data at rest

The customer data in Sync's backend service is protected using the strongest standard AES 256-bit encryptions inside the database. Additionally, the encryption keys are further encrypted and centrally managed by the AWS Key Management Service 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 highly available service. To achieve High Availability (HA), computing resources are highly scalable and load-balanced. The service deployment process is fully automated and the service can be redeployed quickly for any emergency changes without interruption of service. The customer data hosted at each site is continuously backed up locally within the data center. In the event of an emergency, Logitech Sync can recover at any point in a given region without service interruption, covering the past 35 days.



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 their 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, contractor, or have another relevant relationship). We do not capture or store any sound, video, or static images from a meeting room in the cloud at any time. In Chart 1.1 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 (IT user account and organization creation)	• Email address • Password • First name • Last name • Organization name • Country	User authentication and account creation for IT users	AWS
Sync Portal (End user account)	• Name • Email address • User groups • Profile picture	User authentication and account creation for end users	AWS
Sync Portal (System)	• Registered domains • SSO configurations • SCIM integration tokens • Organization activity log • Alerts configuration • Service accounts • Calendar resources • Maps • Sync Cloud API certificates • Reports configuration	Configuration options for your Sync account, alerts, room booking, maps, reports, and organization-level logging	AWS
Sync Portal (Rooms)	• Room name • Seat count • Room attributes • Room alias • Room notes • Room image upload • Group names • Room activity log • License status • Room Booking settings • Group device settings • Update channels settings • BYO background images • Calendar data (If Room Booking is used)	Identification, grouping, and configuration of rooms within Sync	AWS

Data collection source	Type of data collected	Purpose of data collection	Datastore
Sync Portal (Flex desks)	• Desk name • Desk attributes • Desk notes • Group names • Floor maps • Desk activity log • License status • Desk booking settings • Group device settings • Update Channels settings	Identification, grouping, and configuration of flex desks within Sync	AWS
Sync Portal (Personal devices)	• Computer name • Group names	Identification and grouping of personal computers within Sync	AWS
Sync Client (Installed on the meeting room PC, CollabOS device, or Logi Tune)	• Device name • Device unique ID • Device firmware version • Device serial number • Sync app version • Computer OS type • Computer OS version • IP/MAC address • Computer specific metadata • Meeting room occupancy and usage • Flex desk usage data • Service provider • Video bug report (manually provided by customer)	Information is used to provide monitoring, management, and analytics capabilities through Sync Portal	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).

Region	URL	AWS region
Global	sync.logitech.com	us-west-2
EU	eu.sync.logitech.com	eu-central-1
Canada	ca.sync.logitech.com	ca-central-1
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.

Published July 2024

C3239093-1025