LOGI OPTIONS+ SECURITY & PRIVACY

Introduction

The Logi Options+ App is a next-generation application that enables the customization of personal workspace devices including Logitech mice, keyboards, lights, webcams, and touchpads. Built on secure architecture, Options+ helps enterprise customers deploy and manage Logitech peripherals at scale. This whitepaper explains how Logi Options+ handles firmware releases, software development and security and privacy of customer data.

A world leader in developing hardware, software, and services solutions, Logitech connects people to the digital experiences they care about. We offer a diverse selection of user-friendly personal workspace devices, complemented by intuitive software designed to streamline the deployment of Logitech peripherals and elevate the productivity of your users.

Logi Options+ is an integral part of our comprehensive solution for the personal workspace. Administrators can silently and remotely deploy the application to a user base using commonly used enterprise deployment tools. When utilizing mass deployment, administrators can configure the application for quiet installation and enable or disable analytics, the Logitech Flow feature, SSO, and automatic updates.

The Logi Options+ application delivers a multitude of advantages to end users, such as device configuration, gesture-enhanced navigation, automation of repetitive tasks through smart actions, device-specific key functions, and beyond. This toolbox of device customization not only enhances productivity but also helps end users maximize the potential of their Logitech devices.

Our vision for personal workspace software is centered on consistently improving the hardware experience for users through ongoing innovation and value addition. Options+ represents the next generation of software designed to better cater to our enterprise customers by enhancing user experiences and providing enhanced security.

On the topic of security, we created the following whitepaper, which discusses the handling of personal data and the delivery of software updates with Logi Options+. We use such data in a manner consistent with the Logitech Privacy Policy.

Data Security

SECURITY GOVERNANCE AT LOGITECH

Logitech establishes and implements best-practice information security processes. 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). Logi Options+ software development security protocols use NIST 800-53 and ISO/IEC 27001:2013 as guiding roadmaps.

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.

LOGI ID INTEGRATION

The Logi Options+ application offers the ability to sign into Options+ via Logi ID, enabling users to back up their device settings to the cloud. Users can login with the same Logi ID used for other Logitech applications and services. Administrators can disable/enable this feature.

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 a parent company, Logitech International S.A. The Logitech company that controls your data will vary depending on your relationship with us (whether 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 the chart below under "Data Privacy," we offer a full listing of what data we do collect and its usage.

APPLICATION SECURITY TESTING

Logitech conducts security testing internally and by third-party security consultants to identify vulnerabilities. Third- party security assessment and penetration testing is done on major releases, while Logitech runs in-house Static Application Security Testing (SAST) and Software Composition Analysis (SCA) during development cycles. Should any vulnerabilities appear within the context of testing, Logitech will remediate all security issues as identified by the vendor.

DATA IN TRANSIT

The communication and data storage between the Logi Options+ application installed on the user's computer and Logitech's servers happens over the HTTPS network protocol. The traffic is authenticated and encrypted using Transport Level Security (TLS) version 1.2 or above to ensure confidentiality and data integrity over the internet.

DATA AT REST

On the user's computer, the data is stored in an encrypted format. The encryption keys are stored in secure storage.

On Logitech's servers, the data is encrypted in AWS S3 using AWS Key Management Service. Access to the data and cloud logging is limited to two Logitech Devops Admins. Read-only data access is granted to data scientists via AWS IAM role-based security.

MASS DEPLOYMENT

Logi Options+ application can be mass deployed remotely using popular deployment tools including SCCM, InTune, and Jamf. It can also be configured to disable features as you deem fit using specified command line parameters. To learn more, see our Mass Installation Guide.

FIRMWARE UPDATES

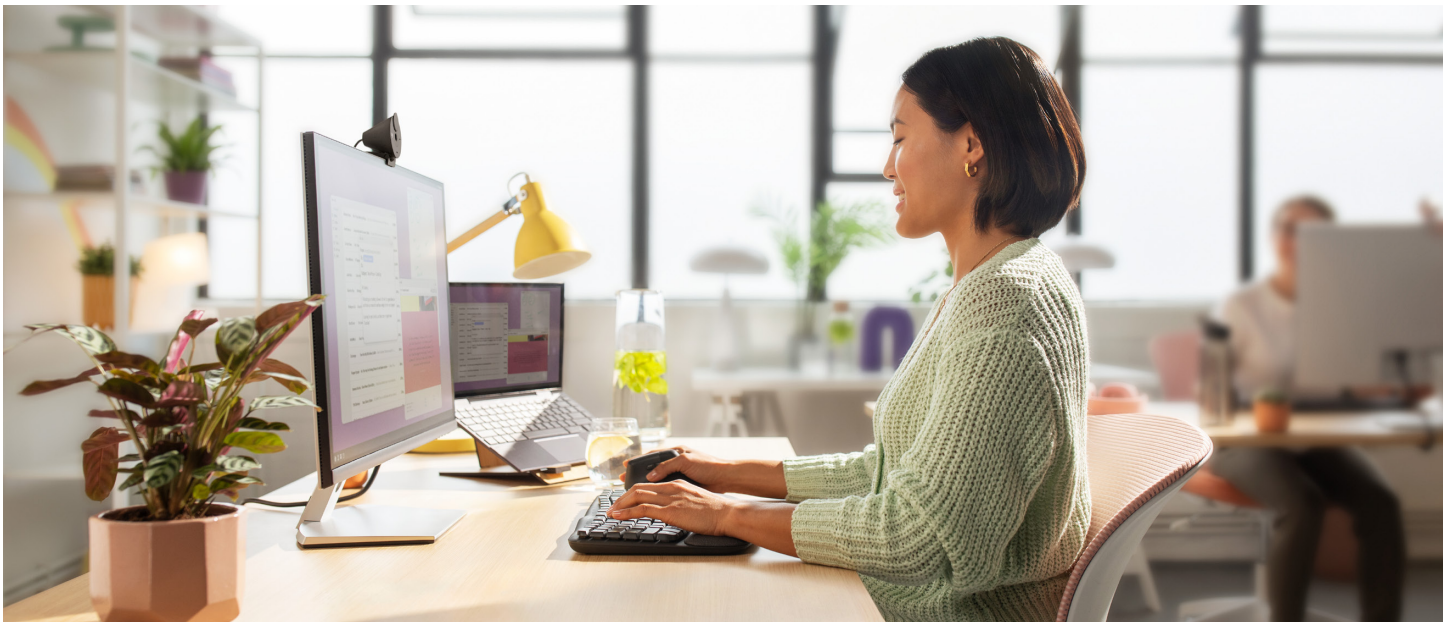
Device firmware updates can be remotely deployed via SCCM, InTune, or Jamf.

LOGITECH FLOW

Logi Options+ provides the feature called Flow which allows a user to use one mouse and keyboard to control multiple machines over a local area network (LAN). Learn More.

Data Privacy

Type of data collected	Purpose of data collection	Data Store
Operational Data • Host ID • OS version • Device model and firmware version • App version For the Logitech Flow feature, to enable automatic discovery of computers during the setup process of Flow, we may collect the user's device ID and IP address. The Flow feature can be disabled by administrators.	The number of computers along with their OS versions on which Options+ is installed enables us to scale server capacity. The device model and firmware version enables us to plan communication efforts in the event of a security event affecting a previous version. The app version enables Logitech to plan communication efforts in the event of a security event affecting a previous version. Logitech Flow data is collected for the purpose of automatic discovery of computers during setup.	AWS
Usage and Diagnostics Data • Host ID • Hashed IP address and location • Crash logs and error reports • Device information such as name, model, ID, and firmware version • System information such as OS type and OS version • Usage of devices, app, and features • Configuration of devices	Debug crashes and technical issues with the app allows us to fix those issues to improve the stability and performance of the product. This usage data provides insights into user behavior to enhance current products and features while shaping the direction of future product development. • Only collected from users who agree to share data. • Not tied to the user's email address. • Can be disabled by administrators.	AWS
User Feedback Users can share feedback about new feature ideas and feature improvements from the app. When they submit feedback, we collect. • Feedback type, title, description and attachments provided by the user • Email address and name (if the user is logged in via Logi ID) • OS version	User feedback helps us improve the current products and services and inform future product development.	UserVoice (3rd-party feedback collection tool) servers
Logi ID Account and Associated Information • Email address • Password • First name • Last name • Profile picture, if users choose to share • Device settings • Computer information like computer name, make, and model to help users identify computers for which device settings have been saved to the cloud. • If users agree to receive email notifications, we collect device models, firmware version, OS version, device configuration, and country/location for language and locale information.	Used for individual user authentication and account creation. Device settings will be saved and made available on any computer where the user logs in to the application. Some data will be used for Logitech email communications as outlined during the account creation process, only if users agree. Creating an account is not required. Can be disabled by administrators.	AWS



SERVICE AND CUSTOMER DATA ACCESS

Logitech contracts with Amazon Web Services 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 deploys or a user installs Logi Options+, all user and device data regularly collected is retained within the service until the customer decides to stop using the service. Administrators may disable analytics during deployment, users may also opt out in the application. In terms of device settings, data is saved in association only when a User ID is added to the application. Once the account has been marked as deleted, all associated customer data will be permanently deleted.

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. The company 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.

Logitech Inc.
3930 North First St
San Jose, CA 95134 USA
Published August 2023