



LOGI OPTIONS+

SECURITY & PRIVACY WHITEPAPER



Logi Options+ is the powerful, easy-to-use, next-gen application that enables customization for Logitech mice and keyboards. 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 range of personal workspace and collaboration tools that are easy to use. And we provide simple-to-use software to help you deploy Logitech peripherals to maximize the benefits to your end-users.

Logi Options+ is an integral part of our personal workspace solutions. 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, enabling/disabling analytics, enabling/disabling the Logitech Flow feature, enabling/disabling SSO and enabling/disabling automatic updates.

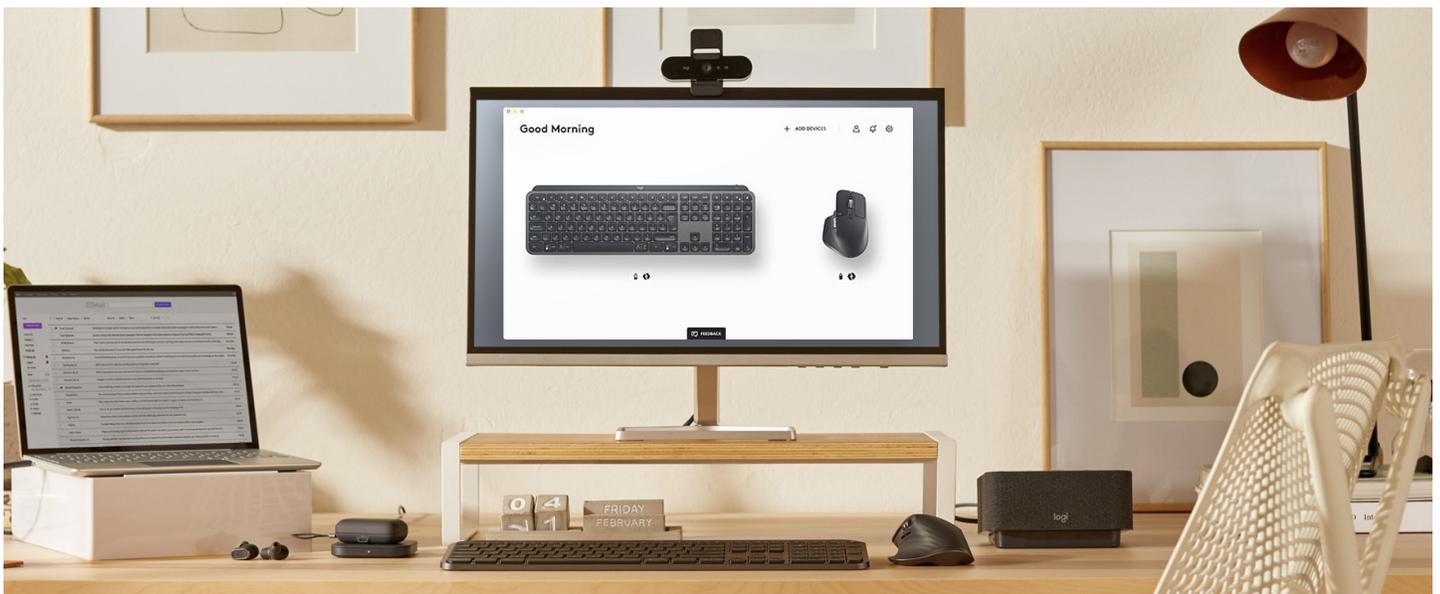
The Logi Options+ application ensures that end-users are provided with a best in class experience. For end-users, it allows device management and customization of Logitech devices for their specific workflow to increase individual

productivity. Options+ processes data and information from connected hardware devices.

Our vision for personal workspace software is to continually improve our hardware experience and provide more value over time. Options+ is the evolution of Logitech Options, our aim was to better support our enterprise customers by providing enhanced security and an improved user experience. Logitech will continue to invest in new Options+ features that drive real business outcomes in productivity.

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 the handling of personal data and the delivery of software updates. We use such data in a manner consistent with the [Logitech Privacy Policy](#).

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. 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 users the ability to sign into Options+ via Logi ID so they can back up their device settings to the cloud. Users can login with the same Logi ID they may be using for other Logitech applications and services. Administrators have the ability to 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 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.

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+ software 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](#).

Type of data collected	Purpose of data collection	Data Store
<p>Operational Data</p> <ul style="list-style-type: none"> • Host ID • OS version • Device model and firmware version • App version <p>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.</p>	<p>The number of computers along with their OS versions on which Options+ is installed enables us to scale server capacity.</p> <p>The device model and FW version enables us to plan communication efforts in the event of a security event affecting a previous version.</p> <p>The app version enables Logitech to plan communication efforts in the event of a security event affecting a previous version.</p> <p>Logitech Flow data is collected for the purpose of automatic discovery of computers during setup.</p>	<p>AWS</p>
<p>Usage and Diagnostics data</p> <ul style="list-style-type: none"> • 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 	<p>Debug crashes & technical issues with the app and fix those issues to improve the stability and performance of the product</p> <p>Understand how users use our products in order to help improve existing products & features, and inform future product development</p> <ul style="list-style-type: none"> - Only collected from users who agree to share data. - Not tied to the user's email address. - Can be disabled by administrators. 	<p>AWS</p>
<p>User Feedback</p> <p>Users can share feedback about new feature ideas and feature improvements from the app. When they submit feedback, we collect.</p> <ul style="list-style-type: none"> • 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 	<p>User feedback helps us improve the current products & services and inform future product development</p>	<p>UserVoice (3rd party feedback collection tool) servers</p>

Type of data collected	Purpose of data collection	Data Store
<p>Logi ID account and associated information</p> <ul style="list-style-type: none"> • 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 they agree to receive email notifications, we collect device models, firmware version, OS version, device configuration, and country/ location for language and locale information. 	<p>User authentication and account creation for individuals.</p> <p>Device settings will be saved and be made available on any computer where the user logs in to the application.</p> <p>Some data will be used for Logitech email communications as outlined during the account creation process only if users agree.</p> <p>Creating an account is not required.</p> <p>Can be disabled by administrators.</p>	<p>AWS</p>



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 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. 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](#).



Contact your reseller or contact us [here](#)

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

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.

©2022 Logitech, Inc. All rights reserved.

Published June 2022