

This document describes the data export functionality and compliance approach of LogMeIn Resolve under the EU Data Act. LogMeIn Resolve (part of the GoTo family of products) provides customers with options to export account and usage data for reporting and analysis, either via the API or the Admin Console.

LogMeIn Resolve API

Can you export data from LogMeIn Resolve using an API?

- Yes, LogMeIn Resolve maintains an API (<https://developer.goto.com/LogMeIn/Resolve>) that enables Customers to export tickets (cases), device inventory, user details, and actions and audit logs.

What data can be exported via the API?

The LogMeIn Resolve API allows Customers to programmatically access and export various data types related to their remote support sessions and device management. Common data types that can be exported via the API include:

Data Category	Description
Case / Session Data	Information about remote support sessions, including case/session ID, title, subject and description, status with full lifecycle timestamps (created, updated, closed and resolved), requester and end-user names, assigned technician and agent names and email addresses, session notes, tags, labels and custom fields, device associated with the session, and priority and SLA information.
Device Data	Information about managed endpoints and connected devices, including device ID, hostname, device status (online, offline, in-session), operating system name and version, last seen and last access timestamps, assigned users, device groups and tenant associations, device tags and labels, hardware attributes (CPU, RAM, BIOS serial number, system manufacturer, model and drives), installed software inventory, geolocation (city, country and continent), and security state data covering antivirus, firewall, endpoint protection and mobile device management.
Alerts	Alert records including alert ID, policy name, device name and platform, alert rule details such as type, priority and trigger conditions, triggered and acknowledged timestamps, and acknowledgement status including who acknowledged or reactivated the alert.

Data Category	Description
Helpdesk Ticket Data	Information about helpdesk incidents, including ticket ID, reference number, title, summary, description and resolution, full lifecycle timestamps (created, updated, closed and resolved), status, priority with SLA response time, category, assigned and requesting user details, followers, full conversation history with attachments, tags, custom fields, linked devices and parent and child ticket relationships.
User Data	User ID, name and account service key, available across services and filterable by user type.
Tenant Data	Tenant names, associated device groups with device counts, contact details per tenant (name, role, email and phone number), tenant notes, associated domains, and external system IDs.
Knowledge Base	Knowledge base documents including document ID, title, format, visibility settings, assigned labels, folder hierarchy, full document content and a complete per-document changelog showing who created or modified the document and when.
MDM	Information about managed devices enrolled via LogMeIn Resolve MDM, including device ID, name, model, manufacturer, category, and ownership type (purchased or leased) with ownership start and end dates, operating system name and version, enrollment status and management type (Android: work profile, fully managed device, or fully managed with work profile; iOS/macOS: supervised or unsupervised; Windows: full or light management), device status and last seen and last reported (check-in) timestamps, device location, security and compliance state (passcode, encryption status, jailbreak or root, iOS activation lock, and Windows secure boot, TPM and antivirus/firewall status), telephony and SIM data (phone number, IMEI, ICCID and IMSI, carrier and roaming) and mobile/Wi-Fi network usage, custom attributes and their values per device, assigned user details including ID, name, email, and tags, user-to-device identifier assignments (serial numbers, IMEIs, and UDIDs), deployed application inventory and deployment configuration, and device organization, location and category associations.

Consult the LogMeIn Resolve API documentation (<https://developer.goto.com/LogMeInResolve>) for details.

What Export Formats Are Available using the API?

The LogMeIn Resolve API provides data in the following formats:

- **JSON:** The response format is JSON. Some complex data (event logs, installed apps) require parsing of nested objects/arrays.
- **CSV:** You must convert JSON data to CSV or Excel locally or via script.

Limitations / Caveats:

- **Integration Variances:** The data available for reporting may change if the product is integrated with third-party platforms or tools.
- **Rate Limits:** API usage is subject to throttling or rate limits (typically a few hundred requests per hour).
- **Data Volume:** You must use pagination mechanisms to retrieve large datasets.
- **Bulk Export Limitations:** Bulk history exports may need to be processed in batches due to volume or system constraints.
- **Data Retention:** Data retention periods are configurable by administrators.
- **Access Rights:** You can only export data you are permitted to access, determined by your API key or account privileges.
- **Agent or Session-Dependent Data:** Access to certain data may require agent installation or an active session on the target device.
- **Sensitive Data:** Sensitive fields may be masked or redacted for privacy. Certain data may require elevated API rights to access.
- **Feature Availability:** Not all account levels support API export.

LogMeIn Resolve Admin Console Reports

Can you export data in LogMeIn Resolve using Console Reports?

Yes. LogMeIn Resolve provides multiple ways for administrators and users (with permissions) to export data from the console, specifically from reporting modules and session/case histories.

What Export Formats Are Available using Console Reports?

Reports from the LogMeIn Resolve Admin Console can be exported in the following formats: **CSV** (comma-separated or semicolon-separated), **XLSX** (Excel 2007+), **PNG** (for graph/widget views), and **PDF** (full-report export). Consult the current Administrator's Guide for format availability per report type.

What data can Customers export?

LogMeIn Resolve provides a wide variety of reports from the Admin Console. Consult <https://support.logmein.com/resolve/help/working-with-reports> for more information.

Limitations / Caveats:

- **Custom Fields:** Some complex custom fields or views may not be fully exported as shown in the UI.
- **Sensitive Data:** Sensitive fields (like password fields, private comments, or full command outputs) may be excluded/redacted for privacy/security.
- **Report Data Fields:** The specific fields may vary depending on product version, enabled modules, customizations, and user permissions.
- **Export Size and Frequency Limit:** Export size and frequency may be limited by subscription plan or system capacity.

What Data is Not Exportable

GoTo does not release information that is specific to the internal functioning of GoTo's data processing service, or data where the release would pose a risk of breach of trade secrets or may jeopardize the security of the Service. For example, GoTo does not release passwords or tokens.