

Rescue Plus AI Privacy & Security FAQ

TABLE OF CONTENTS

- [01 Security & Encryption](#)
 - [02 Data Privacy & Retention](#)
 - [03 Compliance](#)
 - [04 How the AI Works & What Data It Accesses](#)
 - [05 IT Configuration & Network Requirements](#)
 - [06 Opt-Out & Control](#)
-

Overview

At LogMeIn, privacy and security are foundational to how we design every AI feature. LogMeIn Rescue Plus AI is built on the principles of data minimization, least privilege access, transparency, and human control. This ensures your organization's data is protected at every step of a support session. Neither LogMeIn nor any of its AI sub-processors are permitted to use your data to train or fine-tune AI models.

Keeping data safe during AI-powered support sessions is a shared responsibility. LogMeIn is committed to minimizing the data we collect, applying safeguards throughout the AI workflow, and deleting all session data automatically when a session closes. Customers play an equally important role by training technicians to handle sensitive data appropriately and advising end users not to share personally identifiable or classified information during support sessions.

For a full overview of LogMeIn's AI security and privacy commitments, please review our [AI Trust Center](#) and AI Terms.

SECTION 1

Security & Encryption

Is data encrypted at rest and in transit?

Yes, on both counts. Rescue Plus AI uses a combination of cloud object storage and cloud database services from leading cloud infrastructure providers to handle session data. All data stored at rest is encrypted using industry-standard protocols. Cloud object storage is protected using AES-256 encryption, and all database storage is encrypted using dedicated key management services. LogMeIn regularly evaluates its infrastructure providers to continuously improve service performance, accuracy, security, and privacy.

All data transmitted to LogMeIn's AI infrastructure is encrypted in transit using HTTPS and TLS 1.2 or higher, protecting against interception at every point of transfer.

Customers who use the integration between LogMeIn Rescue and ServiceNow have the option to store AI-generated session summary data in the notes field of the ServiceNow ticket.

How does LogMeIn Rescue Plus AI protect against prompt injection attacks?

LogMeIn uses a layered, defense-in-depth approach to prevent prompt injection. This includes restrictive prompt engineering, a multi-layer content filtering system (Azure LLM Content Filter combined with AI Skill Chaining), and regular security reviews. This also includes regular third-party penetration testing, covering AI-specific injection attempts via chat history and screenshot input, the two most likely attack vectors in a remote support session context. Findings are remediated on a risk-prioritized basis according to documented internal timelines. Customers requiring specific details on testing frequency or remediation SLAs may request this information through a security questionnaire or under NDA.

How does LogMeIn handle adversarial attacks or attempts to manipulate AI outputs?

LogMeIn Rescue Plus AI uses enterprise-grade models from its cloud providers, which include their own built-in protections against adversarial manipulation. On top of those baseline protections, LogMeIn implements input and output validation to reject unexpected, irrelevant, or potentially malicious inputs before they reach the model.

What measures are in place to ensure the accuracy and reliability of AI outputs?

LogMeIn ensures accuracy and reliability through careful model selection against quality and performance criteria, prompt engineering, and multi-layer content filtering that helps detect and reduce inappropriate or inaccurate outputs. Evaluation is performed without retaining customer

data. Most importantly, the technician always has the final say on whether and how any AI-generated output is used. No AI action is taken without explicit human approval.

How does LogMeIn stay ahead of evolving security threats?

LogMeIn's organizational security controls include regular security awareness and training programs that are updated to address emerging AI-specific threats. Systems are instrumented with observability measures to detect new security issues quickly, and LogMeIn's modular architecture allows for rapid deployment of patches when vulnerabilities are identified. Usage patterns and logs are reviewed regularly to identify emerging risks or unintended outcomes.

SECTION 2

Data Privacy & Retention

What data does LogMeIn Rescue Plus AI collect during a support session?

LogMeIn Rescue Plus AI only accesses and processes data that the logged-in technician can already see. It inherits the technician's existing permissions and does not access anything beyond that scope. Depending on the session type, this may include:

- Chat messages between the technician and end user
- Screenshots captured during remote control or remote view
- End user device information (hardware specs, CPU/memory usage, running processes, and Windows event logs)
- Outputs from other AI features such as Device Analysis or Error Analysis

Note: The data available to AI varies by session type. For example, a Zero Download session only exposes chat messages and remote view content.

How long is session data stored?

Raw session data collected during a session is stored only for the duration of that session and is deleted when the session ends. A session is considered ended when it is removed from the support queue. If a session remains in the queue but is inactive for more than 24 hours, all collected data is automatically deleted and a session summary can no longer be generated.

Once a session summary has been generated, it becomes a permanent, reportable record stored within Rescue's session history. If your organization has an ITSM integration configured, such as ServiceNow, the summary is also automatically posted back to the corresponding ticket, creating a persistent and auditable support record.

Where is session data stored?

Session data is temporarily stored in secure cloud infrastructure for the duration of the active session only. Data is deleted as soon as the session ends and any session left inactive in the support queue is purged automatically after 24 hours. There is no open-ended retention window for raw session data. All AI data operations are processed across global data centers operated by LogMeIn's AI sub-processors, which are leading cloud infrastructure providers. Data is handled in accordance with the customer's chosen environment (Global or EU) and in full compliance with [LogMeIn's Terms of Service](#) and [AI Terms](#).

Does LogMeIn use our data to train AI models?

No. Neither LogMeIn nor any of its AI sub-processors are permitted to train or fine-tune AI models using customer data. This includes chat histories, device information, and screenshots captured during sessions. All data collected is used solely for the purpose of delivering AI features within that session and is then permanently deleted.

Will other customers ever have access to our data?

No. Customer data isolation begins at the account level. Each customer's sessions are logically segregated by account identifier in both the database and object storage, encrypted at rest, and processed exclusively within that account's own context. There are no shared indexes, and no cross-account queries exist at any stage of data processing. No data flows between customer environments under any circumstances.

Does LogMeIn anonymize data before sending it to third-party AI providers?

LogMeIn applies data minimization principles throughout the AI workflow. That means only the minimum data required to deliver the requested feature is ever collected or processed. Within the processing flow, PII is addressed through prompt-level guardrails that instruct AI models not to output sensitive information, and all temporary session data is automatically deleted when a session closes. Neither LogMeIn nor its AI sub-processors are permitted to use customer data to train or fine-tune AI models.

LogMeIn does not attempt to exhaustively classify every field as sensitive. Instead, we minimize the data processed, apply guardrails to prevent sensitive outputs, and delete all session data on close. Customers remain best placed to identify context-specific sensitive data and should guide technicians accordingly.

Compliance

Does LogMeIn Rescue Plus AI comply with GDPR?

Yes. All data collected and processed by LogMeIn Rescue Plus AI is handled in accordance with GDPR requirements. LogMeIn operates on the principle of data minimization, ensuring that only the minimum amount of data necessary to deliver AI functionality is collected and processed at any time.

Does LogMeIn support EU data residency?

Yes. LogMeIn maintains a fully separate EU deployment of its AI infrastructure, including all temporary data storage, hosted with leading cloud infrastructure providers. EU customers are served exclusively through dedicated EU endpoints:

- *.logmeinrescue.eu
- *.logmeinrescue-enterprise.eu

LogMeIn also uses Large Language Models hosted within the EU, ensuring complete isolation between EU and Global environments. No EU customer data is routed through Global infrastructure.

Does LogMeIn Rescue Plus AI comply with HIPAA?

LogMeIn Rescue Plus AI can support customers' HIPAA compliance obligations. HIPAA-regulated use requires a Business Associate Agreement (BAA) with LogMeIn. Depending on your organization's specific requirements, additional steps may also be needed. Please contact your LogMeIn Account Representative to ensure the appropriate agreements and configurations are in place for your account. Customers are responsible for determining whether their use of the product satisfies applicable HIPAA requirements.

Is LogMeIn Rescue Plus AI considered high-risk under the EU AI Act?

Not under its current design. LogMeIn Rescue Plus AI is a support-productivity tool that operates under technician control and does not make autonomous decisions about individuals, so it is not currently classified as high-risk under the EU AI Act. It is subject to the Act's transparency obligations, which LogMeIn supports by clearly labeling AI-generated output as such.

SECTION 4

How the AI Works & What Data It Accesses

Does the AI act independently during a support session?

Depending on your organization's configuration, LogMeIn Rescue Plus AI may perform certain tasks automatically, such as collecting and analyzing session data or generating a session summary. However, any action affecting a device or external system requires explicit technician approval.

What Large Language Models and cloud vendors does LogMeIn use?

LogMeIn Rescue Plus AI runs on enterprise-grade models hosted securely within LogMeIn's own cloud accounts. These are not public or consumer-facing AI services. Specific models and providers are listed in our [sub-processor documentation](#) and may be updated over time as technology evolves.

What data does the AI actually see during a session?

LogMeIn Rescue Plus AI inherits the technician's existing permissions and cannot access anything beyond what the technician can already see. The AI has no elevated privileges and no access to data outside of the active session. The data available to the AI depends on the session type but may include:

- Chat messages between the technician and end user
- Screenshots from remote control or remote view, analyzed visually in sequence by the AI
- End user device information including hardware specs, CPU/memory usage, running processes, and Windows event logs
- Outputs from other AI features such as Device Analysis, Error Analysis, recommendations or safety alerts
- Ticket context from integrated ITSM tools such as ServiceNow, where applicable

Can the AI access data from tabs in the system info panel that the technician has not opened?

No. The AI can only access data from system info tabs that the technician has actively clicked on during the session. If the technician has not viewed a particular tab, such as processes or drivers, the AI cannot see that data either. This is because viewing certain data requires explicit end user permission, which is only requested when the technician navigates to that tab.

Is AI output clearly identified as AI-generated?

Yes. LogMeIn is fully transparent about which content is AI-generated and marks all AI output as such within the Technician Console. Technicians always have the final say on whether and how any AI-generated output is used.

SECTION 5

IT Configuration & Network Requirements

Which URLs need to be allowlisted to use LogMeIn Rescue Plus AI?

The URLs that need to be allowlisted depend on your environment:

EU environment

- *.logmeinrescue.eu
- *.logmeinrescue-enterprise.eu

Global (US)

- *.logmeinrescue.com
- *.logmeinrescue-enterprise.com

For more information, visit our [allowlisting page](#) on the Rescue support site.

Will LogMeIn Rescue Plus AI work if our network blocks Google or Microsoft Azure URLs?

Yes. There is no direct connection to Google Gemini or Microsoft Azure OpenAI URLs from within the Rescue Technician Console. All AI traffic is routed through LogMeIn's own infrastructure, so existing firewall rules blocking third-party AI provider URLs will not affect the functionality of Rescue Plus AI features.

Does LogMeIn Rescue Plus AI require any changes to existing firewall or proxy configurations?

No. Beyond allowlisting for the environment-specific URLs listed above, no additional firewall or proxy configuration changes are required. All AI traffic is routed through LogMeIn's own infrastructure, so existing firewall rules blocking third-party AI provider URLs will not affect the functionality of Rescue Plus AI features.

Is any data transmitted directly from the end user's device to LogMeIn's AI infrastructure?

No. Data does not flow directly from the end user's device to any AI infrastructure. All data is routed exclusively through Rescue's own session infrastructure, which manages and brokers all

communication with AI providers. The end user's device has no direct connection to any AI service at any point during a session.

Does LogMeIn Rescue Plus AI require any special software installations or elevated permissions on the end user's device?

No. LogMeIn Rescue Plus AI requires no additional software installations or elevated permissions on the end user's device beyond the standard Rescue applet and requirements already in place for a support session. If your organization is already running LogMeIn Rescue, no additional device-level changes are needed to enable AI features.

Do AI features require a specific Technician Console version?

Yes. AI features require the Rescue desktop Technician Console version 7.55.4174 or later. Technicians on earlier versions will need to update their desktop Technician Console or use the Web Technician Console to access AI functionality.

SECTION 6

Opt-Out & Control

Are AI features mandatory when using LogMeIn Rescue?

No. LogMeIn Rescue Plus AI is an optional add-on and is not required to run standard Rescue support sessions. Customers have full control over which AI features are enabled and which technicians have access to them. AI features are designed to enhance technician productivity, but your organization decides if, when, and how they are used.

Can we disable AI features for specific technicians?

Yes. AI features that are part of the Rescue Plus AI add-on can be disabled on a per-technician basis by simply unassigning the AI license from that technician. Those technicians will immediately lose access to the AI features associated with that license, while the rest of your team remains unaffected.

Can we set limits on AI feature use for technician groups?

Yes. You can configure warning thresholds and maximum credit limits for the AI features on a per-session basis in the Admin Center. When a session reaches the warning threshold, technicians will be notified. When the maximum limit is reached, the AI feature will be disabled for that session.

Can we disable AI features at the account level?

Yes. AI features that are included with the Rescue base license can be disabled for your entire account through the Admin Center under Global Settings > AI Settings.

Does LogMeIn Rescue Plus AI make any decisions or take any actions without technician approval?

No. LogMeIn Rescue Plus AI is designed so that the technician always has the final say on whether and how any AI-generated output is used. While certain features, such as Session Summary, will automatically collect and analyze session data once activated, no output is posted to external systems or applied without the technician's explicit review and approval. The AI assists and informs, but the technician decides.

LogMeIn Rescue — Questions about your account? Contact your LogMeIn Account Representative.