



RESCUE AND RESCUE LENS

SECURITY AND PRIVACY OPERATIONAL CONTROLS

LogMeIn Rescue and Rescue Lens Security and Privacy Operational Controls

Publication Date: 02/04/2020

1 Products and Services

This document describes the security and privacy controls for LogMeIn Rescue and Rescue Lens. Rescue is a web-based remote support and customer care service used by helpdesk professionals to provide remote assistance via the Internet, without the need for pre-installed software. With the permission of the end user, Rescue allows a helpdesk professional to access and view and/or assume control of a user's computer. Communicating through a chat window, the technician can vet, diagnose and repair computer problems and otherwise assist a user with operating system and software application issues.

Rescue Lens allows customers to stream their mobile device cameras to a remote agent, allowing the remote agent to view problematic hardware such as a misconfigured router or a damaged automotive component. Rescue Lens is an optional feature within Rescue and can be activated in the Rescue Admin Center. For more details on Rescue Lens, please see the "Rescue Lens User Guide" [1].

2 Product Architecture

LogMeIn Rescue is a Software-as-a-Service (SaaS)-based remote support solution comprised of three main components: a technician console, a customer applet, and an administration center.

The technician console is the interface used by support technicians to conduct remote support sessions. Technicians can initiate new sessions or respond to online customer requests waiting in a shared queue. With the customer's permission, the Rescue applet – the interface through which technicians communicate with customers and conduct remote support – is downloaded to the user's remote PC. The applet is designed to remove itself from the remote PC when the session concludes. Administrators use the web-based administration center to create and assign permissions for other administrators, technicians, and technician groups.

The Rescue technician console interacts with the Rescue applet using a peer-to-peer network connection (see Figure 1). The peer-to-peer process is initiated when the applet is started. It connects to a Rescue gateway, where the session with the technician console is negotiated. For details on how the connection works and the security measures utilized, please refer to "Overview of the Rescue Gateway Hand-off process" section of the "Rescue Architecture and Security" whitepaper [2].

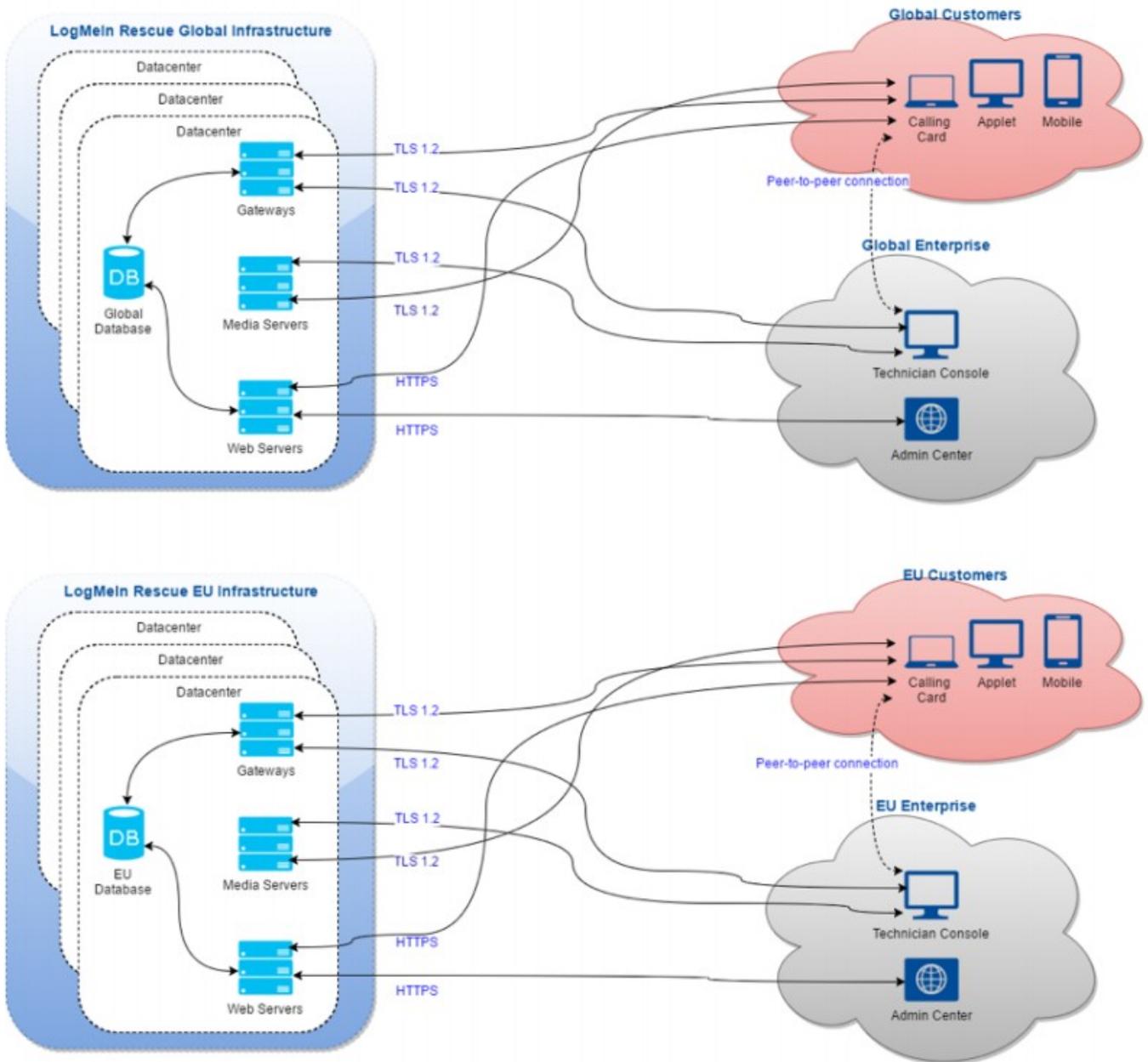


Figure 1- LogMeIn Rescue Global Infrastructure

3 Rescue Technical Security Controls

LogMeIn employs industry standard technical security controls appropriate to the nature and scope of the Services (as the term is defined in the Terms of Service [3]) in order to safeguard the Service infrastructure and data residing therein.

3.1 Logical Access Control

Logical access controls are in place, designed to prevent or mitigate the threat of unauthorized application access and data loss in corporate and production environments. Employees are granted minimum (or “least privilege”) access to specified LogMeIn systems, applications, networks, and devices as needed. Further, user privileges are segregated based on functional role and environment.

LogMeIn Rescue allows single sign-on (SSO) using Security Assertion Markup Language (SAML), and customers can customize access control. For example, Rescue administrators can configure password policy, force password resets, enforce two-factor authorization for Rescue logins, disable technician access, or restrict technician access to Rescue from IP addresses preapproved for specific tasks.

Rescue administrators can also grant or deny specific permissions in the Administration Center. These group permissions include:

- Allow clipboard synchronization
- Allow screen sharing with customers
- Deploy scripts
- Launch desktop viewing
- Launch file manager
- Launch remote control
- Reboot
- Record sessions
- Request Windows credentials
- Send and receive files
- Send URLs
- Start private sessions
- Transfer sessions
- Use single prompt for all permissions
- View system information

For more details on group permissions, please reference the LogMeIn Rescue Administrators Guide [4].

Rescue Lens support providers are identified by their email address and authenticated using a strong password.

3.2 Perimeter Defense and Intrusion Detection

The LogMeIn on-premise network architecture is segmented into public, private, and Integrated Lights-Out (iLO) management network zones. The public zone contains internet-facing servers, and all traffic that enters this network must transit a firewall. Only required network traffic is allowed; all other network traffic is denied, and no network access is permitted from the public zone to either the private or iLO management network zones.

The private network zone hosts application-level administrative and monitoring systems, and the iLO management network zone is for hardware and network administration and monitoring. Access to these networks is restricted to authorized employees via two-factor authentication.

Moreover, LogMeIn employs perimeter protection measures, including a third party, cloud-based, distributed denial of service (DDoS) prevention service, designed to prevent unauthorized network traffic from entering our product infrastructure.

3.3 Data Segregation

LogMeIn leverages a multi-tenant architecture, logically separated at the database level, based on a user's or organization's LogMeIn account. Only authenticated parties are granted access to relevant accounts.

3.4 Physical Security

Datacenter Physical Security

LogMeIn contracts with datacenters to provide physical security and environmental controls for server rooms that house production servers. These controls include:

- Video surveillance and recording
- Multi-factor authentication to highly sensitive areas
- Heating, ventilation, and air conditioning temperature control
- Fire suppression and smoke detectors
- Uninterruptible power supply (UPS)
- Raised floors or comprehensive cable management
- Continuous monitoring and alerting
- Protections against common natural and man-made disasters, as required by the geography and location of the relevant datacenter
- Scheduled maintenance and validation of all critical security and environmental controls

LogMeIn limits physical access to production datacenters to authorized individuals only. Access to an on-premise server room or third-party hosting facility requires the submission of a request through the relevant ticketing system and approval by the appropriate manager, as well as review and approval by Technical Operations.

LogMeIn management reviews physical access logs to datacenters and server rooms on at least a quarterly basis. Additionally, physical access to datacenters is removed upon termination of previously authorized personnel

3.5 Data Backup, Disaster Recovery, Availability

Rescue is designed to have near instantaneous fail-over capabilities for most failure scenarios. The production datacenters utilize redundant high-speed network connections. There are pools of web and gateway servers across geographically distant datacenters. Load balancers distribute network traffic and maintain the availability of these servers in the event of server or datacenter failures.

The Rescue database is synchronized every five minutes to another datacenter. In addition, a differential back-up is completed nightly, and full backups are conducted every weekend. The backup database is stored with the same encryption as the original. Backups are retained on premise for one month and then rotated to a cloud service, no longer actively processed, and retained pursuant to our internal record retention policies. In the event of a complete failure of the datacenter hosting the primary database, Rescue architecture is designed to be restored within five minutes.

3.6 Malware Protection

Malware protection software with audit logging is deployed on all Rescue servers. Alerts indicating potential malicious activity are sent to an appropriate response team.

3.7 Encryption

LogMeIn maintains a cryptographic standard that aligns with recommendations from industry groups, government publications, and other reputable standards groups. The cryptographic standard is periodically reviewed, and selected technologies and ciphers may be updated in accordance with the assessed risk and market acceptance of new standards.

In-Transit Encryption

All network traffic flowing in and out of LogMeIn datacenters, including all Customer Content, is encrypted in transit. In addition, Rescue support sessions are protected with end-to-end 256-bit AES encryption.

At-Rest Encryption

Rescue chat logs and custom fields, which are fields created by the customer, are encrypted at rest with 256-bit AES encryption.

3.8 Vulnerability Management

Internal and external system and network vulnerability scanning is conducted monthly. Dynamic and static application vulnerability testing, as well as penetration testing activities for targeted environments, are also performed periodically. These scanning and testing results are reported into network monitoring tools and, where appropriate and predicated on the criticality of any identified vulnerabilities, remediation action is taken.

Vulnerabilities are also communicated and managed with monthly and quarterly reports provided to development teams, as well as management.

3.9 Logging and Alerting

LogMeIn collects identified anomalous or suspicious traffic into relevant security logs in applicable production systems.

4 Organizational Controls

LogMeIn maintains a comprehensive set of organizational and administrative controls to protect the security and privacy posture of Rescue.

4.1 Security Policies and Procedures

LogMeIn maintains a comprehensive set of security policies and procedures aligned with business goals, compliance programs, and overall corporate governance. These policies and procedures are periodically reviewed and updated as necessary to ensure ongoing compliance.

4.2 Standards Compliance

As a public company, LogMeIn complies with applicable legal, financial, data privacy, and regulatory requirements, and conforms with the following compliance certifications and external audit reports:

- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Type 2 attestation report
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS) compliance for LogMeIn's eCommerce and payment environments
- TRUSTe Enterprise Privacy Certification

4.3 Security Operations and Incident Management

LogMeIn's Security Operations Center (SOC) is staffed by the Security Operations team and is responsible for detecting and responding to security events. The SOC uses security sensors and analysis systems to identify potential issues and has developed an Incident Response Plan that dictates appropriate responses.

The Incident Response Plan is aligned with LogMeIn's critical communication processes, the Information Security Incident Management Policy, as well as associated standard operating procedures. It is designed to manage, identify and resolve suspected or identified security events across its systems and Services, including Rescue. Per the Incident Response Plan, technical personnel are in place to identify potential information security-related events and vulnerabilities and to escalate any suspected or confirmed events to management when appropriate. Employees can report security incidents via email, phone and/or ticket, according to the process documented on the LogMeIn intranet site. All identified or suspected

events are documented and escalated via standardized event tickets and triaged based upon criticality.

4.4 Application Security

LogMeIn's application security program is based on the Microsoft Security Development Lifecycle (SDL) to secure product code. The core elements of this program are manual code reviews, threat modeling, static code analysis, dynamic analysis, and system hardening.

4.5 Personnel Security

Background checks, to the extent permitted by applicable law and as appropriate for the position, are performed globally on new employees prior to the date of hire. Results are maintained within an employee's job record. Background check criteria will vary depending upon the laws, job responsibility and leadership level of the potential employee and are subject to the common and acceptable practices of the applicable country.

4.6 Security Awareness and Training Programs

New hires are informed of security policies and the LogMeIn Code of Conduct and Business Ethics at orientation. This mandatory annual security and privacy training is provided to relevant personnel and managed by Talent Development with support from the Security Team.

LogMeIn employees and temporary workers are informed regularly about security and privacy guidelines, procedures, policies and standards through various mediums including new hire

on-boarding kits, awareness campaigns, webinars with the CISO, a security champion program, and the display of posters and other collateral, rotated at least bi-annually, that illustrate methods for securing data, devices, and facilities.

5 Privacy Practices

LogMeIn takes the privacy of its Customers and end users very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

5.1 Privacy Policy

LogMeIn discloses the types of information it collects and uses to provide, maintain, enhance, and secure its Services in its Privacy Policy on our public website [5]. The company may, from time to time, update the Privacy Policy to reflect changes to its information practices and/or changes in applicable law, but will provide notice on its website for any material changes prior to any such change taking effect.

5.2 GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law on data

protection and privacy for individuals within the European Union. GDPR aims primarily to give control to its citizens and residents over their personal data and to simplify the regulatory environment across the EU. The Service is compliant with the applicable provisions of the GDPR. For more information, please visit www.logmeininc.com/trust.

5.3 CCPA

LogMeIn hereby represents and warrants that it will be in compliance with the California Consumer Privacy Act (CCPA) and will implement and maintain the necessary controls to adhere to the applicable provisions of CCPA no later than January 1, 2020. For more information, please visit www.logmeininc.com/trust.

5.4 EU-U.S. and Swiss Privacy Shield

LogMeIn, Inc. and its US affiliates participate in the EU-U.S. Privacy Shield Framework and Swiss Privacy Shield regarding the collection, use and retention of personal information from European Union member countries and Switzerland [6]. Certification is reviewed annually by TRUSTe and any findings are promptly addressed by LogMeIn.

5.5 Return and Deletion of Customer Content

At any time, Customers may request the return or deletion of their Content through standardized interfaces. If these interfaces are not available or LogMeIn is otherwise unable to complete the request, LogMeIn will make a commercially reasonable effort to support the Customer, subject to technical feasibility, in the retrieval or deletion of their Content. Customer Content will be deleted within thirty (30) days of Customer request.

Customer's Rescue Content shall automatically be deleted within ninety (90) days after the expiration or termination of their final subscription term. Upon written request, LogMeIn will certify to such Content deletion.

5.6 Sensitive Data

While LogMeIn aims to protect all Customer Content, regulatory and contractual limitations require us to restrict the use of Rescue for certain types of information. Unless Customer has written permission from LogMeIn, the following data must not be uploaded or generated to Rescue:

- Government issued identification numbers and images of identification documents.
- Information related to an individual's health, including – but not limited to – Personal Health Information (PHI) identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA) and related laws and regulations.
- Information related to financial accounts and payment instruments, including – but not limited to – credit card data. The only general exception to this provision extends to explicitly identified payment forms and pages that are used by LogMeIn to collect payment for Rescue.
- Any information especially protected by applicable laws and regulation, specifically

information about individual's race, ethnicity, religious or political beliefs, organizational memberships, etc.

5.7 Tracking and Analytics

LogMeIn is continuously improving its websites and products using various third-party web analytics tools, which help LogMeIn understand how visitors use its websites, desktop tools, and mobile applications, what they like and dislike, and where they may have problems. For further details please reference our Privacy Policy [5].

6 Third Parties

6.1 Use of Third Parties

As part of the internal assessment and processes related to vendors and third parties, vendor evaluations may be performed by multiple teams depending upon relevancy and applicability. The Security team evaluates vendors that provide information security-based services including the evaluation of third-party hosting facilities. Legal and Procurement may evaluate contracts, Statements of Work (SOW) and service agreements, as necessary per internal processes.

Appropriate compliance documentation or reports may be obtained and evaluated at least annually, as deemed appropriate, to ensure the control environment is functioning adequately and any necessary user consideration controls are addressed. In addition, third parties that host or that are granted access to sensitive or confidential data by LogMeIn are required to sign a written contract outlining the relevant requirements for access to, or storage or handling of, the information (as applicable).

6.2 Contract Practices

To ensure business continuity and that appropriate measures are in place to protect the confidentiality and integrity of third-party business processes and data processing, LogMeIn reviews relevant third party's terms and conditions and either utilizes LogMeIn-approved procurement templates or negotiates such third-party terms, where deemed necessary.

7 Contacting LogMeIn

Customers can contact LogMeIn at <https://support.logmeininc.com/> for general inquiries or privacy@logmein.com for privacy-related questions.

8 References

- [1] LogMeIn, Inc., "LogMeIn Rescue Lens," [Online]. Available: https://secure.logmeinrescue.com/welcome/documents/pdfs/Rescue_Lens_Userguide.pdf. [Accessed 2 April 2018].
- [2] LogMeIn, Inc, "Rescue Architecture and Security Overview Brochure," 2018. [Online]. Available: https://secure.logmeinrescue.com/welcome/documents/pdfs/rescue_architecture.pdf.

[Accessed February 2018].

- [3] LogMeIn, Inc., "Terms of Service for LogMeIn and Goto Services," LogMeIn, Inc., June 2019. [Online]. Available: <https://www.logmeininc.com/legal/terms-and-conditions>.
- [4] LogMeIn, Inc., "LogMeIn Rescue Administrators Guide," [Online]. Available: https://secure.logmeinrescue.com/welcome/documents/pdfs/rescue_admin_center_use_guide.pdf. [Accessed 2 April 2018].
- [5] LogMeIn, Inc., "LogMeIn Privacy Policy," LogMeIn, Inc., January 2018. [Online]. Available: <https://secure.logmein.com/policies/privacy.aspx>.
- [6] LogMeIn, Inc., "LogMeIn EU-U.S. Privacy Shield Notice," LogMeIn, Inc., September 2019. [Online]. Available: <https://www.logmeininc.com/legal/privacy-shield>.