RESCUEASSIST BY LOGMEIN
Security and Privacy Operational Controls

Publication Date: 04/11/19

V1

March 05, 2019

1 Products and Services

This document focuses on the privacy and security aspects of the RescueAssist infrastructure and communications channels.

RescueAssist enables IT and support professionals to deliver remote support to computers, servers and mobile devices with remote view, remote control or camera share from a web-based agent console.

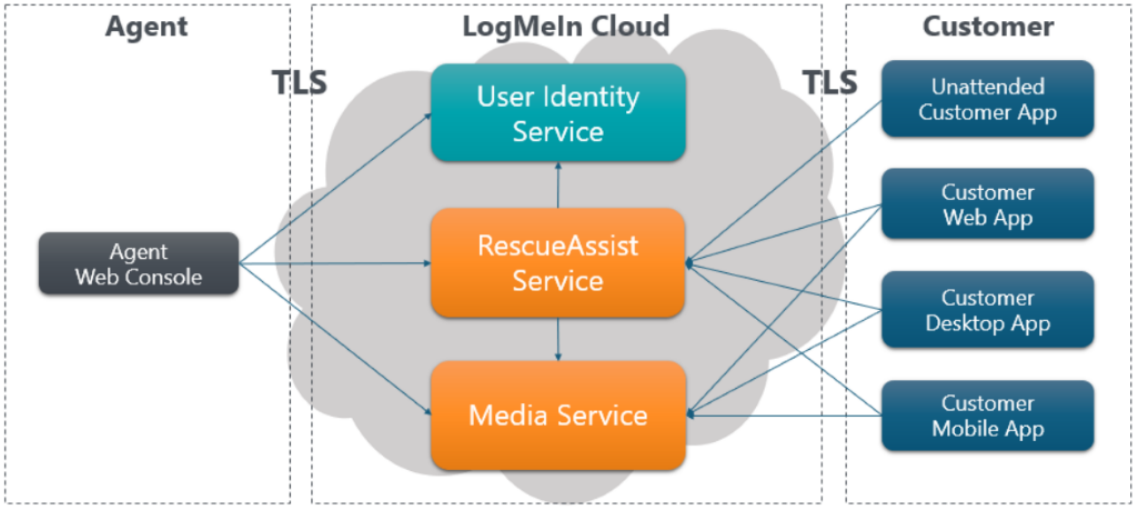
RescueAssist employs robust data security measures in order to defend against both passive and active attacks.

2 Product Architecture

RescueAssist uses an application service provider (ASP) model designed to provide secure operations while integrating with a company's existing network and security infrastructure. Its architecture is designed for optimal performance, reliability and scalability. Redundant switches and routers are built into the architecture and intended to ensure that there is no single point of failure. High-capacity, clustered servers and backup systems are utilized in order to ensure continued operation of application processes in the event of a heavy load or system failure. Service brokers load balance the client/server sessions across geographically distributed communication servers. The communications architecture for RescueAssist is depicted in Section 2.1 below.

2.1 Communications Architecture

The RescueAssist communications architecture is summarized in the figure below.



Agent authentication utilizes the LogMeIn User Identity Service. Communication between participants in a RescueAssist Session occurs via an overlay networking stack that logically sits on top of the conventional UDP and TCP/IP. This network is provided by LogMeIn's RescueAssist Service and Media Service hosted in Amazon AWS.

RescueAssist Session participants (Agent Web Console and Customer Endpoints) communicate with RescueAssist Service and Media Service using outbound TCP connections on port 443 or UDP port 15000, depending on availability. Because RescueAssist is a web-based service, participants can be located nearly anywhere on the Internet — at a remote office, at home, at a business center or connected to another company's network.

3 RescueAssist Technical Controls

LogMeIn employs industry standard technical controls appropriate to the nature and scope of the Services (as the term is defined in the Terms of Service [1]) designed to safeguard the Service infrastructure and Customer Content residing therein.

3.1 Authentication

RescueAssist Agents and Account Administrators are identified by their email address and authenticated using a password. During authorized authentication, the password is never transferred in an unencrypted state.

Authentication procedures are governed by the following policies:

Strong passwords: A strong password must be a minimum of 8 characters in length with sufficient complexity requirements (i.e., must contain both letters and numbers). Passwords are checked for strength when established or changed.

Two-Factor Authentication: As an additional security measure, optional two-factor authentication is available for every RescueAssist company account. If enabled, two-factor authentication requires every user to authorize access via two separate methods.

Account lockout: After five consecutive failed log-in attempts, the user account is put into a mandatory soft-lockout state. This means that the user account holder will not be able to log-in for five minutes. After the lockout period expires, the user account holder will be able to attempt to log-in to his or her account again.

3.2 Logical Access Control

Logical access control procedures are in place, designed to prevent or mitigate the threats 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.

Users authorized to access LogMeIn RescueAssist product components may include LogMeIn's authorized technical staff (e.g., Technical Operations and Engineering DevOps), customer administrators, or end-users of the product. On-premise production servers are only available from jump hosts or through the Operations virtual private network (VPN). Cloud-based production components are available through SSU (Self Service Unix) authentication.

3.3 Permission Based Access Control

3.3.1 Attended Session

An essential part of RescueAssist's security is its permission-based access control model designed to protect access to the Customer's computer and data. During customer-attended live support sessions, the customer is prompted for permission before initiation of any screen sharing, remote control or transfer of files.

Once remote control and screen sharing have been authorized during an Attended Session, the Customer can watch what the Agent does at all times. Further, the service is designed to permit the Customer to easily take control back or terminate the session at any time.

3.3.2 Unattended Session

Unattended support requires the Unattended Customer App to be installed on the Customer's device. It can be set up in one of two ways — either In-Session Setup (during an Attended Session) or using an Out-of-Session Installer, both of which require Customer approval.

In-Session Setup: once the Customer and Agent have entered an Attended Session, the Agent may request extra permission to install the Unattended Customer App. The Customer is prompted for approval and must give explicit authorization.

Out-of-Session Installer: After securely logging in to the RescueAssist website, the Agent can download an installer, which allows installation of the Unattended Customer App on any Windows PC or Mac for which the Agent has administrator access.

3.3.3 In-Session Security

RescueAssist is not designed to override local security controls on the Customer's computer. Specifically, if the Customer returns to the machine while an Unattended Session is in progress, they may, at any time, end the session and can permanently revoke the Agent 's unattended support privileges.

3.4 Role Based Access Control

RescueAssist provides access to a variety of resources and services using a role-based access control system that is enforced by the various service delivery components. The following roles are defined:

Account Administrator: RescueAssist user with full admin privileges to perform administrative functions pertaining to Agents. Account administrators can create, modify and delete Agent accounts and modify subscription data.

Agent: RescueAssist user, able to initiate RescueAssist Sessions in order to provide technical assistance to Customers via remote view, remote control or camera share.

Customer: Unauthenticated person requesting support from the Agent. The Customer can close sessions and must grant permissions for the Agent to access his/her device.

3.5 Perimeter Defense and Intrusion Detection

LogMeIn employs industry standard perimeter protection tools, techniques and services that are designed to prevent unauthorized network traffic from entering its product infrastructure. The LogMeIn network features externally facing firewalls and internal network segmentation. Cloud resources also utilize host-based firewalls.

3.6 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

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 data center
- Scheduled maintenance and validation of all critical security and environmental controls

LogMeIn limits physical access to production datacenters to only authorized individuals. 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

LogMeIn's architecture is designed to perform replication in near-real-time to geographically diverse locations. Databases are backed up using a rolling incremental backup strategy. In the event of a disaster or total site failure in any one of the multiple active locations, the remaining locations are designed to balance the application load. Disaster recovery related to these systems is tested periodically.

3.6 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.

Key points regarding encryption in RescueAssist include:

- RescueAssist session data is protected with TLS 1.2 (if supported) 256-bit AES encryption in transit.
- Session keys are generated server-side by the agent and remain there in order to be able to connect the customer to the agent. The service is designed to ensure that these keys are never exposed or visible to the public.
- Encrypted communication between the customer and the agent in RescueAssist occurs via the Jitsi WebRTC stack.
- Endpoints within the RescueAssist infrastructure use Transport Layer Security (TLS) connections.

3.6.1 In-Transit Encryption

To further safeguard Customer Content (as the term is defined in the Terms of Service [1]) while in transit, LogMeIn uses current TLS protocols and associated cipher suites.

Customer Endpoint and backend communication are encrypted via OpenSSL. Communications security controls based on strong cryptography are implemented on the TCP layer via TLS standard solutions.

Strong authentication measures are utilized in order to help reduce the likelihood of would-be attackers masquerading as infrastructure servers or inserting themselves into the middle of support session communications.

To provide protection against eavesdropping, modification or replay attacks, IETF-standard TLS protocols are used to protect all communication between endpoints and our services. Screen-sharing data, keyboard/mouse control data, transferred files, remote diagnostic data and text chat information are encrypted in transit with TLS 1.2 (2048-bit RSA, AES-256 strong encryption ciphers with 384-bit SHA-2 algorithm).

In order to ensure appropriate compatibility and security balance, the RescueAssist service also supports inbound connections using most supported TLS cipher suites in TLS 1.0, 1.1 and 1.2.

LogMeIn also advises that agents configure their browsers to use strong cryptography by default whenever possible, in order to increase technical safeguards on the agents machine, and to always install the latest operating system and browser security patches.

When connections are established to the RescueAssist website and between RescueAssist components, LogMeIn servers authenticate themselves to clients using GlobalSign public key

certificates. Server-to-server APIs are accessible only within LogMeIn's private network behind robust firewalls.

3.6.2 TCP layer security

Internet Engineering Task Force (IETF)-standard TLS protocols are used in order to protect communication between end-points.

For their own protection, LogMeIn recommends that customers configure their browsers to use strong cryptography by default whenever possible, and to ensure that operating system and browser security patches are kept up-to-date.

3.6.3 Customer Endpoint Protection

Customer Desktop Apps and Unattended Customer Apps must be compatible with a wide variety of desktop environments. RescueAssist accomplishes this using an executable download that employs strong cryptographic measures.

The Customer Desktop Apps and Unattended Customer Apps are downloaded to customer PCs as a digitally signed installer. This helps protect the Customer from inadvertently installing a Trojan or other malware posing as RescueAssist software.

The endpoint softwares are composed of several digitally signed executables and dynamically linked libraries. LogMeIn follows appropriate quality control and configuration management procedures during development and deployment in order to enhance software safety.

3.7 Vulnerability Management

Ensuring the safety and protection of LogMeIn's customer's Content and systems is top priority. LogMeIn implements various security measures throughout the lifecycle of all its products. Security aspects are considered and taken into account during development and operations of RescueAssist.

Dynamic and static application vulnerability testing, as well as Security assessment testing activities for targeted environments, are also performed periodically. Relevant vulnerabilities are also communicated and managed with monthly and quarterly reports provided to development teams, as well as management.

3.7.1 Security Team

LogMeIn's Security team continuously monitors product development and operations in close collaboration with the product engineers in order to keep RescueAssist secure and prevent or reduce the liklihood for possible risks.

3.7.2 Internal and External Audits

LogMeIn's internal audit process includes regular security assessments at both the infrastructure and software level. Our internal audits are complemented by various independent external assessments to ensure that we maintain industry standards.

3.8 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 in order to protect the security and privacy posture of the RescueAssist product.

4.6 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.

4.7 Standards Compliance

As a public company, LogMeIn complies with applicable legal, financial, data privacy, and regulatory requirements, and conforms with the following compliance certification(s) and external audit report(s):

- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Type 2 and SOC3 attestation report for GoToAssist
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI-DSS) compliance for LogMeIn's eCommerce and payment environments
- TRUSTe Verified Privacy Certification

4.8 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 RescueAssist. 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, where appropriate. Employees can report security incidents via email, phone and/or ticket in accordance with 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.

4.9 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, and system hardening.

4.10 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.

4.11 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 [2]. 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. RescueAssist is compliant with the applicable provisions of GDPR. For more information, please visit www.logmeininc.com/gdpr.

5.3 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 [3].

5.4 Return and Deletion of Customer Content

At any time, RescueAssist 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 for RescueAssist will be deleted within thirty (30) days of Customer request. Customers' RescueAssist 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.

5.5 Sensitive Data

While LogMeIn aims to protect all Customer Content, regulatory and contractual limitations require us to restrict the use of the RescueAssist for certain types of information. Unless Customer has written permission from LogMeIn, the following data must not be uploaded to or generated in RescueAssist (by Customer or their end-users):

- 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 Health Insurance Portability and Accountability Act of 1996 (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 RescueAssist.
- Any information especially protected by applicable laws and regulation, specifically information about individual's race, ethnicity, religious or political beliefs, organizational memberships, etc.

5.6 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 [2].

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 relevant vendors that provide information security-based services including the evaluation of third-party hosting facilities. LogMeIn's Legal and Procurement

teams 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, intended to protect the confidentiality and integrity of third-party business processes and data processing, LogMeIn reviews relevant third parties' terms and conditions and either utilizes LogMeIn-approved procurement templates or negotiates, in collaboration with Security, Legal, Procurement, and Finance (in each case, as appropriate) 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., "Terms of Service for LogMeIn and GoTo Services," LogMeIn, Inc., February 2018. [Online]. Available: https://www.logmeininc.com/legal/terms-and-conditions.

[2] LogMeIn, Inc, "LogMeIn Privacy Policy," [Online]. Available: https://secure.logmein.com/policies/privacy.aspx. [Accessed 2 April 2018].

[3] LogMeIn, Inc., "LogMeIn EU-U.S. Privacy Shield Notice," LogMeIn, Inc., November 2017. [Online]. Available: https://www.logmeininc.com/legal/privacy-shield.

9. Appendix – Terminology

Agent: RescueAssist user, who creates RescueAssist Sessions in order to provide technical assistance to Customers via remote view, remote control or camera share.

Agent Web Console: web application that runs on the Agent's PC, Mac, Tablet or Chromebook devices in any of the supported browsers (Chrome, Firefox, Safari) and connects to the RescueAssist Service. It enables the Agent to create and conduct RescueAssist sessions as well as various account management, service management and reporting functions.

Attended Session: support session where the Customer is present during the session and can participate in it.

Customer: person receiving technical support from the Agent via a RescueAssist Session.

Customer Desktop App: desktop application that runs on the Customer's computer (Windows or Mac) and connects to a RescueAssist Session through the RescueAssist Service. It provides remote control capability as well as other advanced functionalities and the ability to install Unattended App on the Customer's computer.

Customer Endpoint: collective term referring to any customer endpoint: Customer Web App, Customer Desktop App, Customer Mobile App, Unattended Customer App.

Customer Mobile App: mobile application (Android and iOS) that runs on the Customer's mobile/tablet device and can connect to a RescueAssist Session through the RescueAssist Service. It provides remote view (Android and iOS) and remote control (Android only) capabilities.

Customer Web App: web application that runs in any supported browser on the Customer's computer/mobile device and connects to a RescueAssist Session through the RescueAssist Service. It can provide chat, remote view and camera share capabilities as well as the possibility to elevate the session anytime to remote control by downloading the Customer Desktop App or installing the Customer Mobile App.

Media Service: a fleet of load-balanced, globally distributed servers providing a variety of high-availability unicast and multicast communication services based on WebRTC protocols.

RescueAssist Sessions: attended chat, remote view, remote control or camera share and unattended remote control.

RescueAssist Service: a fleet of load-balanced, globally distributed servers providing secure access for the Agent Web Console and Customer Endpoints through encrypted web-socket connection and API calls.

Unattended Customer App: installable desktop application (Windows and Mac) that runs in the background on the Customer's computer. It can download and execute a Customer Desktop App to connect to an authorized Unattended Session.

Unattended Session: support session where the Customer is not present. The session is initiated and established by the Agent without Customer involvement through an authorized Unattended Customer App.