Technical and Organizational Measures
Rescue Live Lens

Executive Summary

This Technical and Organizational Measures (TOMs) document outlines GoTo's commitments to privacy, security, and accountability for Rescue Live Lens. GoTo upholds comprehensive global privacy and security programs, along with organizational, administrative, and technical safeguards designed to:

- Ensure the confidentiality, integrity, and availability of Customer Content.
- Protect against threats and hazards to the security of Customer Content.
- Prevent any loss, misuse, unauthorized access, disclosure, alteration, and destruction of Customer Content.
- Maintain compliance with applicable laws and regulations, including data protection and privacy laws.

These measures include:

- **Encryption**:
  - *In-Transit* - Transport Layer Security (TLS) v1.2 or higher.
  - *At Rest* - Advanced Encryption Standard (AES) 256-bit for Customer Content.
- **Cloud-Provider Regions:**[1] United States, Germany, Singapore to support redundancy.
- **Compliance Audits:** SOC 2 / SOC 3 Type II, BSI C5, PCI DSS, PCAOB, TRUSTe Enterprise Privacy and APEC CBPR and PRP certifications, Internal controls assessment as required under a PCAOB annual financial statements audit.
- **Legal/Regulatory Compliance:** GoTo maintains a comprehensive data protection program with processes and policies designed to ensure Customer Content is handled in accordance with applicable privacy laws, including the GDPR, CCPA and LGPD.
- **Penetration Testing:** In addition to in-house testing, GoTo contracts with external firms to conduct regular security assessments and/or penetration testing.
- **Logical Access Controls:** Logical access controls are implemented and designed to prevent or mitigate the threat of unauthorized application access and data loss in corporate and production environments.
- **Data Segregation**: GoTo employes a multi-tenant architecture and logically separates Customer accounts at the database level.
- **Perimeter Defense and Intrusion Detection**: Perimeter protection tools, techniques and services are designed to prevent unauthorized network traffic from entering its product infrastructure. The GoTo network features externally facing firewalls and internal network segmentation.
- **Retention**:
  - Rescue Live Lens Customers may request the return or deletion of Customer Content at any time, which will be fulfilled within thirty (30) days of Customer's request.
  - Customer Content will automatically be deleted: (a) ninety (90) days after expiration of a Customer's then-final paid subscription term; or (b) for free accounts, after one

[1] Hosting locations may vary (i.e., depending on data residency election), consult the applicable Rescue Live Lens Sub-Processor Disclosure found in the Product Resources section of the GoTo Trust and Privacy Center (https:/www.goto.com/company/trust/resource-center).

(1) year of inactivity (e.g., no logins). Recordings are deleted on a rolling basis after ninety (90) days.

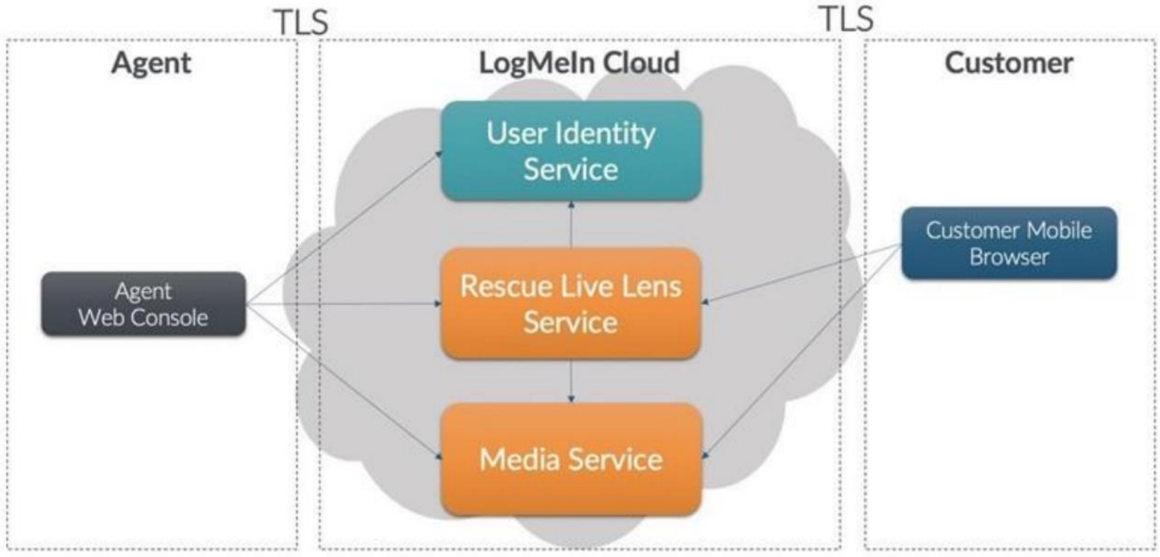
Contents

1 Product Introduction

This document covers the Technical and Organizational Measures (TOMs) for **Rescue Live Lens** infrastructure and communications channels. Rescue Live Lens enables IT and support agents to deliver audiovisual remote support to mobile devices with camera share from a web-based agent console. Rescue Live Lens employs robust data security measures to defend against both passive and active attacks.

2 Product Architecture

Rescue Live Lens 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 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 Rescue Live Lens is depicted below.



2.1 Communications Architecture

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

Rescue Live Lens Session participants (Agent Web Console and Customer Mobile Browser) communicate with Rescue Live Lens and Media Service using outbound TCP connections on port 443 or UDP port 3489,15000, depending on availability. Because Rescue Live Lens 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 Technical Security Controls

GoTo 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) designed to safeguard the Service infrastructure and data residing therein.

3.1 Authentication

Rescue Live Lens Agents and Account Administrators are identified by their email address and authenticated using a password. During authorized authentication, the password is not transmitted by GoTo in an unencrypted state.

Authentication procedures are governed by the following policies:

Strong passwords: A strong password must be a minimum of eight (8) characters in length with appropriate 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 Rescue Live Lens technician group 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 Permission Based Access Control

Camera Share Session - An essential part of Rescue Live Lens security is its permission-based access control model designed to protect access to the Customer's camera and microphone. During Live Lens support sessions, the Customer is prompted for permission before initiation of any access to their camera or microphone.

3.3 Authentication

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

- **Account Administrator:** Rescue Live Lens 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:** Rescue Live Lens user. The agent is able to initiate Live Lens Sessions in order to provide assistance to Customers via 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.

3.4. Encryption

GoTo maintains a cryptographic standard that aligns with recommendations from industry groups, government publications, and other relevant 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 Rescue Live Lens include:

- Rescue Live Lens session data is protected with up to Transport Layer Security (TLS) 1.2 (if supported) 256-bit AES encryption in transit.
- Session keys are generated server-side by the Agent and remain there 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 Rescue Live Lens occurs via the Media Service.
- Endpoints within the Rescue Live Lens infrastructure use TLS connections.

3.4.1. In-Transit Encryption

To further safeguard Customer Content (as the term is defined in the Terms of Service) while in transit, GoTo 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 to 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. All session related data are encrypted in transit with up to TLS 1.2, if supported (2048-bit RSA, AES256 strong encryption ciphers with 384-bit SHA-2 algorithm). The media stream is encrypted using SRTP_AES128_CM_SHA1_80.

GoTo also advises that Agents configure their browsers to use strong cryptography by default whenever possible to increase technical safeguards on the Agent’s machine and to always install the latest operating system and browser security patches.

When connections are established to the Rescue Live Lens website and between Rescue Live Lens components, GoTo servers authenticate themselves to clients using GlobalSign public key certificates. Server-to-server APIs are accessible only within GoTo’s private network behind robust firewalls.

3.4.2. At-Rest Encryption

Rescue Live Lens configurations, all session data, and recording files are encrypted at rest with 256-bit AES encryption.

3.4.3. TCP Layer Security

Internet Engineering Task Force (IETF)-standard TLS protocols are used to protect communication between endpoints.

For their own protection, GoTo recommends that all users 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.

3.5. Vulnerability Management

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

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.

3.5.1 Security Team

GoTo's Security team works closely with product engineers to continuously monitor and enhance the security of Rescue Live Lens. This collaboration ensures that our product remains secure and minimizes potential risks

3.5.2. Internal Assessments and External Audits

GoTo's internal review process includes regular security assessments at both the infrastructure and software level. Internal reviews are complemented by various independent external assessments to ensure that GoTo maintains industry standards.

4 Data Backup, Disaster Recovery and Availability

GoTo's disaster recovery strategy includes clearly defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) metrics to ensure minimal disruption. The RTO is set to a maximum of 35 minutes, ensuring that services can be restored within this timeframe following a disruption. The RPO is less than a minute for Rescue Live Lens and these metrics are obtained through actual disaster recovery testing. These metrics are regularly reviewed and tested to ensure they meet the operational needs and compliance requirements.

5 Hosting Workloads

The GoTo infrastructure is designed to increase service reliability and reduce the risk of downtime from any single point of failure using cloud hosting provider data centers.

Upon account creation, Rescue Live Lens Customers may elect to utilize either GoTo's European Union or Global data infrastructure to store their Customer Content. Hosting locations are specified below[2]:

- **European Union:** Germany, Ireland,
- **Global:** United States, Germany, Singapore

5.1 Cloud hosted workloads

Physical security is the responsibility of the Cloud provider (AWS). Reference to their documentation:

- https://aws.amazon.com/compliance/data-center/controls/

Other than physical security, all cloud provider operates with some form of a shared responsibility model where the cloud provider is responsible for protecting the infrastructure (hardware, software, networking) that runs all the services the provider offers. GoTo is responsible for the configuration of the services used.

6 Logical Access Control

Users authorized to access GoToAssist Remote Support V5 product components may include GoTo's authorized technical staff (e.g., Technical Operations and Engineering DevOps), customer administrators, or end-users of the product. On-premises 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.

7 Customer Content Retention Schedule

Session recordings will be deleted on an ongoing 365-day rolling basis.[3] Additionally, unless otherwise required by applicable law, Customer Content shall automatically be deleted: 1) for paid accounts, ninety (90) days after the termination, cancellation, or expiration and, in each case, deprovisioning of Customer's then-final subscription; or 2) for free accounts, after one (1) year of inactivity (e.g., no logins).

Upon written request, GoTo may provide written confirmation/certification of Content deletion.

[2] Hosting locations may vary (i.e., depending on data residency election), consult the applicable GoTo Resolve Sub-Processor Disclosure found in the Product Resources section of the GoTo Trust and Privacy Center (https://www.goto.com/company/trust/resource-center).

[3] Customers with other retention requirements can elect to locally save recordings to a storage location of their choosing outside of GoTo environments. For more information, see the "Playing Session Recordings" section here.

8 Appendix – Terminology

Agent: Rescue Live Lens user who creates Rescue Live Lens Sessions in order to provide audiovisual assistance to Customers via camera share.

Agent Web Console: A web-based 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 Rescue Live Lens Service. It enables the Agent to create and conduct Live Lens camera sharing Support Sessions as well as various account management, service management and reporting functions.

Support Session: For Rescue Live Lens, the support session is when the Agent and Customer are connected through the Rescue Live Lens Service to experience camera sharing to allow the Agent to assist the Customer.

Customer: The person receiving support from the Agent via a Rescue Live Lens Support Session.

Customer Mobile Browser: A web-based application that runs in any supported browser on the Customer's computer/mobile device and connects to a Rescue Live Lens Session through the Rescue Live Lens Service. It can provide camera share capabilities along with annotation, VOIP.

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.

Rescue Live Lens Service: A fleet of load-balanced, globally distributed servers providing secure access for the Agent Web Console and Customer Mobile Browser through encrypted web socket connection and API calls.