Technical and Organizational Measures
LogMeIn Rescue and Rescue Lens

Executive Summary

This Technical and Organizational Measures (TOMs) document outlines GoTo's commitments to privacy, security, and accountability for LogMeIn Rescue and Rescue 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* - Transparent Data Encryption (TDE) using Advanced Encryption Standard (AES) 256-bit for Customer Content.
- **Cloud Provider regions[1]:** United States, Germany, Australia and Ireland locations to support redundancy and stability.
- **Compliance Audits:** ISO/IEC 27001:2022, SOC 2 / SOC 3 Type II, BSI C5, PCI-DSS, TRUSTe Enterprise Privacy certifications, Internal controls assessment as required under a PCAOB annual financial statements audit and APEC CBPR and PRP certifications.
- **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/CPRA and LGPD.
- **Penetration Testing**: In addition to in-house offensive security testing, GoTo contracts with external firms to conduct penetration testing.
- **Logical Access Controls:** Logical access controls are designed and implemented 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**: GoTo employs advanced perimeter protection tools, techniques, and services to prevent unauthorized network traffic from accessing its product infrastructure. The GoTo network is safeguarded by externally facing firewalls and internal network segmentation to ensure robust security.
- **Retention**:
  - Rescue 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 within 90 days of the expiration of a Customer's then-final subscription term.

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

Contents

1 Product Introduction

LogMeIn Rescue is an online remote support service that enables technicians to provide remote assistance via the internet without the need for pre-installed software. With the End User's permission, Rescue allows a technician to access, view, and take control of the End User's computer. Through a chat window, the technician can diagnose and repair computer problems, as well as assist with operating system and software application issues.

Rescue Lens is an optional feature within Rescue that allows End Users to stream their mobile device cameras through the Lens mobile app to a remote technician. This enables the technician to view and troubleshoot problematic hardware, such as a misconfigured router or a damaged automotive component. Rescue Lens can be activated in the Rescue Admin Center. For more details, please refer to the Rescue Lens User Guide.

Capitalized terms in this document that are not defined within the text are defined in the Terms of Service.

2 Product Architecture

Rescue is a comprehensive Software-as-a-Service (SaaS) remote support solution designed to enhance the efficiency and effectiveness of technical support teams. It comprises three main components: the technician console, the End User mobile app or desktop applet, and the administration center.

The technician console serves as the primary interface for technicians to conduct remote support sessions. Technicians can initiate new sessions or respond to online End User requests in a shared queue. Communication and support are facilitated through Rescue's mobile app, available on both Android and iOS, or the desktop applet, compatible with Windows, macOS, and Linux. The applet is seamlessly downloaded to the End User's remote PC and is programmed to automatically remove itself upon the conclusion of the session.

The Rescue technician console interacts with the Rescue app or applet via a peer-to-peer (P2P) network connection (see Figure 1 below). When the applet is launched, the P2P process is initiated, connecting to a Rescue gateway where the session with the technician console is established.

GoTo's proprietary key exchange forwarding protocol ensures robust security against interception or eavesdropping on GoTo's infrastructure. The connection between the End User and the host is facilitated by the gateway, allowing the End User to connect to the host independently of the network setup. The host establishes a TLS connection to the gateway, which forwards the End User's TLS key exchange to the host through a proprietary key renegotiation request. This process enables the End User and the host to exchange TLS keys securely, without the gateway learning the key.

2.1 Key Agreement

When a support session begins and a connection is established between the End User and the technician, their computers must agree on an encryption algorithm from the available supported options and a corresponding key to be used for the duration of the session.

To validate their identities, the computers use certificates. Since neither the technician nor the End User have software capable of brokering the connection and validating installed security certificates, they both rely on one of the Rescue servers to perform the initial phase of the key agreement. The verification of the certificate by both the technician console and the End User app or applet ensures that only a Rescue server can mediate the process.

2.2 Overview of the Rescue Gateway Hand-off process

When the digitally signed Rescue app or applet is launched on a machine, it contains a session authentication Globally Unique Identifier (GUID). This GUID is embedded in the executable app or applet (e.g., a .exe file) as a resource by the site when downloaded. The app or applet then retrieves a list of available gateways from secure.logmeinrescue.com or secure.logmeinrescue.eu, selects a gateway from the list, and connects to it using TLS. The gateway is authenticated by the applet using its SSL certificate, and the gateway, in turn, authenticates the applet in the database with the GUID, registering that the End User is waiting for a technician.

When a technician picks up a session in the Rescue technician console, a request is sent to the gateway with the session authentication GUID to facilitate connections between the technician console and the End User app or applet. The gateway acts as an intermediary, authenticating the connection and relaying data at the transport level without decrypting it.

Once a connection relay is initiated, the parties attempt to establish a peer-to-peer (P2P) connection. The process is as follows:

- The applet starts listening for a Transmission Control Protocol (TCP) connection on a port assigned by Windows, macOS, or Linux.
- If the TCP connection cannot be established within 10 seconds, an attempt is made to establish a User Datagram Protocol (UDP) connection with the help of the gateway.
- If either a TCP or a UDP connection is established, the parties authenticate the P2P channel using the session authentication GUID, which then takes over traffic from the relayed connection.
- If a UDP connection is set up, TCP is emulated on top of the UDP datagrams using XTCP, a GoTo-proprietary protocol based on the Berkeley Software Distribution (BSD) TCP stack.
- Every connection is secured with the TLS protocol, using AES256 encryption with SHA256 Media Access Controls (MAC). The session authentication GUID is a 128-bit, cryptographically random integer value.

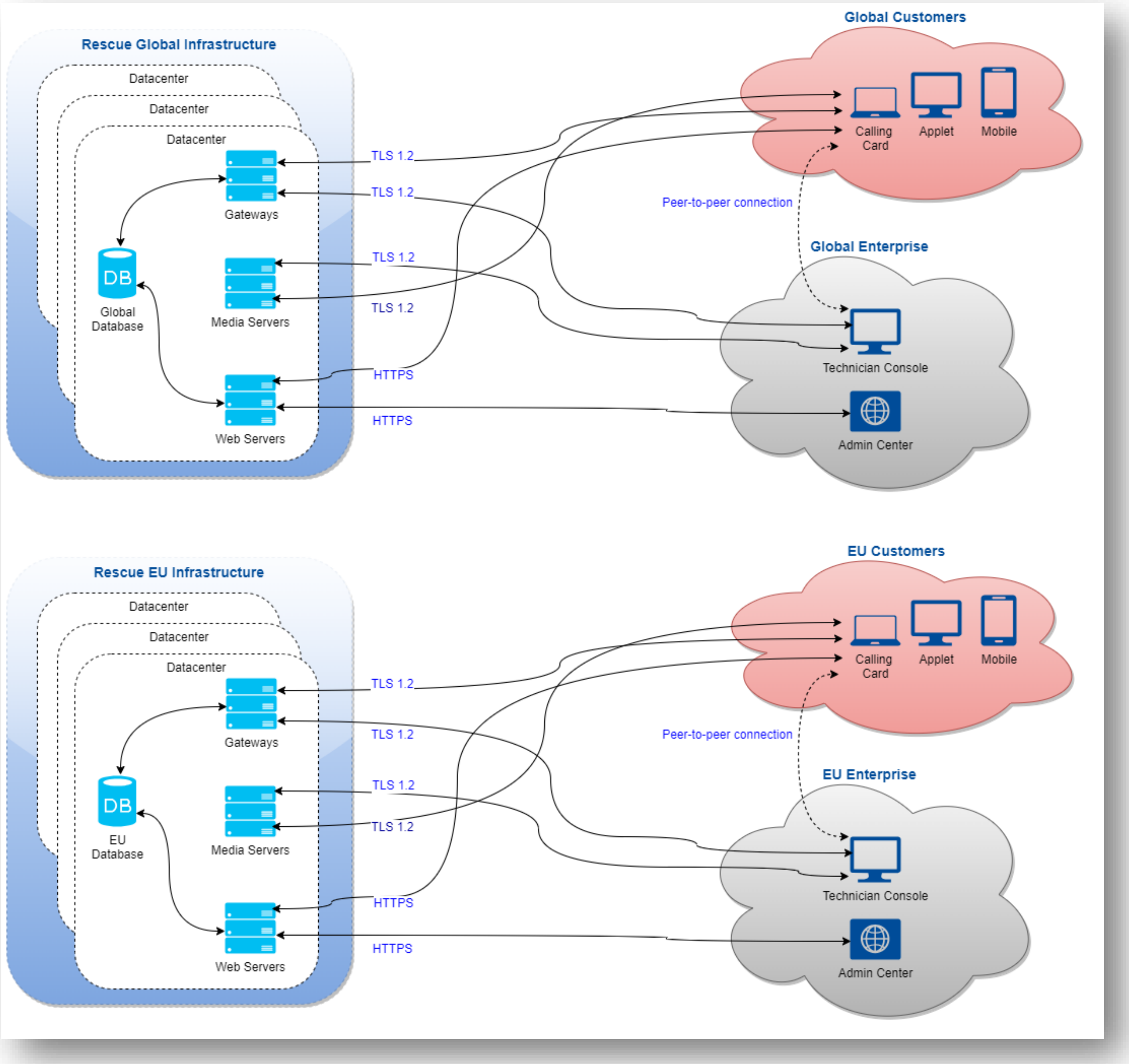

Figure 1: Rescue Architecture

2.3 Rescue Media Architecture

The Rescue media service is a WebRTC-based standalone service that powers Rescue Lens video streaming. It efficiently manages conferences for Rescue sessions utilizing the Lens feature. Conference participants, or peers, can join and leave conferences, while End Users send video and audio streams for other participants to receive. Lens transmits video content in a unidirectional stream from the Lens app to the technician console.

The media service comprises three main components: the Media Software Development Kit (MediaSDK), the session manager, and the streaming server. These components oversee the creation, destruction, joining, and leaving of conferences. They communicate through existing secure connections between the technician console and the website, as well as between the Lens app and the website.

2.3.1 MediaSDK

The media service is built on top of WebRTC with a thin wrapper around the WebRTC code base. Both the technician console and the mobile Lens app utilize MediaSDK.

2.3.2 Session Manager

The session manager is a load-balanced website that provides a Representational State Transfer (REST) API to manage (create, destroy, join) conferences. It only accepts requests from the website.

2.3.3 Streaming Server

The media service employs a custom streaming server solution to handle streams between peers, specifically the technician console and the Lens app. Both the technician console and the Lens app connect to the streaming server. In a Lens session, there are two streams: one sent from the Lens app to the streaming server and one received by the technician console from the server. The streaming server acts as a relay server between peers.

3 Technical Security Controls

GoTo employs technical security controls that are designed to safeguard the Service infrastructure and data residing therein.

3.1 Data Confidentiality

Rescue's secure online system is supported by Secure Sockets Layer and Transport Layer Security (SSL/TLS) and meets the following objectives:

- Authentication of the communicating parties
- Negotiation of encryption keys without interception
- Confidential exchange of messages
- Ability to detect if a message has been modified in transit

Rescue uses OpenSSL and at the time of publication, the version used by Rescue is 1.1.1n and 3.0.10.

3.2 Encryption

GoTo regularly reviews its encryption standards and may update the ciphers and/or technologies used in accordance with the assessed risk and market acceptance of new standards.

3.3 Encryption In Transit

All network traffic flowing in and out of the Rescue data centers, including all Customer Content, is encrypted in transit with TLS 1.2 and HTTPS. In addition, Rescue support sessions are protected with 256-bit AES encryption and MD5 Hash for enhanced traceability of file transfers.

Since all three components of the Rescue communications system are under GoTo's control, the cipher suite used by these components is always the same: AES256-SHA in cipher-block chaining mode with RSA key agreement. This means the following:

- The encryption/decryption algorithm is AES
- The encryption key is 256 bits long
- The encryption keys are exchanged using RSA private/public key pairs, as described in the previous section
- The basis of MAC is SHA-2. A MAC is a short piece of information used to authenticate a message. The MAC value protects both a message's integrity, as well as its authenticity, by allowing the communicating parties to detect any changes to the message.
- Cipher-block chaining (CBC) mode ensures that each ciphertext block is dependent on the plaintext blocks up to that point and that similar messages cannot be distinguished on the network.

Data traveling between the supported End User and the technician are encrypted end-to-end and only the respective parties have access to the information contained within the message stream.

3.4 Encryption At Rest

Rescue Customer Content is encrypted at rest at both the server and database levels with AES256 and TDE. As an example, Customer Content includes chat logs and custom fields, which are fields created by the master account holder or master administrator.

3.5 Rescue Access Controls

Rescue administrators can customize access controls. For example, Rescue administrators can configure a password policy including, a minimum required password strength and a maximum password age, force password resets, enforce two-factor authorization for Rescue logins, restrict technician access to Rescue from IP addresses preapproved for specific tasks, or grant technicians access to only pre-defined applications using a single SSO ID to log in to those applications. If needed, administrators can disable a technician's SSO ID.

Additional access controls include:

- Permission-based access on a granular level (such as permitting some technicians to use remote view, but not remote control)
- Not storing data from remote devices on GoTo servers. Only session logs, End User IP addresses and chat logs are stored — chat text logs can be removed from session details
- Preventing technicians from transferring files
- Requiring that the End User be present at the remote device to permit remote access
- Requiring that the End User maintain control and can terminate the session at any time
- Preventing technicians from using certain features until the End User has explicitly granted them permission (e.g., remote control, desktop view, file transfer, system information, reboot and reconnect)
- Automatic access rights revocation when the session is terminated

- The ability to force automatic logoff based on a predetermined time of inactivity
- Locking an account after five unsuccessful login attempts

3.5.1 Permission-Based Access Control

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

- Allowing clipboard synchronization
- Allowing screen sharing with Users and End-Users
- Deploying scripts
- Launching desktop viewing
- Launching file manager
- Launching remote control
- Rebooting
- Recording sessions
- Requesting credentials
- Sending and receiving files
- Sending URLs
- Starting private sessions
- Transferring sessions
- Using a single prompt for all permissions
- Viewing system information

For more details on group permissions, please reference the Rescue Administrators Guide. Rescue Lens technicians are identified by their email address and authenticated using a password.

3.5.2 Authentication

Rescue's authentication measures are designed to secure the product by employing measures to only permit technicians or administrators to login to the system. Technicians are assigned login IDs (e.g., matching their email addresses) and corresponding passwords by their administrators. Technicians enter these credentials into the login form on the Rescue website upon the beginning of their shift at a minimum. Administrators can configure controls to require authentication on a more frequent basis (e.g., after five minutes idle).

The Rescue system is first authenticated to the technician's web browser with its 2048-bit premium RSA SSL certificate ensuring that the technician will be entering their username and password into the correct website. The technician then logs in to the system with their credentials. Rescue does not store any passwords but instead uses SCrypt to create hashes from passwords that are then stored in the Rescue database. The hashes are salted with a 24-character string generated by CSPRNG for each unique password.

The Rescue system is also authenticated to the supported End User. The app or applet, downloaded and run by the End User, is signed with GoTo's code-signing certificate (based on a 2048-bit RSA key) and this information is typically displayed to the End User by their web browser when they are about to run the software. Rescue does not authenticate the End User to the technician.

Rescue also allows Administrators to implement a Single Sign-On (SSO) policy. Security Assertion Markup Language (SAML) is employed, which is an Extensible Markup Language (XML) standard for exchanging authentication and authorization data between security domains (between an identity provider and a service provider).

Administrators can also require two-step verification for logging in to Rescue. The two-step verification feature can use email, SMS or any Time-based One-time Password (TOTP) authenticator to provide a second layer of protection to a Rescue account by requiring selected members of the organization to set up an additional way of verifying their identity. Setting up the authenticator app is triggered in any of the following cases:

- The selected member tries to log in to their Rescue account on the secure website
- The selected member tries to log in to desktop technician console
- The selected member tries to change their Rescue password

3.5.3 Authorization

Authorization happens at least once during every remote support session. After downloading and running the applet, the supported End User will be contacted by a technician. The technician can chat with the End User via the applet but any further action, such as sending a file or viewing the End User's desktop, requires the End User's express permission. A "single prompt" can also be implemented for lengthy remote support work where the End User might not be present for the entire duration of the session. If this setting is enabled for a technician group, the technicians in that group can request a "global" permission from the End User and, if granted, can perform actions such as viewing system information or entering a remote control session without being further authorized by the End User. Administrators can also impose IP address restrictions so that technicians assigned to a particular task can only access Rescue and perform that task from pre-approved IP addresses. The administrator of a technician group can also disable certain features in the administration center.

The permissions an administrator can grant or deny include:

- Launch remote control
- Reboot
- Launch desktop viewing
- Record sessions
- Send and receive files
- Start private sessions
- Launch File Manager
- Request credentials
- Send URLs
- Allow clipboard synchronization
- View system information
- Deploy scripts
- Use single prompts for all permissions
- Transfer sessions

- Allow screen sharing with Users and End Users

3.6 Audit Controls

The following audit controls are available to Rescue Users and End Users:

- The option to force session recording, with the ability to store audit files on a secure shared network
- Technician sessions and remote session activity logging on the host computer to ensure security and maintain quality control (successful logins, unsuccessful logins, remote control started, remote control ended, reboot initiated, logout)
- Person or entity authentication
- Technician authentication using their unique email address or via an SSO ID
- Allowing technicians to log in only from approved IP addresses
- Audit report available in Admin Center includes changes to account settings and data for each action taken by Administrators on the selected item of the Organization Tree during a particular period

4 Data Backup, Disaster Recovery and Availability

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 for one month locally and copied to AWS S3 Glacier. Purchase-related data is retained for 7 years, while all other databases are kept for 4 years. In the event of a complete failure of the datacenter hosting the primary database, Rescue architecture is designed to be rapidly restored.

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 redundant, active-active infrastructure in cloud hosting provider data centers.

Hosting/storage locations are specified below[2]:

- **European Union:** Germany and Ireland
- **Global:** The United States, Germany, Australia and the United Kingdom

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/
- https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security
- https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html

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

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 Logging, Monitoring and Alerting

Rescue chat logs are saved in the Rescue database. The chat log is transmitted to the Rescue servers by the technician console in real time and contains events as well as chat messages that pertain to a particular support session. Log files will display the following actions by technicians: start and end time of a remote-control session, instances of technicians sharing files with End Users and metadata relating to file sharing (e.g., the name and MD5 Hash thumbprint of a transmitted file). The chat log database can be queried from the administration center.

For active accounts, the contents of the logs will be made available online for two years after the end of a remote support session and archived for two years after that.

To facilitate integration with CRM systems, Rescue can post session details to a URL and administrators can choose to exclude chat text from these details. Chat text is included by default, but Customers can change that setting in the administration center. Additionally, all records of chat texts between technicians and End Users can automatically be omitted from the session details stored at a Rescue data center. Rescue allows technicians to record the events that transpire during a desktop viewing or remote-control session into a video file. The recording files are stored in a directory specified by the technician.

7 Customer Content Retention Schedule

Customer Content Retention Schedule: Unless otherwise required by applicable law, Customer Content shall automatically be deleted within 90 days of the termination, cancellation, or expiration and, in each case, deprovisioning of Customer’s then-final subscription.

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