Technical and Organizational Measures
Miradore

Executive Summary

This Technical and Organizational Measures (TOMs) document outlines GoTo's commitments to privacy, security, and accountability for Miradore. 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* - Virtual machine data is protected with Azure host encryption and RSA 4096 customer-managed keys, while databases use AES 256-bit encryption.
- **Compliance Audits:** Miradore holds ISO/IEC 27001:2022, PCI-DSS, TRUSTe Enterprise Privacy certifications, Internal controls assessment as required under a PCAOB annual financial statements audit, Global CBPR and PRP certifications, 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 and LGPD.
- **Penetration Testing**: In addition to in-house testing, GoTo contracts with external firms to conduct 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 employs 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**:
  - Miradore 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 ninety (90) days after the end of Customer’s then-final subscription term when they cancel or terminate their account.

Contents

1 Product Introduction

Miradore is GoTo's cloud-based mobile device management (MDM) solution for Android and iOS mobile devices and macOS and Windows workstations (the "Service"). Miradore's feature set allows administrators to manage device security, settings and restrictions, data security, app settings, content, automation and reporting—all from a single portal.

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

2 Product Architecture

Miradore is a device management solution for mobile devices and workstations featuring a multi-tier architecture. Miradore leverages Microsoft Azure cloud resources to provide a scalable, highly available solution with no single point of failure. Security measures provide in-depth defense at all levels, from the physical layer through the application layer.

There are multiple Miradore interfaces including the main user interface, the web service API, connectors to third-party systems and managed devices.

2.1 The Main User Interface

Miradore's main user interface is the management console. It is browser-based and employs the secure HTTPS protocol between the Service and the user's browser.

2.2 Web Service API

Miradore API is a Representational State Transfer (REST)-based web service that enables Miradore to integrate with external information systems. The API is used over HTTPS with the GET method to export data directly from Miradore's database in XML or JSON format. All API requests are authenticated with authentication keys that are administered in the management console of each Miradore instance. See the API Support Article for more information

2.3 Miradore in Managed Services

Devices communicate with the Service's server either through the Miradore client, which is a custom program installed on a workstation or device, or through the platform's integrated mobile device management framework provided by Apple (iOS), Google (Android) or Microsoft (Windows).

To become a managed device in Miradore, a device must go through an enrollment process. The device enrollment process is initiated either by the individual using the device ("End User") or the administrator of a Miradore instance ("User") and is authenticated with one-time enrollment credentials created for each enrollment. If the User initiates the enrollment process, the enrollment credentials are included in the enrollment invitation message sent to the End User by email or SMS. If the End User initiates the enrollment process (self-service), they will use a specific company passcode to enroll the device through the enrollment portal (https://login.online.miradore.com/enroll). To access self-service enrollment, an individual must be listed in the specific Miradore instance as a device End User. After a successful enrollment, the End User who completed the enrollment will become the assigned End User of that device in Miradore.

Data moves between a managed device and the Service when the Miradore client polls the Service for commands, the Service returns the commands, and the Miradore client posts back the task results. Examples of commands include enforcement of configuration policy settings, software installations and scheduled task results (e.g., hardware and software inventories). If an instant synchronization is needed, the Service can request that a managed device poll the Service immediately through an applicable push notification service.

The vendor push notification services (Apple Push Notification Service, Firebase Cloud Messaging, Azure SignalR and Windows Push Notification Service) are connected to the managed devices and the Service with HTTPS and vendor-specific protocols. Additionally, the Miradore client for macOS, iOS, Windows, and Android platforms is cryptographically signed to authenticate connections with the Service. Additionally, Miradore client for macOS, iOS, Windows, and Android platforms uses HTTPS protocol for securing the communication and HMAC with SHA-256 and RSA 2048-bit key exchange for data integrity and authentication.

Regardless of the device operating system, End Users are always able to see whether their device is managed with Miradore. Typically, there is a client application or MDM profile visible to the End Users.

3 Technical Security Controls

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

3.1 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.

3.1.1 Encryption In Transit

Miradore utilizes HTTPS TLS 1.2 protocols to secure network traffic. All communications in-transit between the End User and the user interface are encrypted.

3.1.2 Encryption At Rest

All servers are encrypted. At-rest, virtual machine server data is stored with Azure encryption at host and CMK Rivest–Shamir–Adleman (RSA) 4096. Databases are encrypted with service-managed transparent data encryption using the encryption algorithm AES 256-bit.

3.2 User Authentication

Users are authenticated with a username and a password which must be at least fourteen characters long. User passwords are salted and stored in the database as Secure Hash Algorithm (SHA)-512 hashes and are cryptographically signed.

All User connections to the Service and actions within the Service are logged and displayed in the action log to provide an audit trail. If a User forgets their password, they can reset it through a Microsoft school or work account or using the password recovery workflow that is built-in to the Service and available through the login screen.

The password recovery workflow sends an email to the User containing a hyperlink for resetting the User's password. Two-factor authentication is available for the Service and can be configured by an individual User for their own login or as a requirement set by an administrator for an entire Miradore account.

4 Data Backup, Disaster Recovery and Availability

Customer Content backup is done within the same data center in 24-hour and seven-day intervals. In addition, a corresponding backup is made in a geographically distant data center every seven days and is retained for four weeks.

Database servers and front-end web servers hosting the Service are backed up daily. Databases have point-in-time restore available for up to 14 days and weekly long-term database backups available for one year. Web servers have instant recovery possible for two days.

Firewalls are used on network connections between the internet and the data center network to only allow connections over HTTPS (port 443) to designated web servers. A load balancer is used to distribute requests evenly among the web servers.

Server hardware, operating systems, and the Miradore Service are continuously being monitored and persons responsible for servers will be alerted in case of deviations in the Service operability.

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.

Hosting locations may vary (i.e., depending on data residency election), for detailed information, please refer to the LogMeIn Resolve Sub-Processor Disclosure available in the Product Resources section of the GoTo Trust and Privacy Center.

5.1 Cloud hosted workloads

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

- https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

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. The customer is responsible for the configuration of the services they are using.

6 Customer Content Retention Schedule

Unless otherwise required by applicable law, Customer Content shall automatically be deleted.

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

7 Revision History

Version	Month/Year	Description
Version 1.2	July 2024	Updated and published by Legal
Version 1.3	August 2025	Standardized the document to include only Product Specific sections.