Technical and Organizational Measures
Central and Pro

Executive Summary

This Technical and Organizational Measures ("TOMs") document sets out GoTo's privacy, security and accountability commitments for Central and Pro. Specifically, GoTo maintains robust global privacy and security programs and organizational, administrative and technical safeguards designed to: (i) ensure the confidentiality, integrity and availability of Customer Content; (ii) protect against threats and hazards to the security of Customer Content; (iii) protect against any loss, misuse, unauthorized access, disclosure, alteration and destruction of Customer Content; and (iv) maintain compliance with applicable law and regulations, including data protection and privacy laws. Such measures include:

- **Encryption**:
  - *In Transit* Transport Layer Security (TLS) v1.2 or v1.3, where supported.
  - *At Rest* Transparent Data Encryption (TDE) and Advanced Encryption Standard (AES) 256-bit for Customer Content.
- **Data Centers:** Germany, Australia, the United Kingdom, the United States, the Netherlands and Ireland data center locations to support redundancy and stability.
- **Physical Security:** Suitable physical security and environmental controls are in place and designed to protect, control and restrict physical access for systems and servers that maintain Customer Content in order to support uptime, performance and scalability commitments.
- **Compliance Audits:** Central and Pro hold SOC 2 Type II, C5, PCI DSS, PCAOB, TRUSTe Enterprise Privacy 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.
- **Security Assessments**: 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**:
  - Central and Pro 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 expiration of a Customer's then-final subscription term.

Table of Contents

Click the page numbers below to go to the relevant TOMs section

1 Product Introduction

Central is a web-based management console that enables IT professionals to access, manage and monitor remote devices, deploy software updates and patches, automate IT tasks and run hundreds of versions of antivirus software. Central is offered as a premium service with multiple pricing tiers based on the number of devices supported and features desired.

Pro is a remote access service that provides secure access to a remote computer or other internet-enabled device from any other internet-connected device, as well as most smartphones and tablets. Once a Pro host is installed on a device, the service is designed to enable an individual with a sub-account within a Customer account ("User") to access that device's desktop, files, applications and network resources remotely from the User's other internet-enabled devices. Pro can be rapidly deployed and installed without the need for IT expertise.

Central and Pro are designed to allow secure remote access to critical resources over an untrusted network and security is a key consideration during product development.

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

2 Technical Measures

GoTo's products are designed to provide solutions that are secure, reliable and private. The technical measures defined below describe how GoTo implements that design and applies it in practice for Central and Pro.

2.1. Safeguards

GoTo's implementation of safeguards, features and practices involve:

I. Building products that take security and privacy by design and default into account, and including additional layers of security in order to protect Customer Content;

II. Maintaining organizational controls that operationalize internal policies and procedures related to standards compliance, incident management, application security, personnel security and regular training programs; and

III. Ensuring privacy practices are in place to govern data handling and management in accordance with applicable law, including the GDPR, CCPA/CPRA, LGPD, as well as with our own Data Processing Addendum (DPA), and applicable GoTo policies and commitments.

By building security safeguards into the product, we strive to protect GoTo Customer Content from threats and ensure security controls are appropriate to the nature and scope of the Services. GoTo's configurable security features can help administrators minimize threats and risks to systems and networks posed by individuals who use GoTo services.

3 Product Architecture

Central and Pro are SaaS-based applications featuring a multi-tier architecture hosted in geographically distributed data centers. Security measures at all levels, from the physical layer through the application layer, are designed to provide defense in depth.

The Central and Pro applications are composed of three key components that enable a successful remote access session:

- **Client**: the software (e.g., browser, native app, mobile app) accessing a remote resource;
- **Host or server**: the device being accessed, or the product's host software on this device; and
- **Central/Pro gateway**: the service that mediates traffic between the client and the host.

The Central/Pro host is designed to maintain a constant Transport Layer Security (TLS)-secured connection with a gateway server located in one of the GoTo data centers. After it establishes a secure connection to Central or Pro, the client is authenticated and authorized by the host to access the device, and the remote access session begins. The gateway server mediates the encrypted traffic between the two entities but does not require that the host implicitly trust the client. The Central/Pro gateway allows either the client or host (or both) to be firewalled, relieving Users of the need to configure firewalls.

GoTo's proprietary key exchange forwarding protocol is designed to provide security against interception or eavesdropping on our own infrastructure. Specifically, the connection between the client and the host is facilitated by the gateway to ensure that the client can connect to the host independently of the network setup.

With the host already having established a TLS connection to the gateway, the gateway forwards the client's TLS key exchange to the host via a proprietary key renegotiation request. As such, the client and the host exchange TLS keys without the gateway learning the key.

Figure 1: Central Architecture

4 Technical Security Controls

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

4.1. Encryption

GoTo periodically 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 to continuously improve its practices and encryption methods.

Central and Pro services support the following encryption protocols (as applicable): TLS 1.2, 2048-bit RSA and AES256 encryption ciphers with 384-bit SHA-2 algorithm.

Central and Pro support both AES 128 and 256-bit keys, and the client and the server will agree on the strongest compatible and available cipher between those two key lengths. The client sends the server a list of ciphers it is willing to use, and the server chooses the one it prefers. In Central and Pro, the server selects the strongest shared cipher suite that the client has offered.

4.2. Encryption In Transit

All network traffic flowing in and out of Central/Pro data centers, including Customer Content, is encrypted in transit with TLS 1.2 or, where supported, TLS 1.3.

4.3. Encryption At Rest

All Central/Pro Customer Content is stored in MSSQL with Transparent Data Encryption (TDE) and encrypted at rest with AES-256.

4.4. User Authentication

Central/Pro uses a proprietary Common Login Service (“CLS”) for User authentication. CLS employs custom heuristics designed to prevent suspicious User access. For accounts that have a linked GoTo Common Identity Platform (“CIP”) account, the login is further protected by a third-party risk assessment service.

4.5. Multifactor Authentication

Multifactor authentication (also referred to as two-step verification or two-factor authentication) adds a second layer of protection to an account by requiring two distinct forms of identification to log in. After setting up multifactor authentication, Users will enter their credentials and then be prompted to verify their identity through a security code.

Central subscribers can enforce a login policy that forces all Users in their account to use multifactor authentication. For step-by-step instructions, visit support.logmeininc.com/central.

4.6. Printed Security Codes

Customers can opt to use printed security codes as an additional layer of protection. When the User enables this feature, they are required to print out a list of nine-character random passwords generated by the gateway. Each time the User logs in to their account at logmein.com, they will be prompted to enter one of the security codes from the list to gain access to their account. Each code can be used only once. Before the User runs out of printed security codes, they will be required to print another sheet. This invalidates any previously unused security codes.

4.7. Emailed Security Codes

When this feature is turned on and the User authenticates successfully with their email address and password to the Central/Pro gateway, a passcode is generated and sent to the email address. The User receives this passcode in an email and enters the code into the form provided by the gateway. The password expires either upon use or within a few minutes of generation, whichever comes first.

4.8. Authentication of the Gateway to the Client

Central and Pro utilize TLS 1.2 or 1.3 certificate-based authentication (with 1.3 used where supported and not explicitly disabled) to verify server identities and ensure that when a User connects to a Central or Pro server via a gateway, they are connecting with the intended device. When a connection is made, the server’s certificate is verified. A warning is presented if an untrusted certifying authority issued the certificate. A different warning is presented if the hostname in the URL does not match the hostname in the certificate, even if issued by a trusted authority.

If the server passes these verifications, the User’s client generates a pre-master secret (PMS), encrypts it with the server’s public key contained within its certificate, and sends it to the server. Public key cryptography is used so that only the server that holds the corresponding private key can decrypt the PMS. The PMS is then used by both the User and the server to

derive the master secret, which is then used to derive initialization vectors and session keys for the duration of the secure session.

4.9. One2Many – Authentication and Encryption (Central Only)

The One2Many feature allows advanced scripting and deployment capabilities that enable Central Users to perform mass functions across managed organizations. With this tool, Users can execute, manage, and monitor administrative tasks on multiple Windows and Mac devices directly from Central.

Multifactor authentication is required for One2Many. One2Many stores multifactor authentication credentials in two different ways: when executing a task in real-time, it stores the credentials in the browser; when the task is scheduled to be executed later, the credentials are stored in the database of the product.

Credentials used in One2Many are encrypted with the host's public key first, and then further encrypted by the website. The first layer of encryption ensures that only the host can decrypt the credentials with its private key; and the second layer of encryption enables the option to wipe data from the website, even if the host is offline.

4.10. Authentication of Users to the Gateway

Users must be authenticated by both the gateway and the host. A User's email address and password is verified whenever they log on to Central/Pro.

NOTE: Central Customers can enforce a strong password policy. Visit support.logmeininc.com/central for details.

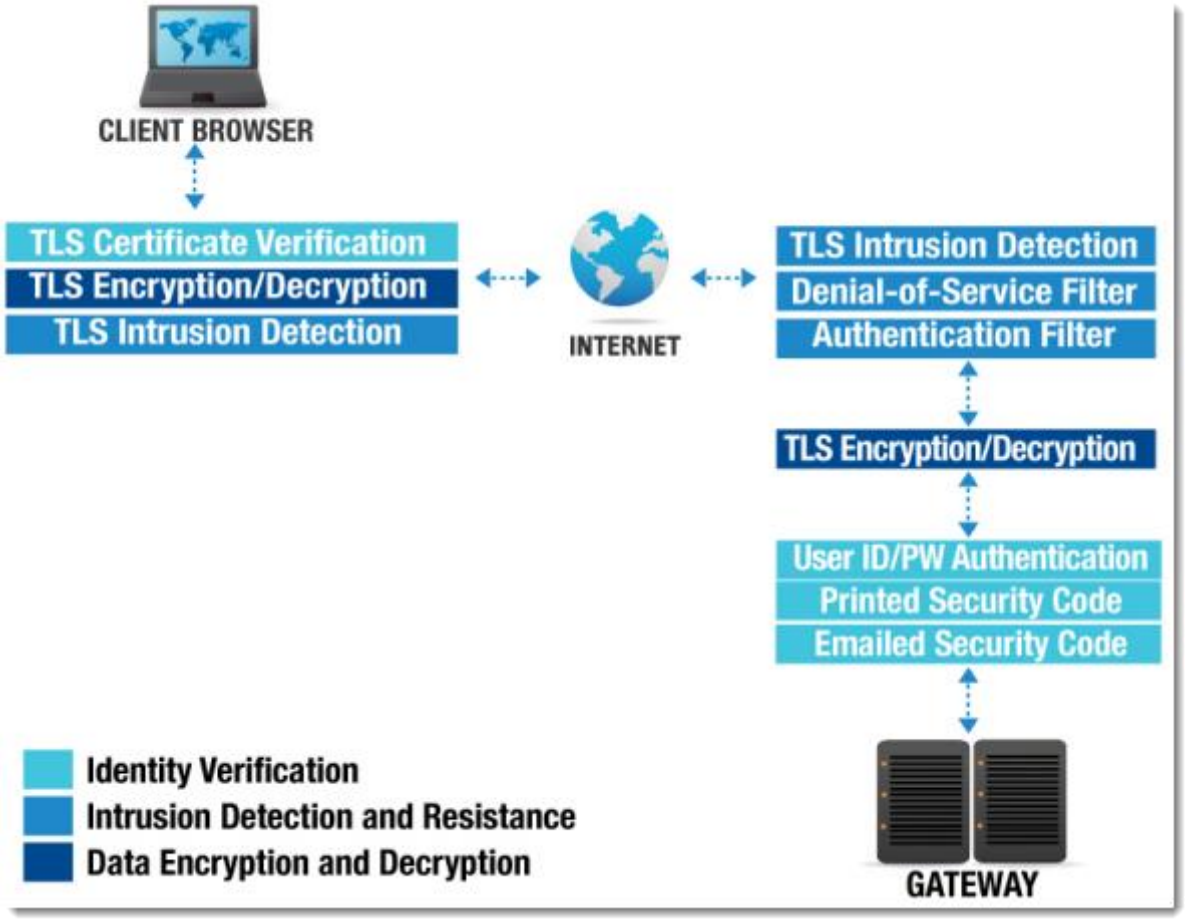

Figure 2: Authentication between Users and the Gateway

4.11. Account Audit

Customers can keep track of activity in their Central/Pro account through email notifications. In addition to default events, Customers can select events about which to be notified such as login attempt failure or password changes.

4.12. Authentication of the Gateway to the Host

The gateway must prove its identity to the host before it is trusted with access codes. The host, when making a connection to the gateway, checks the certificate transported during the TLS “handshake” to make sure it is connecting to one of the GoTo gateway servers.

4.13. Authentication of the Host to the Gateway

The gateway verifies the host’s identity using a long unique identifier string. This string is a shared secret between the two entities and is issued by the gateway when the host is installed. Once the host identifies the unique identifier string, it communicates the string back to the gateway over a TLS-secured channel. Figure 3 illustrates how the host and the gateway

authenticate each other before a host is made accessible to the client. To ensure further security, the host can change its shared secret with a request from the gateway via the secure connection.

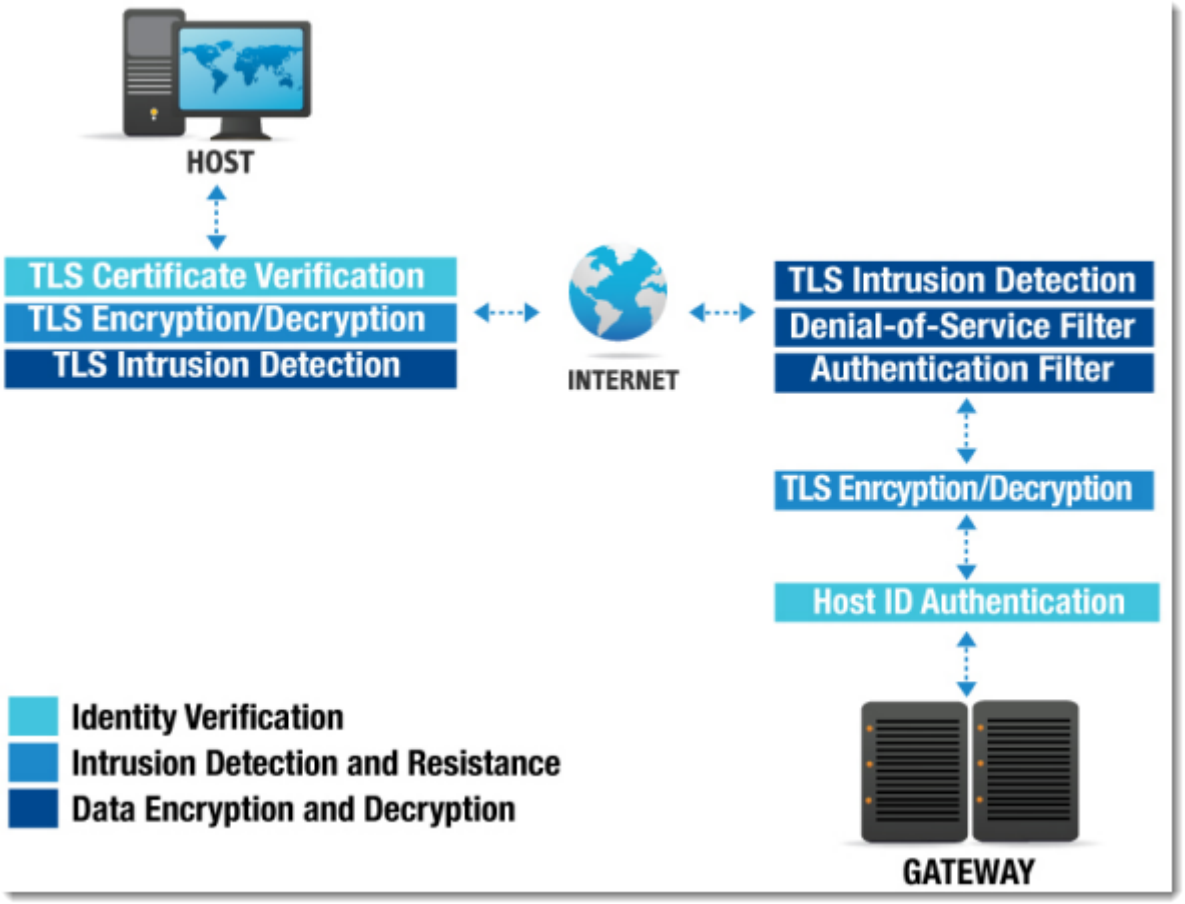

Figure 3: Host and Gateway Authentication

4.14. Intrusion Detection

Central and Pro have two layers of security which are designed to detect intrusion attempts: TLS and GoTo intrusion filters.

4.15. TLS

For the first layer of intrusion detection, Central/Pro utilizes TLS 1.2 or 1.3 certificate-based authentication (with 1.3 used where supported and not explicitly disabled) to ensure that the data has not changed in transit. This is achieved by the following techniques:

Record Sequence Numbering	Record sequence numbering means that TLS records are numbered by the sender and the order is checked by the receiver. This ensures that an attacker cannot remove or insert arbitrary records into the data stream.

Message Authentication Codes	Message authentication codes (MACs) are appended to every TLS record. This is derived from the session key (known only to the two communicating parties) and the data contained within the record. If MAC verification fails, it is assumed that the data were modified in transit.

4.16. Central/Pro Intrusion Filters

The second layer is provided by GoTo itself and is comprised of three intrusion filters:

4.17. IP Address Filter

When Central/Pro receives a connection request from a client, it first checks its list of trusted and untrusted IP addresses and may deny the connection if it is untrusted. An administrator can set up a list of IP addresses within Central/Pro that will be either allowed (trusted) or denied (untrusted) a connection to the selected host (for example, an administrator can designate the company's internal network and another administrator's home IP address as allowed).

4.18. Denial of Service Filter

A Denial of Service Filter rejects connections if the requesting IP address has made an excessive number of requests without authentication within the observation time window to protect the host device from being overloaded.

4.19. Authentication Filter

If the User made an excessive number of failed login attempts, the Authentication Filter rejects the connection. The Authentication Filter is in place to prevent a potential intruder from gaining access to an account by guessing an account name and password.

4.20. Authentication and Authorization of Users to the Host

After being granted access by the previous layers, the User must prove their identity to the host. This is achieved by a mandatory OS-level authentication step: the User is authenticated to the host using their device (e.g., Windows or Mac) username and password. Where relevant, the domain controller will receive this request which validates the User's identity and ensures that network administrators can control who is able to log in to a specific host.

4.21. Personal Password

A personal password is another optional security measure that can be set up on the Central/Pro host. The User can assign a personal password to the host, which, like the OS-level password, is not stored or verified by the gateway. Unlike with the operating system password, the host never asks for the complete personal password, so the User never enters it in its entirety in any single authentication session. The User is usually prompted for three random characters of the personal password for example, the first, the fourth and the seventh) by the host after OS-level authentication has succeeded. If the User enters the correct characters, they are granted access.

4.22. GoTo and RSA SecurID

To add an extra layer of security over the username/password authentication, Users can configure Central/Pro to require RSA SecurID authentication. For information on setting up this feature on a Central/Pro host, visit https://support.logmeininc.com/pro.

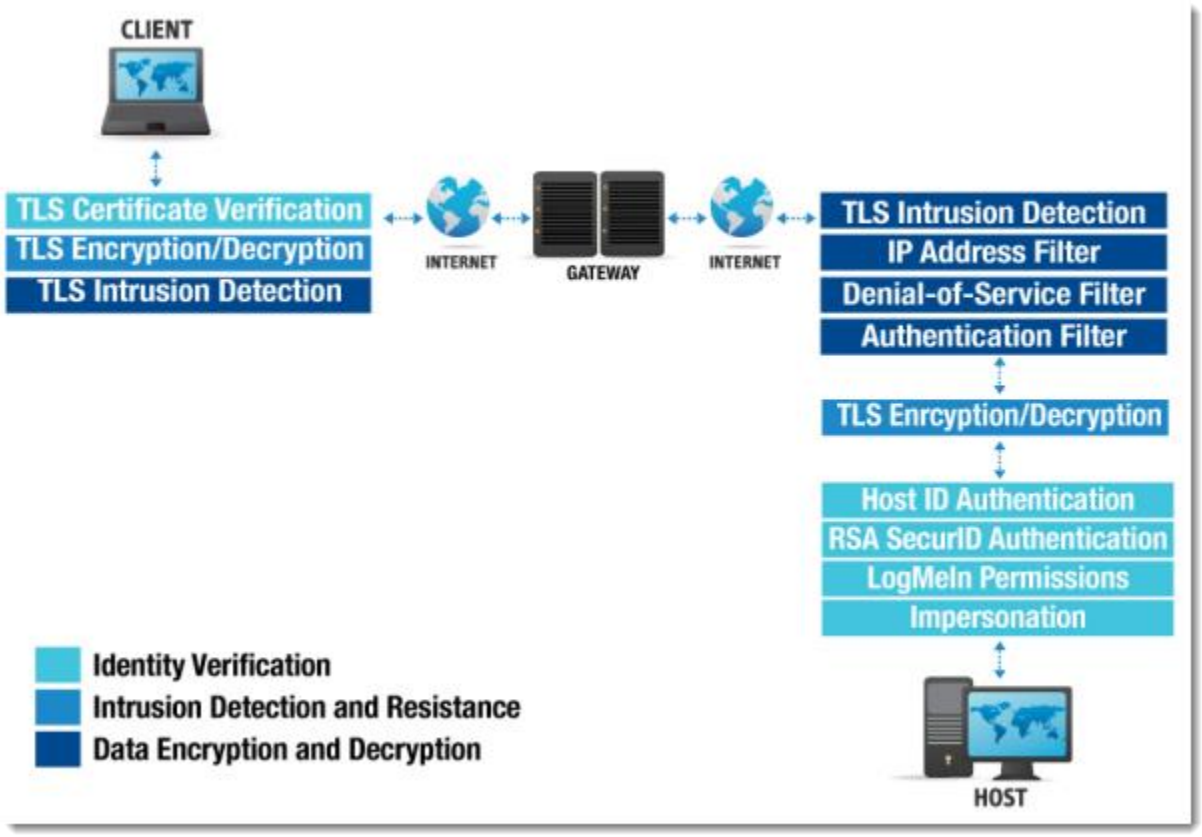

Figure 4: Authentication between Users and the Host

4.23. Authentication and Authorization of Users within the Host

Once Central/Pro has verified the User's identity using the above methods, it checks its own internal User database to see which internal modules the User is allowed to access.

System administrators can configure Central/Pro so that Users with certain roles have access only to a subset of tools offered by GoTo; for example, the Helpdesk department can be granted access to only view a device's screen and performance data, but not actually take over the mouse and the keyboard or make any changes to the system configuration. Alternatively, the Sales department could be given full remote-control access to their respective devices, but not to features such as performance monitoring and remote administration.

Using the operating system access token obtained when the User was authenticated, Central/Pro impersonates the User to the operating system while performing actions on the User's behalf. This ensures that Central/Pro adheres to the operating system's security model,

and Users have access to the same files and network resources as if they were sitting in front of their device. Resources unavailable to Users in Windows or OS X also remain unavailable via Central/Pro.

See "Controlling Who Can Access Your Host Computers" on the Central or Pro support site for details.

4.24. Auditing and Logging

Central and Pro provide extensive logging capabilities. A detailed log of the events that occur within the software is kept in the Central/Pro data log directory. Certain important events are also placed in the Windows or OS X application event log, including logon and logoff actions. The detailed log can also be sent to a custom SYSLOG server of the Customer's choice.

See "How to View Host Event Log Files" on the Pro support site for details. For SYSLOG, see "Define Syslog Settings for the Host" on the Central support site.

4.25. Data Forwarding

The gateway provides end-to-end encryption by forwarding encrypted data between the host and the client.

To enable this, the first part of the TLS negotiation is performed between the gateway and the client. The gateway then passes the exchange on to the host, which re-negotiates the TLS session and agrees on a new session key with the client, thereby providing true end-to-end encryption.

When the traffic is relayed through the gateway, the client establishes a TLS session with the gateway using the gateway's certificate. The gateway transfers this TLS session's state (including the Pre-Master Secret) to the host. After agreeing on a new session key, the host uses this session state to handle the rest of the TLS session directly with the client. The gateway's certificate secures the session, leaving the client communicating directly with the host without the need for the gateway to decrypt and re-encrypt traffic.

4.26. UDP NAT Traversal

User datagram protocol (UDP) is used at the network layer, as defined by the ISO/OSI Network Model, with a transmission control protocol (TCP)-like transport layer built on top of it, complete with flow control, dynamic bandwidth scaling and packet sequence numbering. Logmein.com uses UDP instead of TCP packets (thereby effectively re-implementing a TCP-like transport layer). After a reliable TCP-like stream is constructed from unreliable UDP packets, the stream is further protected by a TLS layer, providing full encryption, integrity protection and endpoint verification capabilities.

To set up a UDP NAT Traversal connection, both the client and the host send several encrypted UDP packets to the gateway. These packets are encrypted using a secret key shared by the gateway and the respective peer and are communicated over the pre-existing TLS connection.

The gateway uses these packets to determine the external (Internet) IP addresses of the two entities. It also tries to predict which firewall port will be used for communication when a new UDP packet is sent. It passes its findings down to the peers, which then attempt to set up a direct connection. If the gateway can determine the port in use, the connection succeeds. The peers verify each other using another shared secret obtained from the gateway. A TLS session is established. The peers then communicate directly.

If a direct connection cannot be set up, the peers will connect back to the gateway over TCP and request that a forwarded, end-to-end encrypted session be used. This process takes only a few seconds, is transparent to the User, improves performance and reduces latency when a direct connection is in use.[1]

4.27. Software Updates and Gateway Security

The Central/Pro host, based on User preferences, can semi-automatically or automatically update itself on the User's device. The host software periodically checks the logmein.com website for newer versions of the software. If a new version is found, it is automatically downloaded, and a message is displayed to the User who can allow the update to take place. The download process uses at most 50% of the available bandwidth, therefore keeping interference with other networking applications to a minimum.

These software updates are digitally signed by logmein.com with a private key that is not found on any of our Internet-connected systems.

Central/Pro passwords are not stored in our database: Central and Pro use a one-way cryptographic key derivation function and a per-account salt value.

5 Security Program Updates

GoTo reviews and updates its security program and engages independent third parties to assess its relevant security controls at least annually to ensure it evolves against the current threat landscape and to ensure compliance with relevant frameworks, industry standards, Customer commitments, and, as applicable, changes in laws and regulations pertaining to the security of GoTo data.

6 Data Backup, Disaster Recovery and Availability

GoTo'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

[1] For further details see US Patent no. 7,558,862

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.

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.

7 Data Centers

The GoTo infrastructure is designed to increase service reliability and reduce the risk of downtime from any single point of failure using:

a) redundant, active-active data centers; or
b) cloud hosting provider data centers.

Data centers are located in either Germany, Australia, the United Kingdom, the United States, the Netherlands or Ireland.

All data centers include monitoring of environmental conditions and have around-the-clock physical security measures in place.

7.1. Data Center Physical Security

GoTo contracts with data centers to provide physical security and environmental controls for systems and servers that contain Customer Content. These controls include the following:

- Video surveillance and recording;
- Heating, ventilation and air conditioning temperature control;
- Fire suppression and smoke detectors;
- Uninterruptible power supply;
- 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; and
- Scheduled maintenance and validation of all critical security and environmental controls.

GoTo limits physical access to production data centers 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 GoTo's technical operations team. All physical access to data centers and server rooms is logged and GoTo management reviews logs on at least a quarterly basis. Additionally, data center physical access authorization is removed promptly upon role change (where such access is no longer required) or upon termination of any previously authorized personnel. Multi-factor access (e.g., biometrics, badge and keypad) is required for highly sensitive areas, which include data centers.

8 Standards Compliance

GoTo regularly assesses its compliance with applicable legal, financial, data privacy and regulatory requirements. GoTo's privacy and security programs have achieved various certifications and been assessed in accordance with external audit standards, including:

- **TRUSTe Enterprise Privacy & Data Governance Practices Certification** to address operational privacy and data protection controls that are aligned with key privacy laws and recognized privacy frameworks. To learn more, please visit our blog post.
- **TRUSTe APEC CBPR and PRP Certifications** for the transfer of Customer Content between APEC-member countries obtained and independently validated through TrustArc, an APEC-approved third-party leader in data protection compliance. To learn more about our APEC certifications, please click here.
- American Institute of Certified Public Accountants (AICPA) **Service Organization Control (SOC) 2 Type II** attestation report incl. **BSI Cloud Computing Catalogue (C5)**.
- **Payment Card Industry Data Security Standard (PCI DSS)** compliance for GoTo's eCommerce and payment environments.
- Internal controls assessment as required under a **Public Company Accounting Oversight Board (PCAOB)** annual financial statements audit.

9 Application Security

GoTo's application security program follows the Microsoft Security Development Lifecycle (SDL) to secure product code. The Microsoft SDL program includes manual code reviews, threat modeling, static code analysis, dynamic analysis and system hardening. GoTo teams also periodically perform dynamic and static application vulnerability testing and penetration testing activities for targeted environments.

10 Logging, Monitoring and Alerting

GoTo maintains policies and procedures around logging, monitoring and alerting, which set out the principles and controls that are implemented to bolster our ability to detect suspicious activity and respond to them on a timely basis. GoTo collects identified anomalous or suspicious traffic in relevant security logs in applicable production systems.

11 Endpoint Detection and Response

Endpoint Detection and Response (EDR) software with audit logging is deployed on all GoTo servers to minimize disruption or impact on the performance of the Service. Security investigations will be initiated in accordance with our incident response procedures if suspicious activity is detected, as appropriate and necessary. See section 17 for more information on GoTo's Security Operations Center and incident response procedures.

12 Threat Management

GoTo's Cyber Security Incident Response Team ("CSIRT") is comprised of multiple teams and is responsible for cyber threat protection. Specifically, the Cyber Threat Intelligence team within the CSIRT collects, vets and disseminates information as it pertains to current and emerging threats. GoTo stays current with threat intelligence and mitigation through review of open and closed sources and participation in sharing groups and industry memberships (IT-ISAC, FIRST.org, etc.).

13 Security and Vulnerability Scanning and Patch Management

GoTo maintains a formal patch management program and, on at least a quarterly basis, performs patch management activities on all relevant systems, devices, firmware, operating systems, applications and other software that process Customer Content. GoTo assesses and scans for system-level, internal and external host/network ("Systems") vulnerabilities, on no less than a monthly basis, as well as after any material change to such Systems and remediates relevant discovered vulnerabilities in accordance with documented policies that prioritize remediation based on risk.

14 Logical Access Control

Logical access control procedures are in place to reduce the risk of unauthorized application access and data loss in corporate and production environments. Employees are granted access to specified GoTo systems, applications, networks and devices based on the "principle of least privilege." User privileges are segregated based on functional role (role-based access control) and environment using segregation of duties controls, processes and/or procedures.

15 Data Segregation

GoTo has implemented controls to prevent Users from seeing the data of other Users. For instance, GoTo leverages a multi-tenant architecture, logically separated at the database level, based on a User's or organization's GoTo account. Parties must be authenticated to gain access to an account.

16 Perimeter Defense and Intrusion Detection

The GoTo 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.

GoTo uses perimeter protection tools, techniques and services in order to protect against unauthorized network traffic entering GoTo's product infrastructure. These include:

- Intrusion detection systems that monitor systems, services, networks and applications for unauthorized access;
- Critical system and configuration file monitoring;
- Web application firewall (WAF) and application-layer DDoS prevention services that proxy GoTo traffic;
- A local application firewall that provides an additional layer of protection against OWASP top ten and other web application vulnerabilities and malicious traffic; and
- Host-based firewalls that filter inbound and outbound connections, including internal connections between GoTo systems.

17 Security Operations and Incident Management

GoTo's Security Operations Center (SOC) is responsible for detecting and responding to security events. The SOC uses security sensors and analysis systems to identify potential issues and has developed incident response procedures, including a documented Incident Response Plan.

GoTo's Incident Response Plan is aligned with GoTo's critical communication processes, policies and standard operating procedures. It is designed to manage, identify and resolve relevant suspected or identified security events across its systems and services, including Central and Pro. The Incident Response Plan sets out mechanisms for employees to report suspected security events and escalation paths to follow when appropriate. Suspected events are documented and escalated as appropriate via standardized event tickets and triaged based upon criticality.

18 Deletion and Return of Content

Deletion and/or Return: Customers may request return and/or deletion of their Customer Content by submitting a request using GoTo's Individual Rights Management Portal ("IRM"), via support.goto.com, or by e-mailing privacy@goto.com. Requests shall be processed within thirty (30) days of receipt by GoTo, however, in the unlikely event we need more time, we will provide notice as soon as possible of any anticipated delayed and revised completion deadline.

Customer Content Retention Schedule: Unless otherwise required by applicable law, Customer Content shall automatically be deleted ninety (90) days after 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.

19 Organizational Controls

19.1. Security Policies and Procedures

GoTo maintains a comprehensive set of security policies and procedures that are periodically reviewed and updated as necessary to support GoTo's security objectives, changes in applicable law, industry standards and compliance efforts.

19.2. Change Management

GoTo maintains a suitable change management process and changes to GoTo Systems are assessed, tested and approved before implementation to reduce the risk of disruption to GoTo services.

19.3. Security Awareness and Training Programs

GoTo's privacy and security awareness program involves training employees about the importance of handling Personal Data and confidential information ethically, responsibly, in compliance with applicable law, and with due care. Newly hired employees, contractors and interns are informed of security policies and the GoTo Code of Conduct and Business Ethics during onboarding. GoTo Employees complete privacy and security awareness training at least annually. Awareness activities take place throughout the year and can include campaigns for Data Privacy Day, Cybersecurity Awareness Month, webinars with the Chief Information Security Officer and a security champions program.

Where appropriate, employees may also be required to complete role-specific trainings. Additionally, all GoTo employees, contractors and subsidiaries must review and adhere to GoTo's policies related to security and data protection.

20 Privacy Practices

GoTo takes the privacy of our Customers, Users and other individuals who use GoTo services ("End Users") very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

20.1. Privacy Program

GoTo maintains a comprehensive privacy program that involves coordination from multiple functions within the company, including Privacy, Security, Governance, Risk and Compliance (GRC), Legal, Product, Engineering and Marketing. This privacy program is centered around compliance efforts and involves the implementation and maintenance of internal and external policies, standards and addenda to govern the company's practices.

20.2. Regulatory Compliance

20.2.1. GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law regarding data protection and privacy for individuals within the EU. GoTo maintains a comprehensive GDPR compliance program and to the extent GoTo engages in processing of Personal Data subject to the GDPR on behalf of the Customer, we will do so in accordance with the applicable requirements of the GDPR. For more information, visit https://www.goto.com/company/trust/privacy.

20.2.2. CCPA

The California Consumer Privacy Act, as amended by the California Privacy Rights Act (collectively referred to as "CCPA") grants Californians additional rights and protections regarding how businesses may use their personal information. GoTo maintains a comprehensive compliance program and to the extent GoTo engages in processing of Personal Data subject to the CCPA on behalf of the Customer, we will do so in accordance with the applicable requirements of the CCPA. For more information about our compliance with the CCPA, see GoTo's Privacy Policy and Supplemental California Consumer Privacy Act Disclosures.

20.2.3. LGPD

The Brazilian Data Protection Law (LGPD) regulates the processing of Personal Data in Brazil and/or of individuals located in Brazil at the time of collection. GoTo maintains a comprehensive compliance program and to the extent GoTo engages in processing of Personal Data subject to the LGPD on behalf of the Customer, we will do so in accordance with the applicable requirements of the LGPD. For more information, visit https://www.goto.com/company/trust/privacy.

20.3. Data Processing Addendum

GoTo offers a global Data Processing Addendum (DPA), available in English and German. This DPA meets the requirements for GDPR, CCPA and other applicable regulations and governs GoTo's processing of Customer Content.

Specifically, our DPA incorporates several GDPR-focused data privacy protections, including:

(a) data processing details and sub-processor disclosures as required under Article 28;
(b) revised (2021) Standard Contractual Clauses (a.k.a., the EU Model Clauses); and
(c) GoTo's product-specific technical and organizational measures.

Additionally, to account for CCPA requirements, our global DPA includes:

(a) revised definitions mapped to the CCPA;
(b) access and deletion rights; and
(c) warranties that GoTo will not sell our Customer's, Users' and End Users' personal information.

Our global DPA also includes provisions to:

(a) address GoTo's compliance with the LGPD;
(b) support lawful transfers of Personal Data to/from Brazil; and
(c) ensure that our Users enjoy the same privacy benefits as our other global Users.

20.4 Transfer Frameworks

GoTo supports lawful international data transfers under the following frameworks:

20.4.1 Standard Contractual Clauses

The Standard Contractual Clauses (SCCs), sometimes referred to as EU Model Clauses, are standardized contractual terms, recognized and adopted by the European Commission, to ensure that any Personal Data leaving the European Economic Area (EEA) will be transferred in compliance with EU data protection law. The SCCs, revised and issued in 2021, are incorporated in GoTo's global DPA to enable GoTo Customers to transfer data out of the EEA in compliance with the GDPR.

20.4.2 APEC CBPR and PRP Certifications

GoTo has obtained Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) certifications. The APEC CBPR and PRP frameworks are the first data regulation frameworks approved for the transfer of Personal Data between APEC-member countries and were obtained and independently validated through TrustArc, an APEC-approved third-party data protection compliance vendor

20.5 Supplemental Measures

In addition to the measures specified in these TOMs, GoTo has created an FAQ designed to outline the supplemental measures implemented to support lawful transfers under Chapter 5 of the GDPR and address and guide any case-by-case analyses recommended by the European Court of Justice in conjunction with use of the SCCs.

20.6 Data Requests

GoTo maintains comprehensive processes to facilitate receiving data protection and security-related requests, including the IRM portal, Privacy email address (privacy@goto.com) and Customer support at https://support.goto.com.

20.7 Sub-Processor and Data Center Disclosures

GoTo publishes Sub-Processor Disclosures on its Trust & Privacy Center (https://www.goto.com/company/trust/resource-center). These disclosures specify the names, locations and processing purposes of data hosting providers and other third parties that process Customer Content as a part of providing the Service to GoTo Customers.

20.8 Sensitive Data Processing Restrictions

Unless expressly requested by GoTo or Customer has otherwise received written permission from GoTo, the following types of sensitive data must not be uploaded or otherwise provided to GoTo:

- 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) as identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA), as well as other relevant applicable 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 GoTo to collect payment for the Service.
- Any information especially protected by applicable laws and regulation, specifically information about individual's race, ethnicity, religious or political beliefs, organizational memberships, etc.

20.9 Compliance in Regulated Environments

Customers are responsible for implementing appropriate policies, procedures and other safeguards related to their use of GoTo Resolve to support devices in regulated environments.

21 Security and Privacy Third-Party Controls

Prior to engaging third-party vendors that process Customer Content or confidential, sensitive, or employee data, GoTo reviews and analyzes the vendor's security and privacy practices using the appropriate Procurement channels. As appropriate, GoTo may obtain and evaluate compliance documentation or reports from vendors periodically to ensure their control environment and standards continue to be sufficient.

GoTo enters into written agreements with all third-party vendors and either utilizes GoTo-approved procurement templates or negotiates such third parties' standard terms and conditions to meet GoTo-accepted privacy and security standards, where deemed necessary. The Finance, Legal, Privacy and Security teams are involved in the vendor review process and verify that vendors meet specific mandatory data handling and contractual requirements, as necessary and/or appropriate. GoTo's third party risk policies govern privacy and security requirements of vendors on the basis of type and duration of data processing and level of access. Where appropriate (e.g., where Customer Content is processed or stored), agreements with vendors include "compliance with applicable law" requirements, a DPA or similar document that addresses topics such as GDPR, CCPA, LGPD and use and sale restrictions, as appropriate. For instance, GoTo's Supplier DPA has restrictions around data "selling" as defined under the CCPA. Similarly, security addenda with suitable controls and systems requirements are put in place with relevant vendors.

22 Contacting GoTo

Customers can contact GoTo at support.goto.com for general inquiries. For questions or requests related to data protection or security, please visit our IRM portal or send an email to privacy@goto.com.