Technical and Organizational Measures
GoToAssist Corporate

Executive Summary

This Technical and Organizational Measures (TOMs) document outlines GoTo's commitments to privacy, security, and accountability for GoTo Assist Corporate. 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.
- **Compliance Audits:** GoToAssist Corporate 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, 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/CPRA 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**:
  - GoToAssist Corporate 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) 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 GoToAssist Corporate, a hosted service designed to enable multi-agent support teams to deliver live remote technical assistance to corporate users of Windows-based and Mac computers. GoToAssist Corporate is customizable to a company's unique environment and features advanced administrative, collaborative, and customer-queuing features, including team collaboration, session transfer, customer surveys, and session recording.

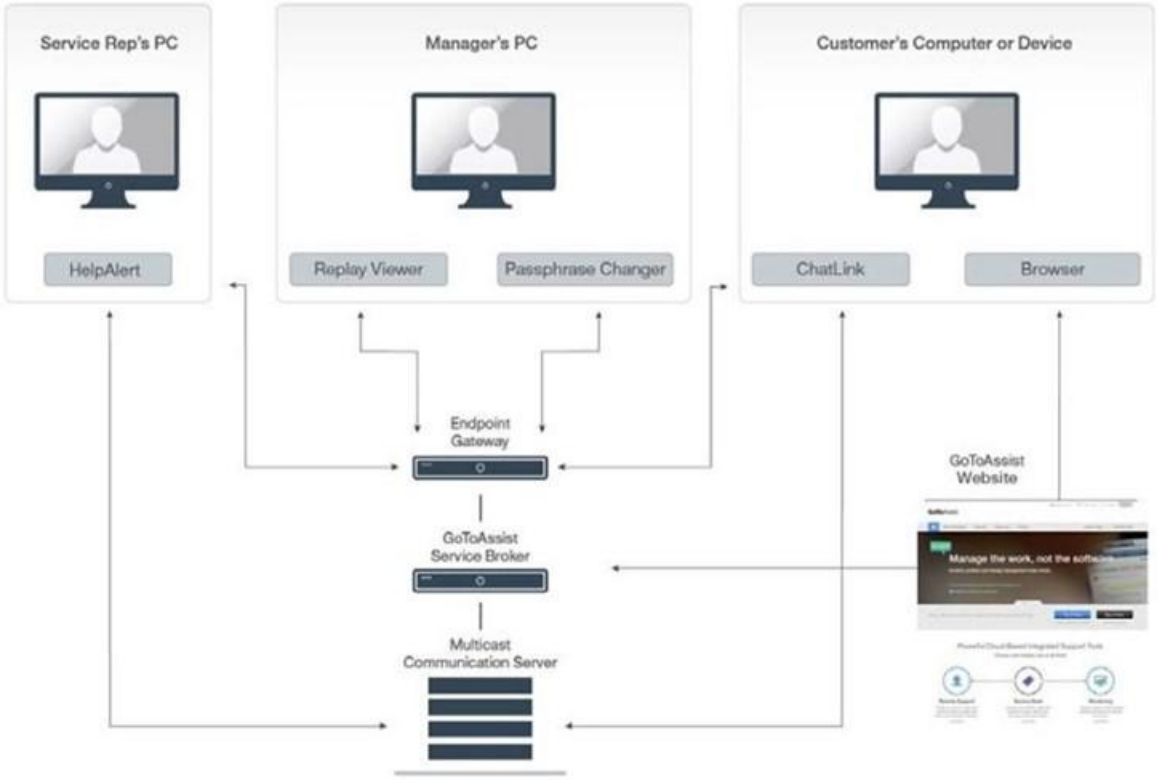
2 Product Architecture

GoToAssist Corporate 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 performance, reliability and scalability. Redundant switches and routers are built into the architecture which is designed to ensure that there is no single point of failure. High-capacity, clustered servers and backup systems are intended to ensure 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 in order to ensure performance.

The web, application, communication and database servers are housed in secure cloud hosting provider datacenters featuring redundant power and environmental controls. Physical access to servers is tightly restricted and continuously monitored. Firewall, router and VPN based access controls are employed to secure our private-service networks and backend servers. Infrastructure security is continuously monitored, and vulnerability testing is conducted regularly by internal staff and outside third-party auditors. Cloud providers are responsible for protecting their datacenters in a similar way as colocation datacenters.

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.



GoToAssist Corporate Website - Web application that provides access to the GoToAssist Corporate website and web based internal and external administration portals. The websites are hosted in AWS data centers.

GoToAssist Corporate Service Broker - Web application that realizes GoToAssist Corporate account and service management, persistent storage and reporting functions. Brokers are hosted in AWS data centers.

Endpoint Gateway (EGW) - A special-purpose gateway used by various endpoint applications to securely access the GoToAssist Corporate Service Broker for a variety of purposes using remote procedure calls. EGW are hosted in AWS data centers.

Multicast Communication Servers (MCS) - A fleet of globally distributed servers used to realize a variety of high-availability unicast and multicast communication services. MCS are hosted in Oracle Cloud (OCI).

4.1 Malware Protection

Malware protection software with audit logging is deployed on all GoToAssist Corporate Servers. Alerts indicating potential malicious activity are sent to the appropriate response team.

4.2 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 GoToAssist Corporate include:

- Public-key-based Secure Remote Password (SRP) protocol authentication provides authentication and key establishment between endpoints
- 128-bit AES encryption is used to safeguard session data
- Session keys are generated by endpoints, and are never known to GoTo or its systems
- Communication servers route only encrypted packets and do not have the session encryption key.

4.2.1 In-Transit Encryption

To further safeguard Customer Content while in transit, GoTo uses current Transport Layer Security (TLS) protocols and associated cipher suites to protect many internet protocols. In addition, GoTo uses the latest version of Secure Shell (SSH) for certain administrative functions. Connectivity to internal networks is protected through appropriate Virtual Private Network (VPN) technologies, intended to ensure the confidentiality and integrity of GoTo internal traffic.

4.3 Communication security features

Communication between participants in a GoToAssist Corporate session occurs via an overlay multicast networking stack that logically sits on top of the conventional TCP/IP stack within each user's computer. This network is realized by a collection of Multicast Communication Servers (MCS).

4.4 Communication confidentiality and integrity

GoToAssist Corporate provides additional security measures that are designed to address both passive and active attacks against confidentiality, integrity and availability. Screen-sharing data, keyboard/mouse control data and text chat information are never exposed in unencrypted form while temporarily resident within communication servers or during transmission across public or private networks.

When recording is disabled, the GoToAssist Corporate session key is not sent to the servers in any form. Thus, for example, breaking into a server would not reveal the key for any encrypted stream that a malicious actor may have captured. When recording is enabled, chat, screensharing and screen-viewing data is stored in encrypted form. The session key is also stored, but it is protected with 1024-bit RSA public/private key encryption. A portal specific public key and a customizable passphrase is used to encrypt the session key before storage. As a measure to safeguard session data, session replays require the following: access to the session recording, the encrypted session key and the portal's private key plus the passphrase. Communications security controls based on strong cryptography are implemented at two layers: the "TCP layer" and the "Multicast Packet Security Layer" (MPSL).

4.5 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 customers configure their browsers to use strong cryptography by default whenever possible, and to ensure that operating system and browser security patches are kept up to date.

When TLS connections are established to the website and between GoToAssist Corporate components, GoTo servers authenticate themselves to clients using public key certificates. For added protection against infrastructure attacks, mutual certificate-based authentication is used on all server-to-server links (e.g., MCS-to-MCS or MCS-to-Broker).

4.6 Multicast packet security layer

More features provide an additional layer of encryption for keyboard/mouse control data and text chat information, independent of those provided by TLS. Specifically, all session data is protected by encryption and integrity mechanisms that prevent anyone with access to our communications servers (whether friendly or hostile) from eavesdropping on a session or manipulating data without detection.

This enhanced security measure operates within the TLS layer, providing an extra layer of encryption that ensures our data packets remain unreadable in the event of a TLS inspection like when data flows through Zscaler or similar solution.

Key establishment is accomplished by using a randomly generated 128-bit seed value selected by the GoToAssist Corporate service broker that is distributed to all endpoints over TLS and used as the input to a NIST approved key-derivation function. The seed value is erased from the GoToAssist Corporate service broker memory when the session ends.

Session data is further protected from eavesdropping using 128-bit AES encryption in counter mode. Plaintext data is typically compressed before encryption using proprietary, high-performance techniques to optimize bandwidth. Data integrity protection is accomplished by including an integrity check value currently generated with HMAC-SHA-1. Because of consequent use of robust cryptographic mechanisms, customers can have a high degree of confidence that session data is protected against unauthorized disclosure or undetected modification.

Furthermore, there is no additional cost, performance degradation or usability burden associated with these essential communication security features. High performance and standards-based data security is a built-in feature of every session.

4.7 Vulnerability Management

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.

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 GoTo Assist Corporate is set to a maximum of 2 hours, ensuring that services can be restored within this timeframe following a disruption. The RPO is set to a maximum of 30 minutes 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 data centers.

Hosting locations may vary (i.e., depending on data residency election), for detailed information, please refer to the GoTo Connect 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. Reference to their documentation:

- https://aws.amazon.com/compliance/data-center/controls/
- https://www.oracle.com/corporate/security-practices/corporate/physical-environmental.html

Other than physical security, all cloud providers operate 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 Logical Access Control

Users authorized to access GoToAssist Corporate product components may include GoTo's authorized technical staff (e.g., Technical Operations and Engineering DevOps), customer administrators, or end-users of the product. Cloud-based production components are available through restricted VPN.

7 Customer Content Retention Schedule

Session recordings will be deleted on an ongoing 90-day rolling basis.[1] 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.

8 Revision History

Version	Month/Year	Description
Version 1.3	July 2024	Updated and published by Legal
Version 1.4	December 2025	Standardized the document to include Product Specific sections only.

[1] 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.