Technical and Organizational Measures
GoToAssist Remote Support V4

Executive Summary

This Technical and Organizational Measures (TOMs) document outlines GoTo's commitments to privacy, security, and accountability for GoToAssist Remote Support v4 (GTARSv4). GoTo upholds comprehensive global privacy and security programs, along with organizational, administrative, and technical safeguards designed to:

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

These measures include:

- **Encryption**:
  - *In-Transit* - Transport Layer Security (TLS) v1.2 or higher.
  - *At Rest* - Advanced Encryption Standard (AES) 256-bit for Customer Content.
- **Cloud Provider regions[1]:** United States, Germany and India locations to support redundancy.
- **Compliance Audits:** 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.
- **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 GDPR, CCPA 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 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**:
  - GTARSv4 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 paid subscription term. Recordings are deleted on a rolling basis after ninety (90) days.

[1] Hosting locations may vary (i.e., depending on data residency election), consult the applicable GTARSv4 Sub-Processor Disclosure found in the Product Resources section of the GoTo Trust and Privacy Center (https:/www.goto.com/company/trust/resource-center).

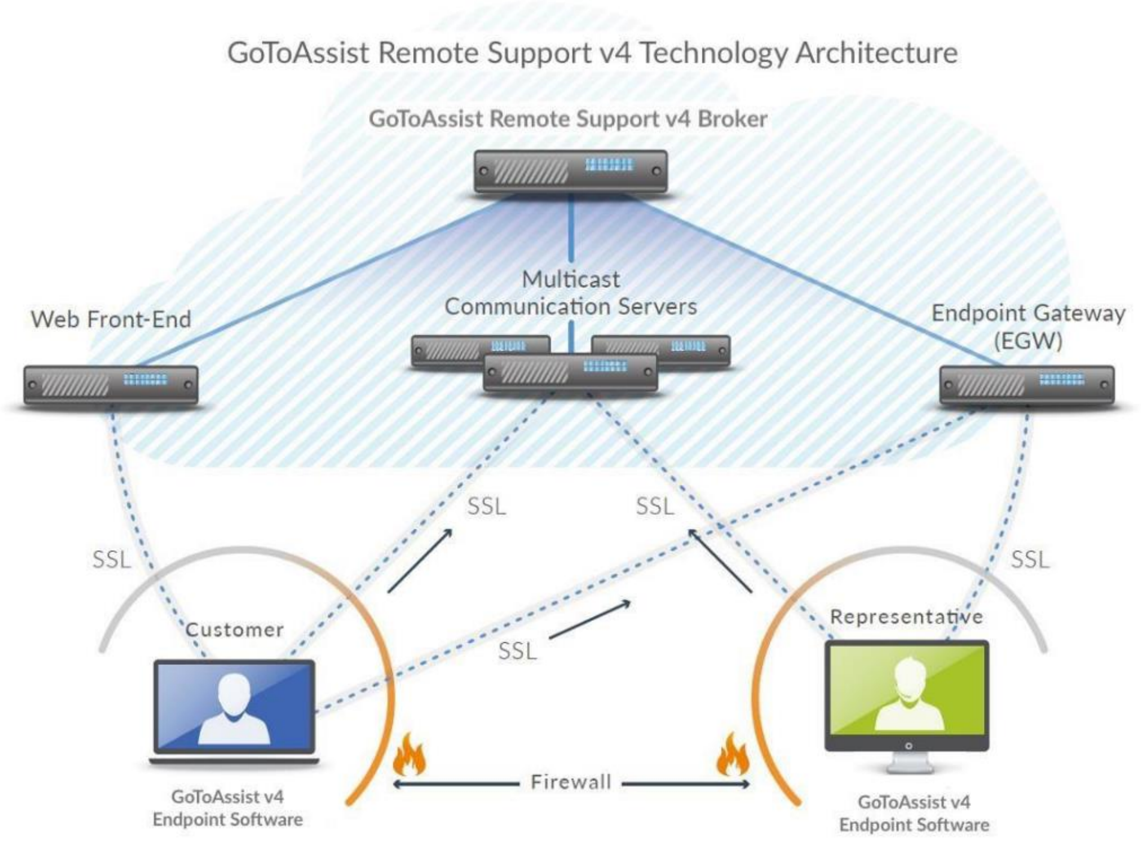
Contents

1 Product Introduction

This document covers the Technical and Organizational Measures (TOMs) for GTARSV4 which is a cloud-based service that enables support professionals to resolve customers' technical issues using screen sharing, mouse and keyboard control and other capabilities. Individual IT professionals or teams can deliver on-demand support or access unattended desktops and servers.

2 Product Architecture

GTARSV4 uses an application service provider (ASP) model designed to provide secure operations while integrating with a company’s existing network and security infrastructure. Its architecture is designed for optimal performance, reliability and scalability. Redundant switches and routers are built into the architecture and intended to ensure that there is no single point of failure. High-capacity, clustered servers and backup systems are utilized to ensure continued operation of application processes in the event of a heavy load or system failure. Service brokers load balance the client/server sessions across geographically distributed communication servers. The communications architecture for GTARSV4 is depicted as follows:


GoToAssist Remote Support v4 Technology Architecture
GoToAssist Remote Support v4 Broker
Web Front-End
Multicast Communication Servers
Endpoint Gateway (EGW)
SSL
SSL
SSL
SSL
SSL
Customer
Representative
Firewall
GoToAssist v4 Endpoint Software
GoToAssist v4 Endpoint Software

The web, application, communication and database servers are housed in secure cloud infrastructure facilities that feature redundant power and environmental controls. Access to servers is tightly restricted and continuously monitored. Firewall, router and Software Defined Parameter (SDP) solution are employed to secure GoTo's private-service networks and backend servers. Infrastructure security is continuously monitored, and vulnerability testing is conducted regularly by internal staff and qualified third-party auditors.

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. This results in the client and the host exchanging TLS keys without the gateway learning the key.

3 Technical Security Controls

GoTo employs industry standard technical 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. Find the Terms of Service at https://www.goto.com/company/legal/terms-and-conditions.

3.1 Malware Protection

Malware protection software, equipped with audit logging capabilities, is deployed across all GTARSV4 servers. Any relevant alerts indicating potential malicious activity are promptly forwarded to the appropriate response team for immediate action.

3.2 Encryption

GoTo maintains a cryptographic standard that aligns with recommendations from industry groups, government publications, and other reputable 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 the GoToAssist Product Suite include:

- Public-key-based SRP authentication provides authentication and key establishment between endpoints.
- GTARSV4 session data is protected with 256-bit AES encryption.
- Session keys are generated server-side by the technician and remain there to be able to connect the customer to the technician. These keys are never exposed or visible to the public.
- Communication servers only route encrypted packets and do not maintain the session encryption key.

3.3 In-Transit Encryption

To further safeguard Customer Content (as the term is defined in the Terms of Service) while in transit, GoTo uses current TLS protocols and associated cipher suites 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 Software-Defined Perimeter technologies, utilized to ensure the confidentiality and integrity of GoTo internal traffic.

GTARSV4 provides data security measures that are designed to address both passive and active attacks against confidentiality, integrity and availability. All Remote Support connections are encrypted and accessible only by authorized support session participants. Screensharing data, keyboard/mouse control data, transferred files, remote diagnostic data and text chat information are encrypted while temporarily residing within GoTo communication servers and during transmission across public or private networks.

Communication security controls based on strong cryptography are implemented at two layers: the Transmission Control Protocol (TCP) layer and the multicast packet security layer (MPSL).

3.4 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 Product Suite 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.

3.5 Multicast packet security layer (MPSL)

Additional features have been implemented to provide complete security for multicast packet data, independent of those provided by TLS. Specifically, all multicast session data is protected by encryption and integrity mechanisms designed to prevent anyone with access to GoTo communication servers (whether friendly or hostile) from eavesdropping on a Remote Support 6 session or manipulating data without detection. Unique to GoTo products, the MPSL provides an added level of communication confidentiality and integrity.

MPSL key establishment is accomplished using a public-key-based Secure Remote Password SRP-6 authenticated key agreement, employing a 1024-bit modulus to establish a wrapping key.

This wrapping key is then used for group symmetric key distribution using the AES Key Wrap Algorithm, IETF RFC 3394. All keying material is generated using a pseudo-random number generator, based on relevant FIPS standards, seeded with entropy collected at run-time from multiple sources on the host machine. These robust, dynamic key generation and exchange methods offer strong protection against key guessing and key cracking. MPSL further protects multicast packet data from eavesdropping using 256-bit AES encryption in Counter Mode. Plaintext data is compressed before encryption using proprietary, high-performance techniques to optimize bandwidth. Data integrity protection is accomplished by including an integrity check value generated with the HMAC-SHA-1 algorithm. GoToAssist Product Suite uses strong, industry-standard cryptographic measures designed to protect multicast support session data against unauthorized disclosure or undetected modification.

4 Data Backup, Disaster Recovery and Availability

GoTo's disaster recovery strategy includes clearly defined Recovery Time Objective (RTO) and Recovery Point Objective (RPO) metrics to ensure minimal disruption. The RTO is set to a maximum of 60 minutes, ensuring that services can be restored within this timeframe following a disruption. The RPO is set to 5 minutes for GTARSv4, 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 redundant, active-active infrastructure in cloud hosting provider data centers. Hosting locations are in the United States, Germany and India.

GTARSv4 stores data only in the United States; in other locations, data is only in transit.

5.1 Cloud hosted workloads

Physical security is the responsibility of the GoTo's cloud providers (e.g. AWS, OCI). 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 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 GoTo uses.

6 Logical Access Control

Users authorized to access GTARSv4 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 managed through restricted Software-Defined Perimeter solution.

7 Customer Content Retention Schedule

Session recordings are deleted on an ongoing 90-day rolling basis.[2] Additionally, unless otherwise required by applicable law, Customer Content shall be deleted automatically for paid accounts 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.

For users with an active subscription only, support session reports are available for up to 12 months.

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

8 Appendix - Terminology

Attended Session: support session where the Customer is present during the session and can participate in it.

Customer: person receiving technical support from the Expert via a GTARSV4 Session.

Customer Desktop App: desktop application that runs on the Customer's computer (Windows or Mac) and connects to a GTARSV4 Session through the GTARSV4 Service. It provides remote control capability as well as other advanced functionalities and the ability to install Unattended App on the Customer's computer.

Customer Endpoint: collective term referring to any customer endpoint: Customer Web App, Customer Desktop App, Customer Mobile App, Unattended Customer App.

Customer Mobile App: mobile application (Android only) that runs on the Customer's mobile/tablet device and can connect to a GTARSV4 Session through the GTARSV4 Service. It provides remote view and remote-control capabilities.

Expert: GTARSV4 user, who creates GTARSV4 Sessions in order to provide technical assistance to Customers via remote view, remote control or camera share.

Expert Desktop App: desktop application that runs on MacOS and Windows computers and connects to the GTARSV4 Service.

Expert Mobile App: mobile application (Android and iOS) used by an Expert, that connects to the GTARSV4 Service.

GTARSV4 Sessions: attended chat, remote view, remote control or camera share and unattended remote control.

GTARSV4 Service: a fleet of load-balanced, globally distributed servers providing secure access for the GoToAssist Expert Desktop App and Customer Endpoints through encrypted web-socket connection and API calls.

Unattended Customer App: installable desktop application (Windows and Mac) that runs in the background on the Customer's computer. It can download and execute a Customer Desktop App to connect to an authorized Unattended Session.

Unattended Session: support session where the Customer is not present. The session is initiated and established by the Expert without Customer involvement through an authorized Unattended Customer App.