Technical and Organizational Measures
GoTo Assist Remote Support v5

Executive Summary

This Technical and Organizational Measures (TOMs) document outlines GoTo's commitments to privacy, security, and accountability for GoToAssist Remote Support v5 (GTARSv5). 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 locations to support redundancy.
- **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.
- **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 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**:
  - GoTo Assist Remote Support v5 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.
  - Recordings are deleted on a rolling basis after three hundred and sixty-five (365) days.

[1] Hosting locations may vary (i.e., depending on data residency election), consult the applicable GTARSv5 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

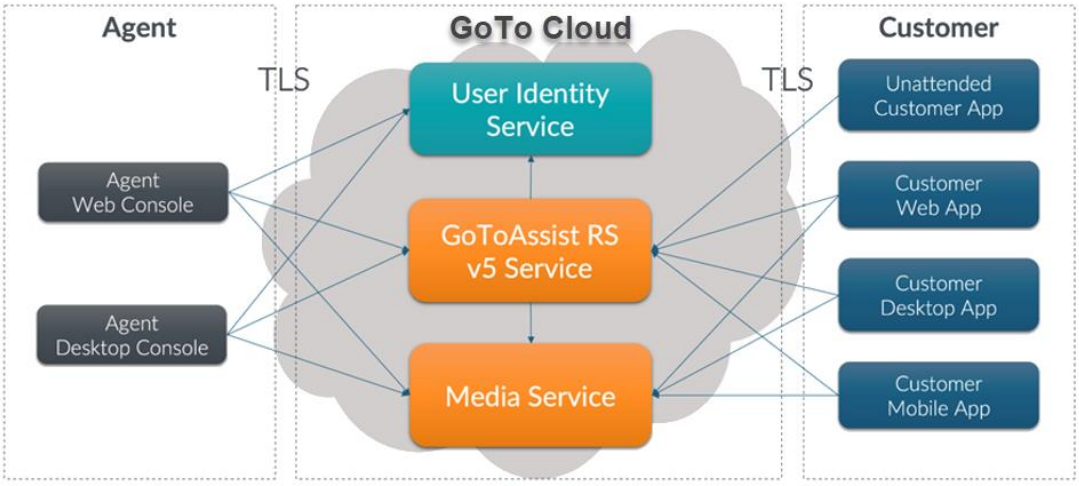
This document covers the Technical and Organizational Measures (TOMs) for **GoToAssist Remote Support V5** (formerly known as RescueAssist) which enables IT and support professionals to deliver remote support to computers, servers and mobile devices with remote view, remote control or camera share from a web-based or desktop agent console. GoToAssist Remote Support V5 employs robust data security measures to defend against both passive and active attacks.

2 Product Architecture

GoToAssist Remote Support V5 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 GoToAssist Remote Support V5 is depicted in Section 2.1 below.

2.1 Communications Architecture

The GoToAssist Remote Support V5 communications architecture is summarized in the figure below.



Agent authentication utilizes the GoTo User Identity Service. Communication between participants in a GoToAssist Remote Support V5 Session occurs via an overlay networking stack that logically sits on top of the conventional UDP and TCP/IP. This

network is provided by GoToAssist Remote Support V5's Service and Media Service hosted in Amazon AWS.

GoToAssist Remote Support V5 session participants (Agent Web Console, Agent Desktop Console and Customer Endpoints) communicate with GoToAssist Remote Support V5 Service and Media Service using outbound TCP connections on port 443 or UDP port 15000, depending on availability. Because GoToAssist Remote Support V5 is a web-based service, participants can be located nearly anywhere on the Internet — at a remote office, at home, at a business center or connected to another company's network.

2.2 Agent Desktop console

The agents can use the Agent Web Console or the installable Agent Desktop Console to connect to the GoToAssist Remote Support V5 Service. The Desktop Console uses the cross-platform Qt toolkit to run on MacOS and Windows and leverages the open-source Chromium web browser to utilize components of the Web Console.

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. Find the Terms of Service at https://www.goto.com/company/legal/terms-and-conditions.

3.1 Authentication

GoToAssist Remote Support V5 Agents and Account Administrators are identified by their email address and authenticated using a password. During authorized authentication, the password is never transferred in an unencrypted state.

Authentication procedures are governed by the following policies:

- **Strong passwords:** A strong password must be a minimum of 8 characters in length with sufficient complexity requirements (i.e., must contain both letters and numbers). Passwords are checked for strength when established or changed.
- **Two-Factor Authentication:** As an additional security measure, optional two-factor authentication is available for every GoToAssist Remote Support V5 company account. If enabled, two-factor authentication requires every user to authorize access via two separate methods.
- **Account lockout:** After five consecutive failed log-in attempts, the user account is put into a mandatory soft-lockout state. This means that the user account holder will not be able to log-in for five minutes. After the lockout period expires, the user account holder will be able to attempt to log-in to his or her account again.

3.2 Permission Based Access Control

3.2.1 Attended Session

An essential part of GoToAssist Remote Support V5's security is its permission-based access control model designed to protect access to the Customer's computer and data. During customer-attended live support sessions, the customer is prompted for permission before initiation of any screen sharing, remote control or transfer of files.

Once remote control and screen sharing have been authorized during an Attended Session, the Customer can watch what the Agent does at all times. Further, the service is designed to allow the Customer to easily take back control or terminate the session at any time.

3.2.2 Unattended Session

Unattended support requires the Unattended Customer App to be installed on the Customer's device. It can be set up in one of two ways — either In-Session Setup (during an Attended Session) or using an Out-of-Session Installer, both of which require Customer approval.

In-Session Setup: once the Customer and Agent have entered an Attended Session, the Agent may request extra permission to install the Unattended Customer App. The Customer is prompted for approval and must give explicit authorization.

Out-of-Session Installer: After securely logging in to the GoToAssist Remote Support V5 website or desktop application, the Agent can download an installer, which allows installation of the Unattended Customer App on any Windows PC or Mac for which the Agent has administrator access.

3.2.3 In-Session Security

GoToAssist Remote Support V5 is not designed to override local security controls on the Customer's computer.

Specifically, if the Customer returns to the machine while an Unattended Session is in progress, they may, at any time, end the session and can permanently revoke the Agent 's unattended support privileges.

3.3 Role Based Access Control

GoToAssist Remote Support V5 provides access to a variety of resources and services using a role-based access control system that is enforced by the various service delivery components. The following roles are defined:

- **Account Administrator**: GoToAssist Remote Support V5 user with full administrator privileges to perform administrative functions pertaining to Agents. Account administrators can create, modify and delete Agent accounts and modify subscription data.
- **Agent**: GoToAssist Remote Support V5 user. The agent can initiate GoToAssist Remote Support V5 Sessions in order to provide technical assistance to Customers via remote view, remote control or camera share.

- **Customer**: Unauthenticated person requesting support from the Agent. The Customer can close sessions and must grant permissions for the Agent to access their device.

3.4 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 GoToAssist Remote Support V5 include:

- GoToAssist Remote Support V5 session data is protected with TLS 1.3 or TLS 1.2 (if supported) 256-bit AES encryption in transit.
- Session keys are generated server-side by the agent and remain there to be able to connect the customer to the agent. The service is designed to ensure that these keys are never exposed or visible to the public.
- Encrypted communication between the customer and the agent in GoToAssist Remote Support V5 occurs via a custom media service solution.
- Endpoints within the GoToAssist Remote Support V5 infrastructure use Transport Layer Security (TLS) connections.

3.5 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. Customer Endpoint and backend communication are encrypted via OpenSSL. Communications security controls based on strong cryptography are implemented on the TCP layer via TLS standard solutions.

Strong authentication measures are utilized in order to help reduce the likelihood of would-be attackers masquerading as infrastructure servers or inserting themselves into the middle of support session communications.

To provide protection against eavesdropping, modification or replay attacks, IETF-standard TLS protocols are used to protect all communication between endpoints and our services. Screen-sharing data, keyboard/mouse control data, transferred files, remote diagnostic data and text chat information are encrypted in transit with TLS 1.3 or TLS 1.2 (2048-bit RSA, AES-256 strong encryption ciphers with 384-bit SHA-2 algorithm).

In order to ensure appropriate compatibility and security balance, the GoToAssist Remote Support V5 service also supports inbound connections using most supported TLS cipher suites in TLS 1.3 or TLS 1.2.

GoTo also advises that agents configure their browsers to use strong cryptography by default whenever possible, in order to increase technical safeguards on the agents' machine, and to always install the latest operating system and browser security patches.

When connections are established to the GoToAssist Remote Support V5 website and between GoToAssist Remote Support V5 components, GoTo servers authenticate

themselves to clients using DigiCert public key certificates. Server-to-server APIs are accessible only within GoTo's private network behind robust firewalls.

3.6 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.

3.7 Customer Endpoint Protection

Customer Desktop Apps and Unattended Customer Apps must be compatible with a wide variety of desktop environments. GoToAssist Remote Support V5 accomplishes this using an executable download that employs strong cryptographic measures.

The Customer Desktop Apps and Unattended Customer Apps are downloaded to customer PCs as a digitally signed installer. This helps protect the Customer from inadvertently installing a Trojan or other malware posing as GoToAssist Remote Support V5 software.

The endpoint software is composed of several digitally signed executables and dynamically linked libraries. GoTo follows appropriate quality control and configuration management procedures during development and deployment to enhance software safety.

3.8 Logging and Alerting

GoTo collects identified anomalous or suspicious traffic into relevant security logs in applicable production systems.

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, or if there is a full restore needed that depends on the DB size, ensuring that services can be restored within this timeframe following a disruption. The RPO is set to less than 5 minutes for GTARSv5 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-passive infrastructure in cloud hosting provider data centers. Hosting locations are United States and Germany.

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/

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 Logical Access Control

Users authorized to access GTARSv5 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

Customer Content Retention Schedule: Session recordings will be deleted on an ongoing 365-day rolling basis.[2] Additionally, unless otherwise required by applicable law, Customer Content shall automatically be deleted.

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

[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

Agent: GoToAssist Remote Support V5 user, who creates GoToAssist Remote Support V5 Sessions in order to provide technical assistance to Customers via remote view, remote control or camera share.

Agent Web Console: web application that runs on the Agent's PC, Mac, Tablet or Chromebook devices in any of the supported browsers (Chrome, Firefox, Safari) and connects to the GoToAssist Remote Support V5 Service. It enables the Agent to create and conduct GoToAssist Remote Support V5 sessions as well as various account management, service management and reporting functions.

Agent Desktop Console: desktop application that runs on MacOS and Windows computers and connects to the GoToAssist Remote Support V5 Service and leverages the GoToAssist Remote Support V5 Agent Web Console technology, Qt and the Chromium web engine. Provides the same functionality as the Agent Web Console but in a native look and feel.

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

Customer: person receiving technical support from the Agent via a GoToAssist Remote Support V5 Session.

Customer Desktop App: desktop application that runs on the Customer's computer (Windows or Mac) and connects to a GoToAssist Remote Support V5 Session through the GoToAssist Remote Support V5 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 and iOS) that runs on the Customer's mobile/tablet device and can connect to a GoToAssist Remote Support V5 Session through the GoToAssist Remote Support V5 Service. It provides remote view (Android and iOS) and remote control (Android only) capabilities.

Customer Web App: web application that runs in any supported browser on the Customer's computer/mobile device and connects to a GoToAssist Remote Support V5 Session through the GoToAssist Remote Support V5 Service. It can provide chat, remote view and camera share capabilities as well as the possibility to elevate the session anytime to remote control by downloading the Customer Desktop App or installing the Customer Mobile App.

Media Service: a fleet of load-balanced, globally distributed servers providing a variety of high-availability unicast and multicast communication services based on WebRTC protocols.
GoToAssist Remote Support V5 Sessions: attended chat, remote view, remote control or camera share and unattended remote control.

GoToAssist Remote Support V5 Service: a fleet of load-balanced, globally distributed servers providing secure access for the Agent Web Console 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 Agent without Customer involvement through an authorized Unattended Customer App.