TECHNICAL AND ORGANIZATIONAL MEASURES FOR GOTOASSIST REMOTE SUPPORT V4 (INCL. SERVICEDESK AND SEEIT)

SECURITY AND PRIVACY OPERATIONAL CONTROLS

Publication date: February 2022

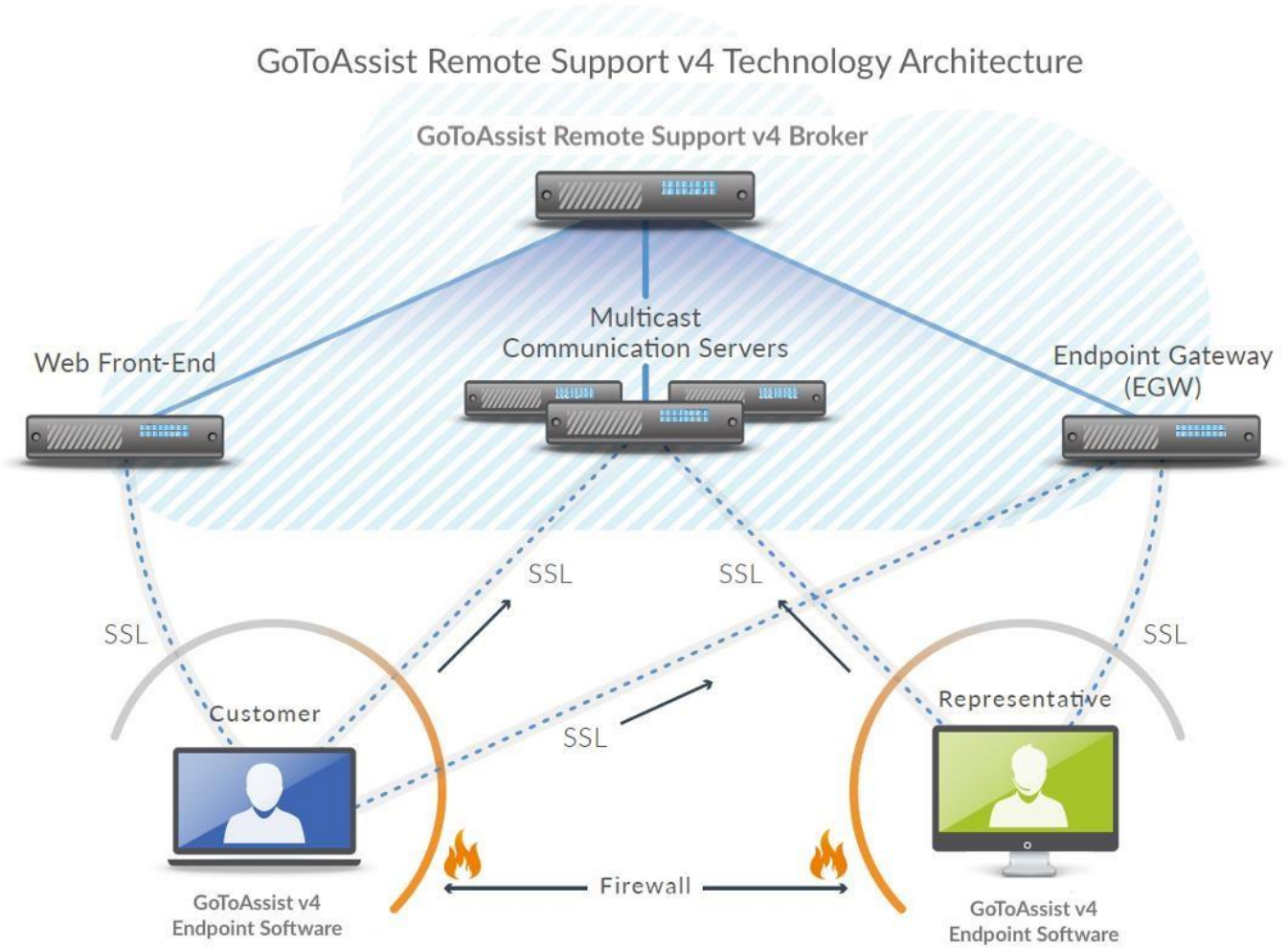
1 Products and Services

This document covers the Technical and Organizational Measures (TOMs) for GoToAssist Remote Support v4, GoToAssist Service Desk and GoToAssist Seeit (collectively referred to as the GoToAssist Remote Support v4).

- **GoToAssist Remote Support v4** 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.
- **GoToAssist Service Desk** is a cloud-based IT services application for incident, problem, change, release and configuration management. Service Desk integrates with GoToAssist Remote Support v4 via Service Desk ticket.
- **GoToAssist Seeit** allows customers to stream their mobile device cameras to a remote agent, allowing the remote agent to view problematic hardware such as a misconfigured router or a damaged automotive component.

2 Product Architecture

GoToAssist Remote Support v4 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 in order 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 v4 is depicted as follows:



The web, application, communication and database servers are housed in secure co-location datacenters that feature 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 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 in order 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 GoToAssist Corporate 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. Logical Access Control

Logical access control procedures are in place, designed to prevent or mitigate the threats of unauthorized application access and data loss in corporate and production environments. Employees are granted minimum (or "least privilege") access to specified GoTo systems, applications, networks, and devices as needed. Further, user privileges are segregated based on functional role and environment.

Users authorized to access GoToAssist product components may include GoTo's technical staff (e.g., Technical Operations and Engineering DevOps), customer administrators, or end-users of the product. On-premise production servers are only available from jump hosts or through the Operations virtual private network (VPN) and both are protected by multi-factor authentication (MFA). Cloud-based production components are available through SSU (Self Service Unix) authentication.

3.2. Perimeter Defense and Intrusion Detection

GoTo employs industry standard perimeter protection tools, techniques and services that are designed to prevent unauthorized network traffic from entering its product infrastructure. The GoTo network features externally facing firewalls and internal network segmentation. Cloud resources also utilize host-based firewalls. In addition, a third party, cloud-based distributed denial of service (DDoS) prevention service is used to protect against volumetric DDoS attacks; this service is tested at least once per year. These controls are designed to protect critical system files against malicious and unintended infection or destruction.

3.3. Data Segregation

GoTo leverages a multi-tenant architecture, logically separated at the database level, based on a user's or organization's GoTo account. Only authenticated parties are granted access to relevant accounts.

3.4. Physical Security

GoTo contracts with datacenters to provide physical security and environmental controls for server rooms that house production servers. These controls include:

- Video surveillance and recording
- Multi-factor authentication to highly sensitive areas
- Heating, ventilation and air conditioning temperature control
- Fire suppression and smoke detectors
- Uninterruptible power supply (UPS)
- 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 datacenter
- Scheduled maintenance and validation of all critical security and environmental controls

GoTo limits physical access to production datacenters to authorized individuals only. Access to an on-premises 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 Technical Operations. GoTo management reviews physical access logs to datacenters and server rooms on at least a quarterly basis. Additionally, physical access to datacenters is removed upon termination of previously authorized personnel.

3.5. Data Backup, Disaster Recovery and Availability

GoTo's architecture is generally 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 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.

3.6. Malware Protection

Malware protection software with audit logging is deployed on all GoToAssist Remote Support v4 servers. Relevant alerts indicating potential malicious activity are sent to an appropriate response team.

3.7. 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:

<u>GoToAssist Remote Support v4</u>

- Public-key-based SRP authentication provides authentication and key establishment between endpoints.
- GoToAssist Remote Support v4 session data is protected with 128-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.

<u>GoToAssist Seeit</u>

- Endpoints within the Seeit infrastructure use SSL connections.

- Seeit sessions are encrypted at the database-level with AES-256.
- Encrypted communication between the user and the technician in Seeit occurs via the OpenTok WebRTC stack.

GoToAssist Service Desk

- Communicates with the browser using Transport Layer Security (TLS) and 256-bit Advanced Encryption Standard (AES) encryption.

3.7.1. 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 Virtual Private Network (VPN) technologies, utilized to ensure the confidentiality and integrity of GoTo internal traffic.

GoToAssist Remote Support v4 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. Screen-sharing data, keyboard/mouse control data, transferred files, remote diagnostic data and text chat information are encrypted while temporarily resident 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).

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.

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 architected to prevent anyone with access to GoTo communication servers (whether friendly or hostile) from eavesdropping on a Remote Support

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 128-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.

3.8. 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, predicated on the criticality of any identified vulnerabilities, remediation action is taken.

GoTo communicates and manages vulnerabilities by providing monthly reports to development teams and management.

3.9. Logging and Alerting

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

4 Organizational Controls

GoTo maintains a comprehensive set of organizational and administrative controls to protect the security and privacy posture of the GoToAssist Product Suite.

4.1. Security Policies and Procedures

GoTo maintains a comprehensive set of security policies and procedures aligned with business goals, compliance programs, and overall corporate governance. These policies and procedures are periodically reviewed and updated as necessary to ensure ongoing compliance.

4.2. Standards Compliance

GoTo complies with applicable legal, financial, data privacy, and regulatory requirements, and conforms with the following compliance certification(s) and external audit report(s):

- 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.
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 2 Type II attestation report incl. BSI Cloud Computing Catalogue (C5)
- American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC) 3 Type II attestation report
- 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

4.3. Security Operations and Incident Management

GoTo's Security Operations Center (SOC) is staffed by the Security Operations team and is responsible for detecting and responding to security events. The SOC uses security sensors and analysis systems to identify potential issues and has developed an Incident Response Plan that dictates appropriate responses.

The Incident Response Plan is aligned with GoTo's critical communication processes, the Information Security Incident Management Policy, as well as associated standard operating procedures. These policies and procedures are designed to manage, identify and resolve suspected or identified security events across GoTo systems and Services, including the GoToAssist Product Suite. Per the Incident Response Plan, technical personnel are in place to identify potential information security-related events and vulnerabilities and to escalate any suspected or confirmed events to management, where appropriate. Employees can report security incidents via email, phone and/or ticket, according to the process documented on the GoTo intranet site. All identified or suspected events are documented and escalated via standardized event tickets and triaged based upon criticality.

4.4. Application Security

GoTo's application security program is based on the Microsoft Security Development Lifecycle (SDL) to secure product code. The core elements of this program are manual code reviews, threat modeling, static code analysis, dynamic analysis, and system hardening.

4.5. Personnel Security

Background checks, to the extent permitted by applicable law and as appropriate for the position, are performed globally on new employees prior to the date of hire. Results are maintained within an employee's job record. Background check criteria will vary depending upon the laws, job responsibility and leadership level of the potential employee and are subject to the common and acceptable practices of the applicable country.

4.6. Security Awareness and Training Programs

New hires are informed of security policies and the GoTo Code of Conduct and Business Ethics at orientation. This mandatory annual security and privacy training is provided to relevant personnel and managed by Talent Development with support from the Security Team.

GoTo employees and temporary workers are informed regularly about security and privacy guidelines, procedures, policies and standards through various mediums including new hire onboarding kits, awareness campaigns, webinars with the CISO, a security champion program, and the display of posters and other collateral, rotated at least bi-annually, that illustrate methods for securing data, devices, and facilities.

5 Privacy Practices

GoTo takes the privacy of its Customers, which for the purposes of this Section 5 is the subscriber to the GoTo Services, and end-users very seriously and is committed to disclosing relevant data handling and management practices in an open and transparent manner.

5.1. GDPR

The General Data Protection Regulation (GDPR) is a European Union (EU) law on data protection and privacy for individuals within the European Union. GDPR aims primarily to give control to its citizens and residents over their personal data and to simplify the regulatory environment across the EU. GoToAssist Remote Support v4 is compliant with the applicable provisions of GDPR. For more information, please visit https://www.goto.com/company/trust/privacy.

5.2. CCPA

GoTo hereby represents and warrants that it is in compliance with the California Consumer Privacy Act (CCPA). For more information, please visit https://www.goto.com/company/trust/privacy.

5.3. Data Protection and Privacy Policy

GoTo is pleased to offer a comprehensive, global Data Processing Addendum (DPA), available in English and German, to meet the requirements of the GDPR, CCPA, and beyond and which governs GoTo's processing of Personal Data.

Specifically, our DPA incorporates several GDPR-focused data privacy protections, including: (a) data processing details, sub-processor disclosures, etc. as required under Article 28; (b) EU Standard Contractual Clauses (also known as the EU Model Clauses); and (c) inclusion of GoTo's technical and organizational measures. Additionally, to account for CCPA coming into force, we have updated our global DPA to include: (a) revised definitions which are mapped to CCPA; (b) access and deletion rights; and (c) warranties that GoTo will not sell our users' 'personal information.'

For visitors to our webpages, GoTo discloses the types of information it collects and uses to provide, maintain, enhance, and secure its Services in its Privacy Policy on the public website.

The company may, from time to time, update the Privacy Policy to reflect changes to its information practices and/or changes in applicable law, but will provide notice on its website for any material changes prior to any such change taking effect.

5.4. Transfer Frameworks

GoTo has a robust global data protection program which takes into account applicable law and supports lawful international transfers under the following frameworks:

5.4.1. Standard Contractual Clauses

The Standard Contractual Clauses (or “SCCs”) are standardized contractual terms, recognized and adopted by the European Commission, whose primary purpose are to ensure that any personal data leaving the European Economic Area (“EEA”) will be transferred in compliance with EU data-protection law. GoTo has invested in a world-class data privacy program designed to meet the exacting requirements of the SCCs for the transfer of personal data. GoTo offers customers SCCs, sometimes referred to as EU Model Clauses, that make specific guarantees around transfers of personal data for in-scope GoTo services as part of our global DPA. Execution of the SCCs helps ensure that GoTo customers can freely move data from the EEA to the rest of the world.

Supplemental Measures

In addition to the measures specified in these TOMs, GoTo has created the following FAQ designed to outline its supplemental measures utilized 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 the SCCs.

5.4.2. APEC CBPR and PRP Certifications

GoTo has additionally 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 across APEC-member countries and were obtained and independently validated through TrustArc, an APEC-approved third-party leader in data protection compliance.

5.5. Return and Deletion of Customer Content

At any time, GoToAssist Remote Support v4 or Service Desk Customers may request the return or deletion of their Content through standardized interfaces. If these interfaces are not available or GoTo is otherwise unable to complete the request, GoTo will make a commercially reasonable effort to support the Customer, subject to technical feasibility, in the retrieval or deletion of their Content. Customer Content for GoToAssist Remote Support v4 or Service Desk will be deleted within thirty (30) days of Customer request. Customers’ GoToAssist Remote Support v4 or Service Desk Content shall automatically be deleted within ninety (90) days after the expiration or termination of their final subscription term. Customers’ GoToAssist Seeit Content is deleted within 72 hours after a session ends. Upon written request, GoTo will certify to such Content deletion.

5.6. Sensitive Data

While GoTo aims to protect all Customer Content, regulatory and contractual limitations require us to restrict the use of GoToAssist Corporate for certain types of information. Unless Customer has written permission from GoTo, the following data must not be uploaded or generated to GoToAssist Corporate:

- 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) identified in the U.S. Health Insurance Portability and Accountability Act (HIPAA) and related 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 GoToAssist Corporate
- Any information especially protected by applicable laws and regulation, specifically information about individual's race, ethnicity, religious or political beliefs, organizational memberships, etc.

5.7. Tracking and Analytics

GoTo is continuously improving its websites and products using third-party web analytics tools which help GoTo understand how visitors use its websites, desktop tools, and mobile applications, as well as user preferences and problems. For further details please reference the Privacy Policy.

6 Third Parties

6.1. Use of Third Parties

As part of the internal assessment and processes related to vendors and third parties, vendor evaluations may be performed by multiple teams depending upon relevancy and applicability. The Security team evaluates relevant vendors that provide information security-based services including the evaluation of third-party hosting facilities. GoTo's Legal and Procurement teams may evaluate contracts, Statements of Work (SOW) and service agreements, as necessary per internal processes. Appropriate compliance documentation or reports may be obtained and evaluated at least annually, as deemed appropriate, to ensure the control environment is functioning adequately and any necessary user consideration controls are addressed. In addition, third parties that host or that are granted access to sensitive or confidential data by GoTo are required to sign a written contract outlining the relevant requirements for access to, or storage or handling of, the information (as applicable).

6.2. Contract Practices

To ensure business continuity and that appropriate measures are in place, intended to protect the confidentiality and integrity of third-party business processes and data processing, GoTo reviews relevant third parties' terms and conditions and either utilizes GoTo-approved procurement templates or negotiates such third-party terms, where deemed necessary.

7 Contacting GoTo

Customers can contact GoTo at https://support.goto.com for general inquiries or privacy@goto.com for privacy-related questions.

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 GoToAssist Remote Support V4 Session.

Customer Desktop App: desktop application that runs on the Customer's computer (Windows or Mac) and connects to a GoToAssist Remote Support V4 Session through the GoToAssist Remote Support V4 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 GoToAssist Remote Support V4 Session through the GoToAssist Remote Support V4 Service. It provides remote view and remote-control capabilities.

Expert: GoToAssist Remote Support V4 user, who creates GoToAssist Remote Support V4 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 GoToAssist Remote Support V4 Service.

Expert Mobile App: mobile application (Android and iOS) used by an Expert, that connects to the GoToAssist Remote Support v4 Service.

GoToAssist Remote Support V4 Sessions: attended chat, remote view, remote control or camera share and unattended remote control.

GoToAssist Remote Support V4 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.