# Remote Support Security for the Modern Enterprise

GoToAssist Corporate provides robust end-to-end data security measures that address both passive and active attacks against confidentiality, integrity and availability.

GoToAssist Corporate is a hosted service that provides a way to deliver remote support to Windows-based and Mac computers. GoToAssist Corporate allows a user to request support from a support representative and then allows that representative to view and optionally control the end user's computer remotely.

This document focuses on the information security features of GoToAssist Corporate. The reader is assumed to have a basic understanding of the product and it features. Additional materials on GoToAssist Corporate may be found online at **www.gotoassist.com** or by contacting a representative.

GoToAssist Corporate service delivery architecture

The diagram below provides a schematic overview of all major GoToAssist Corporate service delivery components and communication paths.
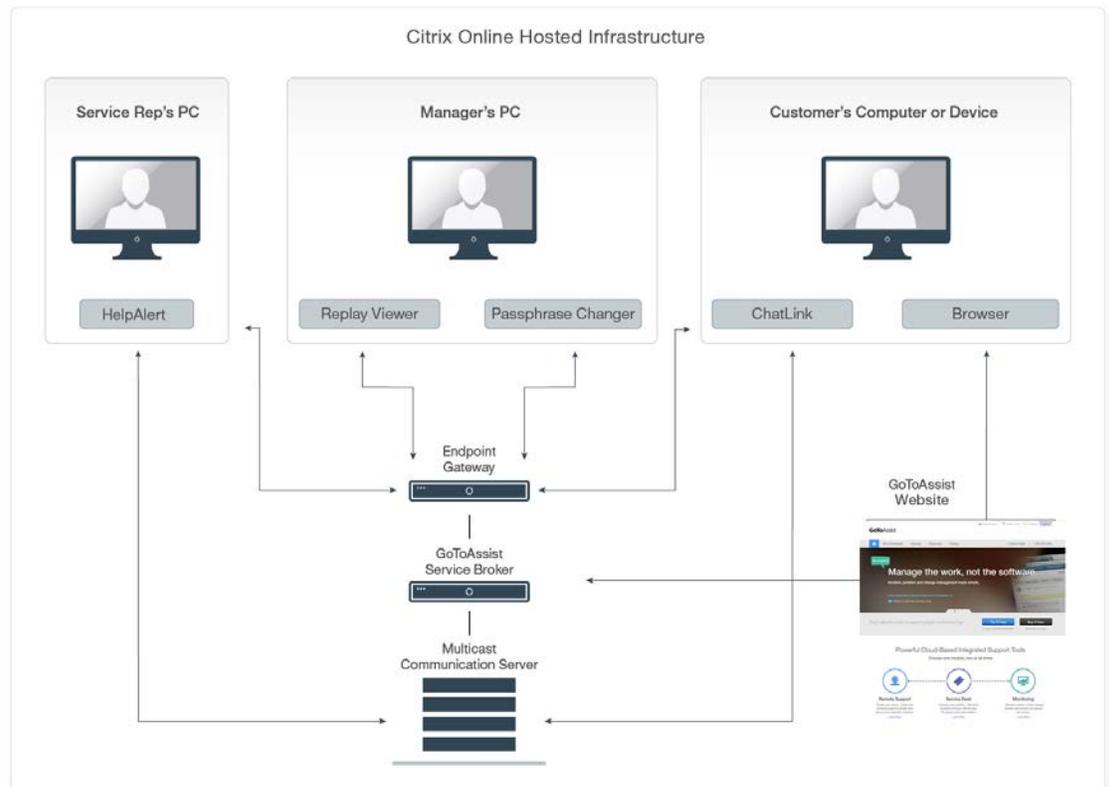
Definitions

HelpAlert

Win32 executable that resides on the service representative's computer and enables the representative to receive and reply to incoming customer queries.

ChatLink

Endpoint application that facilitates text-based communication between a customer and a service representative.

Browser

Standard Internet web browser, such as Chrome, Firefox, Internet Explorer, etc.

Replay Viewer

Endpoint application that allows company managers, team managers and representative managers to replay recorded GoToAssist Corporate sessions. Replay viewer can replay remote screen sharing, local screen sharing, chat and remote diagnostics.

Passphrase Changer

Endpoint application that facilitates the changing of the passphrase used to protect cryptographically-enforced access to session recordings.

GoToAssist Website

Web application that provides access to the GoToAssist website and web-based internal and external administration portals.

GoToAssist Service Broker

Web application that realizes GoToAssist Corporate account and service management, persistent storage and reporting functions.

Multicast Communication Server

One of a fleet of globally distributed servers used to realize a variety of high-availability unicast and multicast communication services.

Endpoint Gateway

A special-purpose gateway used by various endpoint applications to securely access the GoToAssist Service Broker for a variety of purposes using remote procedure calls.

Application security

GoToAssist Corporate 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 roles and related terms are defined in the table below:

Roles	
Administrator (or admin)	The employee who creates Groups and Portals in a company's GoToAssist Corporate Management Center. Admins can create, modify and delete GoToAssist Corporate accounts, portals, company managers and team managers; modify subscription and pricing data; and perform other administrative functions.
Company	GoToAssist Corporate customer for whom portals are set up.
Company Manager	A client company's employee that has access to its GoToAssist Corporate Management Center. Allowed to modify accounts, portals teams and representatives associated with his account.
Customer	The person requesting support from the client company via GoToAssist Corporate.
Group/Team	Collection of representatives that are assigned to a particular portal. Every representative belongs to exactly one group or team; every group or team is assigned to exactly one portal. Groups/teams contain some default settings for representatives.
Group Manager/ Team Manager	A client employee authorized by a company manager to modify certain aspects of a team, and that team's associated portal and representatives.
Representative	The support person who answers customer queries via HelpAlert.

Authentication

GoToAssist Corporate administrators, managers and representatives are authenticated using an account name and a strong password.

Passwords are governed by the following policies:

Strong passwords: A strong password is 8-32 characters in length and must contain at least three of the following four: upper-case alphabet [A-Z], lower-case alphabet [a-z], numbers [0-9], and special symbols [~`!@#$%^&*()_-+={}[]|\:;"'<>,.?/]. Strong passwords must not be the same as the login name or the actual first name or last name on the account. Passwords are checked for strength when initialized or changed.

Password expiration period: Expiration period of the password is configurable (min: 10 days, max: 120 days, default: 90 days). If the account holder logs in and the password has expired, the account holder is forced to change his or her password.

Password history: A history of passwords is maintained. A password cannot be changed to a password that exists in the password history. Password history depth is configurable (min: 1, max: 5, default: 3).

Account lockout: After 3 consecutive failed login attempts, the account is put into a mandatory soft-lockout state. This means that the account holder will not be able to log in for a configurable amount of time (min: 5 minutes, max: 30 minutes, default: 5 minutes). After the lockout period expires, the account holder will be able to attempt to log in to his or her account again.

Hard-lockout enforcement is an additional configurable option. After a configurable amount of failed login attempts, the account is put in the hard-lockout state. This means that the account holder cannot log in until his or her account password is reset by another privileged account holder. A hard lockout is enabled after a configurable number of attempts (min: 10, max: 50, default: 10).

Protection of customer computer and data

An essential part of GoToAssist Corporate security is its permission-based access control model for protecting access to the customer's computer and the data contained therein.

First, all GoToAssist Corporate sessions must be initiated by the remote customer. GoToAssist Corporate is not designed for unattended support scenarios.

Second, the customer is always prompted for permission before any screen sharing, remote control, or transfer of diagnostic data, files or other information is initiated.

If remote control and screen sharing has been authorized, the customer can watch what the representative does at all times. Further, the customer can easily take control back or terminate the session at any time.

Local security controls on the customer's PC or Mac are never overridden; the customer or the representative must still provide any Windows or application authentication credentials.

Finally, all connection activities are logged and the screen sharing and chat session can be optionally recorded and played back for review at a later time.

Communications security features

Communication between participants in a GoToAssist Corporate session occurs via an overlay multi-cast 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) . The communications architecture is summarized in the figure below.
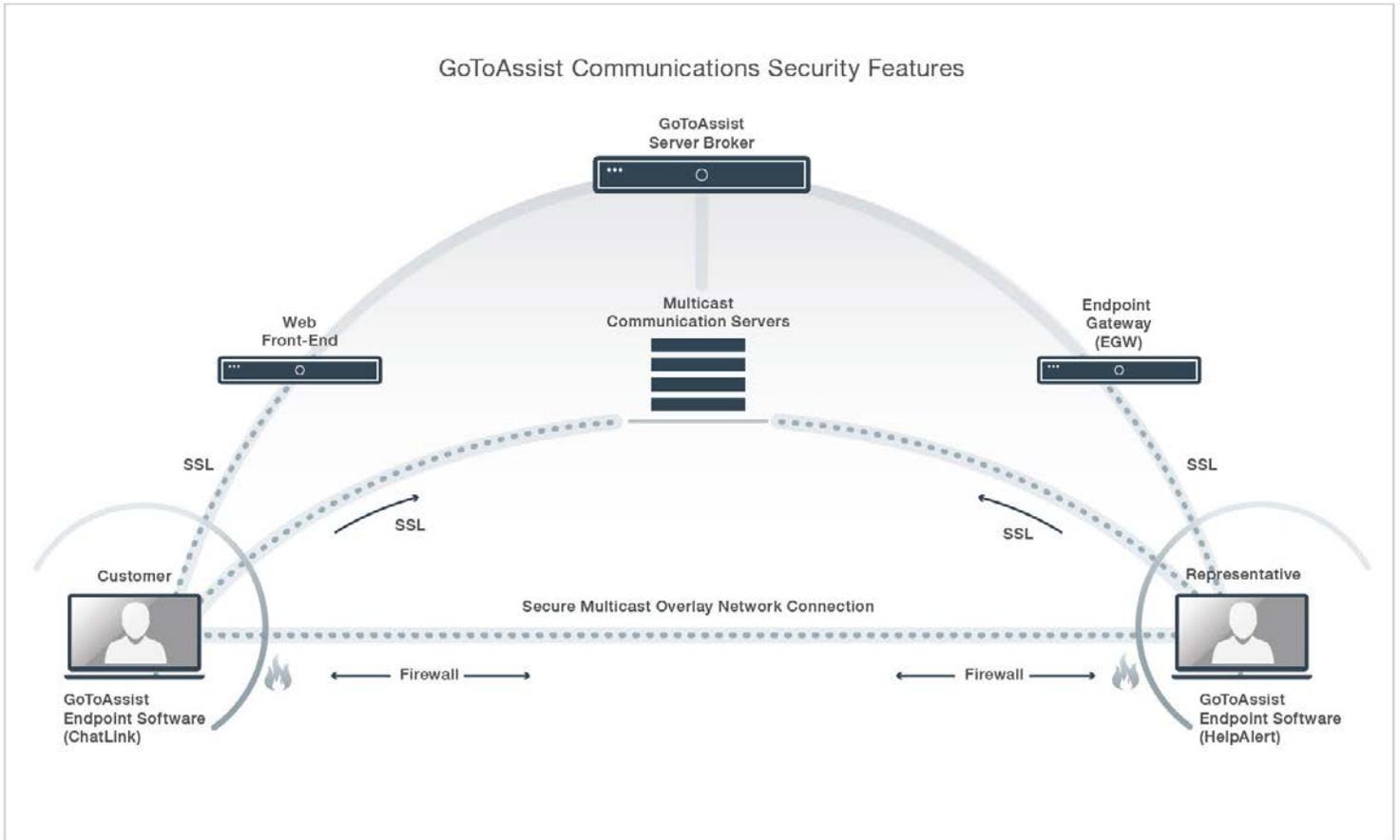
GoToAssist Corporate session participants ("endpoints") communicate with infrastructure communication servers and gateways using outbound TCP/IP connections on ports 8200, 443 and 80. Because GoToAssist Corporate is a hosted web-based service, participants can be located anywhere on the Internet — at a remote office, at home, at a business center or connected to another company's network.

Anytime/anywhere access to the GoToAssist Corporate service provides maximum flexibility and connectivity. However, to preserve the confidentiality and integrity of private business communication, GoToAssist Corporate also incorporates robust communication security features.

Communications confidentiality and integrity

GoToAssist Corporate provides true "end-to-end" data security measures that address both passive and active attacks against confidentiality, integrity and availability. All GoToAssist Corporate connections are "end-to-end" encrypted and accessible only by authorized support session participants.

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 kept on the servers in any form. Thus, breaking into a server cannot reveal the key for any encrypted stream that the intruder may have captured.

When recording is enabled, chat, screen-sharing 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 is used to encrypt the session key before storage. For replay, three items are needed: the session recording, the encrypted session key and the portal's private key.

Communications security controls based on strong cryptography are implemented at two layers: the "TCP layer" and the "Multicast Packet Security Layer" (MPSL).

TCP layer security

IETF-standard Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are used to protect all communication between endpoints. To provide maximum protection against eavesdropping, modification or replay attacks, the only SSL cipher suite supported for non-website TCP connections is 1024-bit RSA with 128-bit AES-CBC and HMAC-SHA1. However, for maximum compatibility with nearly any web browser on any user's desktop, the GoToAssist website supports in-bound connections using most supported SSL cipher suites. For the customers' own protection, we recommend that they configure their browsers to use strong cryptography by default whenever

possible and to always install the latest operating system and browser security patches.

When SSL/TLS connections are established to the GoToAssist website and between GoToAssist Corporate components, our servers authenticate themselves to clients using VeriSign/Thawte 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, MCS-to-Broker). These strong authentication measures prevent would-be attackers from masquerading as infrastructure servers or inserting themselves into the middle of support session communications.

Multicast packet security layer

Additional features provide complete "end-to-end" security for multicast packet data, independent of those provided by SSL/TLS. Specifically, all multicast session data is protected by "end-to-end" 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. The multicast packet security layer (MPSL) provides an added level of communication confidentiality and integrity and is unique to our products. Company communications are never visible to any third party, including both users who are not invited to a given session.

MPSL key establishment is accomplished by using a randomly generated 128-bit seed value selected by the service broker that is distributed to all endpoints over TLS and used as the input to a NIST approved HMAC-SHA1-based key derivation function. The seed value is erased from the service broker's memory when the session ends.

MPSL further protects multicast packet data

from eavesdropping using 128-bit AES encryption in Counter Mode. Plain-text 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. Because GoToAssist Corporate uses very strong, industry-standard cryptographic measures, customers can have a high degree of confidence that multicast support 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 GoToAssist Corporate session.

Key Points
- 128-bit AES encryption is used for session confidentiality
- Initial session key is chosen randomly by Broker then passed to endpoints over authenticated and encrypted channels
- Endpoints then negotiate a final session key just among themselves
- Final session key is not known to Broker
- Communication servers only route encrypted packets and do not have the session encryption key
- The GoToAssist Corporate architecture minimizes session data exposure risk while maximizing its ability to link agents to those requesting help

Firewall and proxy compatibility
Like other GoTo products, GoToAssist Corporate includes built-in proxy detection and connection management logic that helps automate software installation, avoid the need for complex network (re)configuration and maximize user productivity.

Firewalls and proxies already present in your network generally do not need any special configuration to enable use of GoToAssist Corporate.

When GoToAssist Corporate endpoint software is started, it attempts to contact the GoToAssist service broker via the Endpoint Gateway (EGW) by initiating one or more outbound SSL-protected TCP connections on ports 8200, 443 and/or 80. Whichever connection responds first will be used and the others will be dropped. This connection provides the foundation for participating in all future support sessions by enabling communication between hosted servers and the user's desktop.

When the user attempts to join a support session, GoToAssist Corporate endpoint software establishes one or more additional connections to communication servers, again using SSL-protected TCP connections on ports 8200, 443 and/or 80. These connections carry support session data during an active session.

In addition, for connectivity optimization tasks, the endpoint software initiates one or more short-lived TCP connections on ports 8200, 443 and/or 80 that are not SSL protected. These network "probes" do not contain any sensitive or exploitable information and present no risk of sensitive information disclosure.

By automatically adjusting the local network conditions using only outbound connections and choosing a port that is already open in most firewalls and proxies, GoToAssist Corporate provides a high degree of compatibility with existing network security measures. Unlike some other products, GoToAssist Corporate does not require companies to disable existing network perimeter security controls to allow online support session communication. These features maximize both compatibility and overall network

security.

Endpoint system security features

Online support session software must be compatible with a wide variety of desktop environments, yet create a secure endpoint on each user's desktop. GoToAssist Corporate accomplishes this using web-downloadable executables that employ strong cryptographic measures.

Signed endpoint software

All our executables are digitally signed for integrity protection. Strict quality control and configuration management procedures are followed during development and deployment to ensure software safety. The endpoint software exposes no externally available network interfaces and cannot be used by malware or viruses to exploit or infect remote systems. This protects other desktops participating in a session from being infected by a compromised host used by another attendee.

Cryptographic subsystem implementation

All cryptographic functions and security protocols employed by GoToAssist Corporate client endpoint software are implemented using open source OpenSSL cryptographic libraries. Use of the cryptographic libraries is restricted to the GoToAssist Corporate endpoint application; no external APIs are exposed for access by other software running on that desktop. All encryption and integrity algorithms, key size, and other cryptographic policy parameters are statically encoded when the application is compiled. Because there are no end-user-configurable cryptographic settings, it is impossible for users to weaken GoToAssist Corporate session security through accidental or intentional misconfiguration. A company that uses GoToAssist Corporate can be certain that the same level of online support session security is present on all participating endpoints, regardless of who owns or operates each desktop.

Hosted infrastructure security features

We deliver GoToAssist Corporate using an application service provider (ASP) model designed expressly to ensure robust and secure operation while integrating seamlessly with a company's existing network and security infrastructure.

Scalable and reliable infrastructure

The GoTo global service architecture has been designed for maximum performance, reliability and scalability. The GoToAssist Corporate service is driven by industry-standard, high-capacity servers and network equipment with the latest security patches in place. Redundant switches and routers are built into the architecture to ensure that there is never one single point of failure. Clustered servers and backup systems help guarantee a seamless flow of application processes — even in the event of heavy load or system failure. For optimal performance, the GoToAssist broker load balances the client/server sessions across geographically distributed communication servers.

Physical security

All GoToAssist Corporate web, application, communication and database servers are housed in secure co-location datacenters. Physical access to servers is tightly restricted and continuously monitored. All facilities have redundant power and environmental controls.

Network security

We employ firewall, router and VPN-based access controls to secure our private-service networks and backend servers. Infrastructure security is continuously monitored and vulnerability testing is conducted regularly by internal security staff and outside third-party auditors.

Customer privacy

Because maintaining the trust of our users is a priority for us, we are committed to respecting your privacy. A link to a copy of the current GoToAssist Corporate privacy policy can be found on the service website at www.gotoassist.com.

Compliance in regulated environments

Because of its comprehensive set of application and communications security controls, including its customer-authorized, permission-based security model, GoToAssist Corporate may be confidently used to support computers and applications in environments subject to HIPAA, Gramm-Leach-Bliley Act or Sarbanes-Oxley regulations, where robust data confidentiality and integrity controls must be employed.

We recommend that organizations carefully review all standard and configurable security features of GoToAssist Corporate in the context of their specific environments, user populations and policy requirements to determine which features should be enabled and how best to configure them. In some cases, communicating additional usage guidelines to users may be advisable to ensure the security goals of all stakeholders are satisfactorily met. We can provide additional materials regarding best practices for deployment and usage of GoToAssist Corporate.

Conclusion

GoToAssist Corporate's intuitive and secure interface and feature set make it the most effective solution for conducting online support sessions. Using GoToAssist Corporate, support, consulting and IT professionals can quickly and easily deliver technical help to customers across the globe.

Behind the scenes, our hosted service architecture transparently supports multi-point collaboration by providing a secure, reliable environment. As this paper shows, GoToAssist Corporate promotes ease of use and flexibility without compromising the integrity, privacy or administrative control of business communications or IT assets.

Appendix:

Security standards compliance

GoToAssist Corporate is compliant with the following industry and U.S. government standards for cryptographic algorithms and security protocols:

- OpenSSL FIPS 140-2 Validated Object Module. Certificate #1747
- The TLS/SSL Protocol, Version 1.0 IETF RFC 2246
- Advanced Encryption Standard (AES), FIPS 197
- AES Cipher suites for TLS, IETF RFC 3268
- AES Key Wrap Algorithm, IETF RFC 3394
- RSA, PKCS #1
- SHA-1, FIPS 180-1
- HMAC-SHA-1, IETF RFC 2104
- Pseudorandom Number Generation, ANSI X9.62 and FIPS 140-2