

Web conference security

We provide data security measures that address both passive and active attacks against confidentiality, integrity and availability when using GoToMeeting, GoToWebinar and GoToTraining.

We built GoToMeeting, GoToWebinar and GoToTraining with security in mind. For each solution, standards-based cryptography, a high-availability hosted service infrastructure and an intuitive user interface combine to maximize confidentiality, integrity and availability.

This document provides a technical description of the security features for GoToMeeting, GoToWebinar and GoToTraining. We have written it for technical evaluators and security specialists who are responsible for ensuring the safety of their company's network and the privacy and integrity of business communications.

GoToMeeting, GoToWebinar and GoToTraining are web conferencing tools that allow multiple PC, Mac, iOS, Android and Linux users to interact using screen sharing, video, text chat and other features. GoToMeeting is ideal for sales demos and collaborative online meetings. Built for larger audiences, GoToWebinar is great for marketing presentations and company events. And GoToTraining provides features specifically for web-based training, such as online access to tests and materials and a hosted course catalog.

These products are hosted services, delivered via web browsers, downloadable client executables and a network of communication servers. Sessions are scheduled, convened and moderated using our website and client software. GoToMeeting, GoToWebinar and GoToTraining automatically integrate with VoIP and phone conferencing for ease of use and solution completeness.

Business needs for secure collaboration

Easy-to-use online business collaboration tools like GoToMeeting, GoToWebinar and GoToTraining can help companies increase productivity by enabling them to

communicate and interact more effectively with co-workers, business partners and customers. But such tools vary greatly when it comes to embedded security features. Moreover, it is essential to understand the security implications of online collaboration and comply with safe usage guidelines.

Using any web conferencing solution requires careful consideration of potential threats and resulting business risks. Business security needs that must typically be addressed when adopting a web conferencing product include:

- Preventing unauthorized use of the service and its features so that only legitimate users can schedule online sessions
- Avoiding any compromise of company assets, including client computers and the private networks to which they are attached
- Protecting the privacy and integrity of confidential communication, including screen sharing, text messages, video and audio interaction
- Ensuring availability and reliability of the service itself, so that business communications cannot be denied or disrupted
- Integrating seamlessly with other network/computer security measures, so that web conferencing services can leverage (not degrade) an organization's existing safeguards

Our web conferencing tools were developed from the ground up to satisfy these common business security needs. By incorporating security features and making them easy to administer and use, GoToMeeting, GoToWebinar and GoToTraining enable effective and secure online business collaboration.

Role-based security features

To enable account owners to enforce company access policies related to service and feature use, every GoToMeeting, GoToWebinar and GoToTraining user is assigned one of several application-defined roles.

- Organizers (or trainers) are authorized to schedule meetings, webinars and/or training sessions. An organizer sets up each session, invites participants, initiates and ends the session and designates the current presenter.

- Attendees are people invited to participate in sessions. Attendees can view the presenter's screen, chat with other attendees or view the attendee list.
- Presenters are attendees who can share their screen with other attendees. On the desktop app, presenters can also grant other attendees shared control of their keyboard and mouse.
- Internal administrators are LogMeIn staff members authorized to manage GoToMeeting, GoToWebinar and GoToTraining services and accounts.
- External administrators are individuals from a customer site authorized to manage multi-user accounts. External administrators can configure account features, authorize organizers and access a variety of reporting tools.

The GoToMeeting, GoToWebinar and GoToTraining user interfaces provide intuitive session controls and status indicators that facilitate productive and secure online sessions.

Controls and privileges available to each user depend on the currently assigned role: organizer, active presenter or general attendee.

Organizer privileges

Organizers (or trainers) have the most control in a session and the ability to grant and revoke various privileges for the other participants.

Specific organizer privileges include:

- The ability to invite attendees before or during the session
- The ability to see the complete list of attendees and their current roles and privileges, so the organizer always remains aware of those present
- The ability to start and end the session, which prevents others from disrupting the session accidentally or otherwise
- The ability to make any attendee the active presenter, controlling which desktop can be viewed at any point in time throughout the session
- The ability to disallow the use of chat by one or more

attendees, and permitting sidebar discussions only when appropriate

- The ability to disconnect attendees
- The ability to transfer the organizer role to another attendee (a privilege that cannot be revoked) so the session can continue if the organizer must leave early

Presenter privileges

A presenter is the user actively sharing his or her desktop screen with other attendees. Only one attendee at a time within a session may be granted the active presenter role. Presenters have the following controls available to them:

- The ability to enable, disable or pause sharing of multiple screens or individual applications, which can be helpful to avoid displaying confidential data that might otherwise appear on the presenter's desktop (e.g., while searching files or folders)
- The ability to grant/revoke remote keyboard and mouse control, which facilitates efficient communication through desktop interaction
- The ability to make another attendee the presenter, providing for a flexible, dynamic flow during sessions

Whenever a presenter is sharing his or her screen with other attendees, a screen-sharing indicator is displayed on the presenter's control panel. To share his or her screen, the presenter must click the Screen button on the control panel. These features ensure that presenters always know when desktop sharing is active so that desktop screens are never shared accidentally.

Attendee privileges

Users with the basic attendee role have the following privileges:

- The ability to join sessions held by organizers
- The ability to view the presenter's screen unless the presenter has paused or disabled screen sharing
- If granted, the ability to remotely control the presenter's keyboard and mouse (a privilege that is automatically revoked whenever the active presenter role is changed)
- The ability to use chat to send text messages to all other

attendees or to one specific attendee (features that can be disabled by an organizer)

- The ability to leave a session at any time

Basing access rights and privileges on assigned roles allows flexible sessions that facilitate highly dynamic interaction between attendees, without sacrificing either control or visibility. Organizers can easily add attendees or change the presenter as needed throughout the session. Presenters remain in complete control of their own desktops, and organizers have everything required to manage the session effectively.

Account & session authentication features

Role-based authorization depends upon the ability to identify and authenticate users. To ensure that organizers and attendees have the right privileges, we have incorporated account and session authentication features into GoToMeeting, GoToWebinar and GoToTraining.

Website account login

To access a user account on the GoToMeeting, GoToWebinar and GoToTraining website, users must supply a valid email address and corresponding user account password. To make them hard to guess, all passwords must contain at least eight characters and include both letters and numbers. We also have a protection in place against brute-force login attacks.

We do not store user passwords in plaintext. Rather, we store passwords using a cryptographic hash function that is highly resilient to dictionary attacks. Furthermore, passwords are never transmitted in plaintext. We use transport layer security (TLS) protocols along with a password-authenticated key-agreement protocol for added security.

Authentication of session attendees

Because most organizations hold many sessions with restricted attendance, attendees cannot simply browse through scheduled sessions looking for one to attend. Instead, attendees need a unique meeting, webinar or training ID to join, as well as an optional password if the organizer chooses.

Whenever an organizer schedules a session, a pseudorandom number generator is used to create the meeting, webinar or training ID, which is checked against transactional database

tables to ensure it is not currently being used or has been used recently. The organizer can then share this ID with attendees using email, instant messaging or other communication methods.

To join the session, each attendee must provide the meeting, webinar or training ID by either clicking on a URL that contains the ID or by manually entering the value into a form presented by GoToMeeting, GoToWebinar or GoToTraining. When dialing in using a telephone, attendees must enter the ID on their keypad. If the ID is valid, each attendee is provided a session-unique role-token that is then presented to the communication servers during the join process.

Administration site security

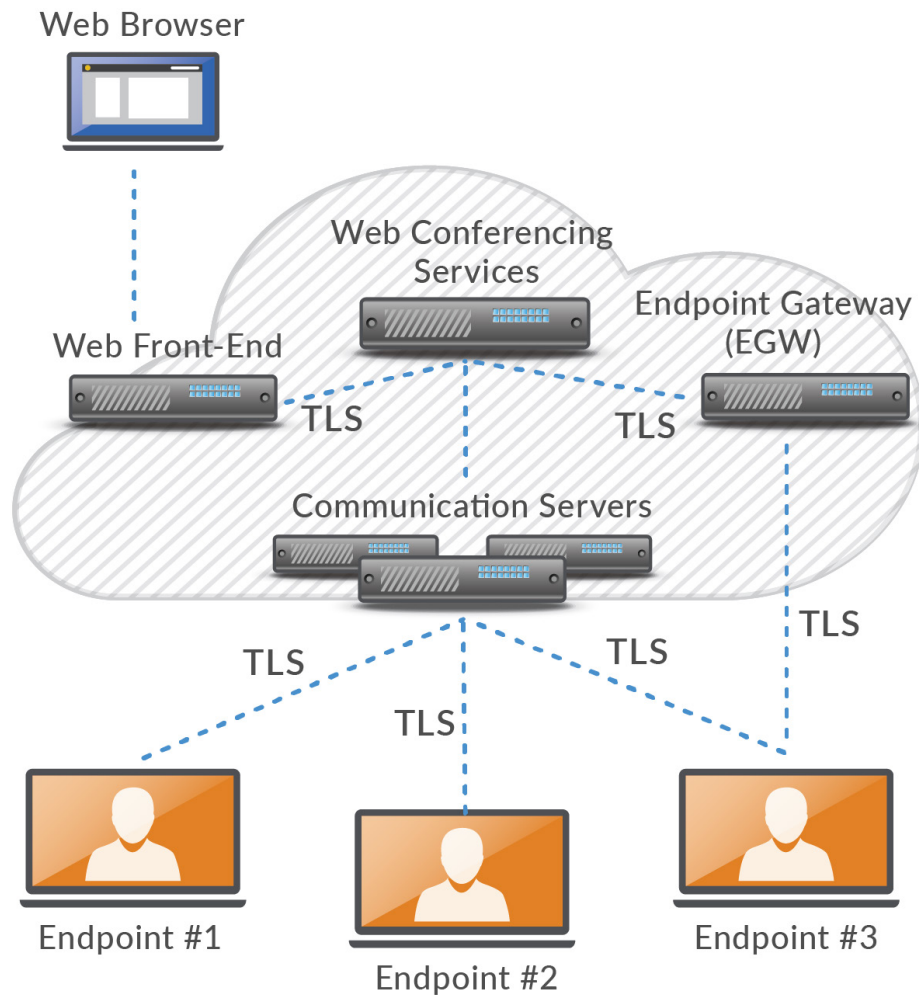
Like all connections to the GoToMeeting, GoToWebinar and GoToTraining website, connections to the administration portal are protected using TLS. Administrative functions are protected using strong passwords, activity logging, regular audits and a variety of internal physical and network security controls.

Communications security features

Screen-sharing communication between participants in a GoToMeeting, GoToWebinar or GoToTraining session occurs via an overlay networking stack that logically sits on top of the conventional TCP/IP stack within each user's PC. This network is realized by a collection of communications servers.

Participants (session endpoints) communicate with infrastructure communication servers and gateways using outbound TCP/IP connections on ports 8200, 443 and 80. Because GoToMeeting, GoToWebinar and GoToTraining are hosted web-based services, 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 GoToMeeting, GoToWebinar and GoToTraining services provides maximum flexibility and connectivity. However, to preserve the confidentiality and integrity of private business communication, these tools also incorporate robust communication security features.

Web conferencing service architecture



Data confidentiality and integrity

GoToMeeting, GoToWebinar and GoToTraining provide data security measures that address both passive and active attacks against confidentiality, integrity and availability. Screen-sharing data, keyboard/mouse control data and text chat information, referred to as “session data,” have communication security controls with multiple layers of strong cryptography.

TCP layer security

IETF-standard TLS protocols are used to protect all communication between endpoints. To provide protection against eavesdropping, modification or replay attacks, the only non-website connections we allow are those encrypted with AES. However, for maximum compatibility with nearly any web browser on any user’s desktop, the GoToMeeting, GoToWebinar and GoToTraining website supports in-bound connections using most supported TLS cipher suites as well.

For the customers’ own protection, we recommend that customers configure their browsers to use strong cryptography by default whenever possible and to always install the latest

operating system and browser security patches. We keep our servers up to date to support the latest and most secure cipher suites.

When TLS connections are established to the website and between GoToMeeting, GoToWebinar or GoToTraining components, our servers authenticate themselves to clients using DigiCert and Amazon public key certificates. For added protection against infrastructure attacks, mutual certificate-based authentication is used on servers that handle audio and video data. These strong authentication measures prevent would-be attackers from masquerading as infrastructure servers or inserting themselves into the middle of session communications.

Additional layer security

More features provide an additional layer of encryption for session data, 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.

Key establishment is accomplished by using a randomly generated 128-bit seed value selected by the GoToMeeting service 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 GoToMeeting service 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 the HMAC-SHA-1 algorithm (soon to be SHA-2). Because GoToMeeting, GoToWebinar and GoToTraining use very strong, industry-standard cryptographic measures, 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.

Firewall and proxy compatibility

Like our other products, GoToMeeting, GoToWebinar and GoToTraining include 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 our web conferencing tools.

When the GoToMeeting, GoToWebinar or GoToTraining desktop endpoint software is started, it attempts to contact the endpoint gateway (EGW) by initiating one or more outbound TLS-protected TCP connections on ports 443, 8200 and alternatively on port 80. Whichever connection responds first will be used and the others will be dropped. This connection provides the foundation for participating in all future sessions by enabling communication between hosted servers and the user's desktop. For other endpoints, including mobile and web, REST calls are made directly to the web conferencing services.

When the user attempts to join a session, the endpoint software establishes one or more additional connections to our communications servers, again using TLS-protected TCP connections. These connections carry data during an active session.

In addition, for network path prediction (NPP), the endpoint software periodically initiates one or more short-lived, out-of-session TCP connections on ports 8200, 443 or 80 that are not TLS protected. These network probes take advantage of SYN/ACK/FIN sequences to determine connectivity and round-trip times and do not contain any sensitive or exploitable information.

By automatically adjusting the local network conditions using only outbound connections and choosing a port that is already open in most firewalls and proxies, GoToMeeting, GoToWebinar and GoToTraining provide a high degree of compatibility with existing network security measures. Unlike some other products, ours do not require companies to disable existing security measures to allow web conferencing communication. These features maximize both compatibility and overall network security.

Audio security

We provide integrated audio conferencing for GoToMeeting, GoToWebinar and GoToTraining sessions through the telephone network (PSTN) as well as Voice over Internet Protocol (VoIP). The PSTN already provides for the confidentiality and integrity of voice communications. To protect the confidentiality and integrity of VoIP connections from the endpoints to the voice servers, we use an SRTP with AES-128-HMAC-SHA1-based protocol over both UDP and TCP. Keys are exchanged by the client and server over the already established TLS-protected HTTPS connection.

Video security We provide integrated video conferencing for GoToMeeting, GoToWebinar and GoToTraining sessions over the Internet. To protect the confidentiality and integrity of video connections from the endpoints to the video servers, we use an SRTP with AES-128-HMAC-SHA1-based protocol. Keys are exchanged by the client and server over the already established TLS-protected HTTPS connection.

Webcast security GoToWebinar webcasts use communications servers, broadcast gateways and a third-party content delivery network (Amazon CloudFront) to scalably deliver screen sharing, audio and video to attendees joining from a browser. The media is transmitted through the HTTP Live Streaming (HLS) protocol, while the broadcast gateways mix and transcode the data into multiple bitrates to enable adaptive delivery for clients with sub-optimal network connections. The gateways use RTP and HTTP to transport the output media streams to the CDN, which then delivers the streams to attendees over HTTPS.

Endpoint system security features Web conferencing software must work with a wide variety of desktop environments, yet create a secure endpoint on each user's desktop. GoToMeeting, GoToWebinar and GoToTraining accomplish 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, configuration management procedures and a Security Development Lifecycle (SDL) model are followed during development and deployment to ensure software safety. The endpoint software does not listen for inbound connections so that it 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 GoToMeeting, GoToWebinar and GoToTraining client endpoint software are implemented using open source OpenSSL cryptographic libraries.

Use of the cryptographic libraries is restricted to the GoToMeeting, GoToWebinar and GoToTraining endpoint applications; 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 our security through accidental or intentional misconfiguration. A company that uses GoToMeeting, GoToWebinar and/or GoToTraining can be certain that the same level of web conferencing security is present on all participating endpoints, regardless of who owns or operates each desktop.

Hosted infrastructure security features

We deliver GoToMeeting, GoToWebinar and GoToTraining 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 service architecture has been designed for maximum performance, reliability and scalability. The GoToMeeting, GoToWebinar and GoToTraining solutions are 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 a heavy load or system failure. For optimal performance, GoToMeeting, GoToWebinar and GoToTraining load balance the client/server sessions across geographically distributed communication servers.

Physical security

Our 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. When needed for improved performance, we also scale our services into trusted third-party cloud networks such as AWS.

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 staff and outside third-party auditors.

Content Security GoToMeeting, GoToWebinar and GoToTraining allow organizers to record their live sessions, including audio, video and screen content. When an organizer starts recording, every attendee is notified that the recording has begun, and a visual indicator appears on the control panel to reflect that recording is in progress.

Cloud recording Recordings can be saved locally on the organizer's computer or stored in their online account. If organizers choose to use our cloud recording option, there is no storage limit. We use a trusted third-party cloud network (AWS S3) for storage, and files are encrypted at rest using server-side encryption.

Organizers can easily share recordings with attendees after a session through unique, direct links, and attendees can view the recording playback from within their web browser. The share URLs do not expire; however, organizers can enable or disable sharing access at any time. The download and playback links are pre-signed URLs with a limited validity.

Transcripts For a richer post-session experience, organizers can enable the option to generate transcripts, slides and other content from recordings. We use Google Cloud Speech-to-Text technology to transcribe the session recordings, as requested by organizers, and we adhere to a strict data sharing policy. The audio file is transferred using TLS to Google Cloud storage, where the file is encrypted at rest and deleted immediately after the processing is complete.

Content uploading Some of our products provide capabilities for organizers to upload videos directly for their own use in live sessions. This uploaded content is also stored in AWS S3 with encryption enabled at rest as well as in transit.

Business messaging security An extension of GoToMeeting, business messaging is a downloadable instant messaging application where GoToMeeting customers can see the status of team members, exchange text messages and share files.

Team definition Team defines the scope for visibility and discoverability of various users. A team includes all users that are associated with your account, regardless of the type of GoToMeeting license. The account administrator is therefore also the team administrator.

Presence Business messaging users can see the presence state of any other user within their team as soon as they are included in their

contact list. Presence updates are pushed over a TLS-secured channel to our chat and presence service (CaPS), which then pushes notifications to all subscribers.

Messages

Messages can be exchanged with all members of your team and, if explicitly included via an invite by email, with external users as well. External in this context means a business messaging user who is not a member of your team (e.g., customer, prospect or partner).

Messages are sent to CaPS via a TLS-secured channel and then pushed to all users in scope for that message. The scope for a message can be:

- **A one-to-one conversation:** Only the two participants of that conversation can see the message.
- **A private group:** Only members of that private group can see the message. To become a member of a private group, an explicit invite from one of the group members is required.
- **A public group:** Every messaging user in your team can discover and join a public group and thereby get access to messages in that group.

Sharing content

In addition to sending text messages, users can share arbitrary content within business messaging by uploading and downloading files. Files are transferred through a TLS-secured channel and stored in private, secure cloud storage. The shared file is available for download for all users with the same scope as for text messages (see above). That means everyone who can read the shared message can also download the shared content. Content is made available through cryptographically signed URLs that link to the content.

Discoverability of contacts

A business messaging user can be found for one-to-one conversations, group invites or inclusion in a contact list only by people within your team.

Discoverability of groups

Groups can be found only if the group is public and within the same team. When a group gets created, the creator decides whether it will be public or private. This attribute of a group cannot be changed afterwards.

GoToStage security

An extension of GoToWebinar, GoToStage is an online portal where GoToWebinar organizers can create customizable Channels and publish their webinar recordings. We showcase published recordings on the GoToStage homepage, organized by business categories. At any point, organizers can unpublish their recordings, which removes the video from their Channel page and the GoToStage ecosystem.

Recording discoverability

Any video published to GoToStage is available for discovery on the GoToStage homepage and in search engine results. An organizer can control this and prevent discoverability through settings on his or her Channel page. In this case, the organizer's videos will not be featured on the homepage, and search engines will no longer index the content.

Viewing videos

Once an organizer publishes a recording to his or her Channel page, anyone with a direct link to the Channel or to the video's unique Watch Now page can watch the recording. However, all visitors are first required to register for GoToStage before they can play videos. Visitors can sign up by providing their name and email or by connecting one of several social media accounts. Once registered, a signed S3 URL with a set TTL is used to playback the webinar recording.

Organizer administration

Organizers can manage their Channels directly on the page itself with admin tools enabled based on their application-defined roles. Administrative functions are secured using strong passwords, and all connections in the GoToStage portal are protected using TLS.

Customer privacy

Because maintaining the trust of our users is a priority for us, we are committed to respecting your privacy. A copy of the current privacy policy can be found online at <https://secure.logmein.com/home/en/policies/privacy>.

Conclusion

With GoToMeeting, GoToWebinar and GoToTraining, it's easy to conduct meetings, present information and demonstrate products online to improve business communication. These tools' intuitive and secure interfaces and feature sets make them the most effective solutions for conducting and attending web conferencing sessions.

Behind the scenes, our hosted service architecture transparently supports multi-point collaboration by providing a secure, reliable environment. As this paper shows, GoToMeeting, GoToWebinar and GoToTraining promote ease of use and flexibility without compromising the integrity, privacy or administrative control of business communication.

Appendix: Security standards compliance

GoToMeeting, GoToWebinar and GoToTraining are compliant with the following industry and U.S. government standards for cryptographic algorithms and security protocols:

- The TLS Protocol, Version 1.2 IETF RFC 5246
- Advanced Encryption Standard (AES), FIPS 197
- AES Cipher suites for TLS, IETF RFC 5246
- RSA, PKCS #1
- SHA-2, FIPS PUB 180-4
- HMAC-SHA-2, IETF RFC 4868
- Pseudorandom Number Generation, ANSI X9.62 and FIPS 140-2