ReadyTalk

Audio & Web Conferencing

Network Security Overview

Dedicated to Security

Meet with confidence with ReadyTalk's audio and web conferencing services that are highly reliable and intuitive to use. ReadyTalk makes it easy for you to conduct and manage your meeting; you can concentrate on the substance of your conference or webinar, not the technology.

Providing a secure and reliable environment should be the number one priority of any conferencing service; ReadyTalk's services are designed and developed with security as its cornerstone.

This dedication to a secure environment gives customers the peace of mind to conduct worry-free conferences with their most trusted information.

Physical Security

ReadyTalk conferencing services are hosted in state-of-the-art ISO 9001:2000 certified data centers operated by U.S.-based providers. The data centers are monitored and staffed 24/7/365 and use multiple levels of security including video surveillance, software monitoring and alerts, network monitoring, physical access logging and reporting. The data centers also operate on multiple city power grids, multiple battery systems, multiple diesel backup generators and have contracts with multiple diesel distributors in case of prolonged power outages. Physical access to the conferencing systems is restricted to personnel whose access is logged and reported by the data center staff.

Network Security and Redundancy

The meeting service has multiple data paths across many Internet providers allowing data to travel along the shortest route and bypass downed routes and Internet connection failures. This intelligent network allows for fastest routes no matter where in the world meeting participants are located.

The meeting service uses encrypted network paths to communicate with the central service, and therefore, other meeting participants. All attendees initiate a Secure Sockets Layer (SSL) connection to the ReadyTalk service using the HTTPS (HTTP Secure) protocol, which encrypts data sent over the connection; a public key authenticates the server and the client, and establishes an encryption method and a unique session key. This method ensures that message privacy and message integrity is maintained when a user begins a secure session. The ReadyTalk service supports 128-bit AES encryption for most common browsers as well as 256-bit AES for next generation browsers and clients.

Stored Data Security

All data stored on the ReadyTalk service is protected using AES 256-bit encryption, which is the highest level of the AES standard and is the recommended encryption scheme used by the NSA for protecting sensitive information. Slides and data that are uploaded and/or recordings created using the ReadyTalk service are stored using this same encryption protocol to ensure the data remains secure. The uploaded content is delivered to attendees over a secure AES encrypted network.

Persistent Content

At your discretion, your uploaded content can remain in your ReadyTalk account and on the ReadyTalk network after you log out. This enables presenters to deliver the same presentation on numerous occasions without having to upload it each time they start a conference. Not only does this save time, it also allows the content to reside in a secure area while not in use.

Recordings and Archived Content

Chairpersons have the option of recording the audio and visual portions of their meeting. These recordings are created and stored in several formats within the ReadyTalk Storage Area Network (SAN). The stored recording files, which include both audio and visual data, are protected by AES 256 encryption on disk. Access to these files is provided over a standard SSL connection (AES 128) through the chairperson's browser.

In order to access a recording for playback, the user must have the unique link to the recording or know the alpha-numeric recording ID. For additional security, the chairperson may restrict access to recording playback by providing a passcode that is required each time playback is requested. This passcode can be changed or disabled at anytime. Additionally, recordings can be downloaded from the ReadyTalk server entirely and then deleted. Subscriptions can be setup to have recordings deleted automatically after a fixed period of time.

Data does not leave the central storage facilities by any means other than through the authorized system for playing and deleting recorded information and via secured backups to tape, which contain only encrypted data and are vaulted offsite. Recordings are not stored with any meta information that would allow a user to associate any usable identification information to any of the millions of files the system contains.

Application Security

Requests to the ReadyTalk conferencing services are securely authenticated against a master authentication server. During a successful login, a token key is issued that restricts access to the data and services based on the security role that was requested and authenticated.

Application servers verify the authentication validity of every request. The authorization keys required for access are time-based and expire after a short amount of inactivity or upon direct logout. Once a key has been invalidated, it can no longer be used to access any part of the service. The service maintains both data protection and user identity by using network layer encryption and application layer key-based authorization. Keys are used to correlate a user's identity with a security level. These security levels dictate what users are allowed to invoke and what data they are allowed to retrieve or change. Each level is completely controlled by the chairperson and can be enabled or disabled on a per conference basis:

Basic Level
The basic level is the default level of security. At this level, all meeting participants with the right meeting start time and proper access code can enter the conference. No additional authentication is required. This level of security is perfect for large meetings, such as webinars where there are potentially thousands of attendees.

Secure Level
When more security is needed, participants can be required to enter both an access code and an additional security code. The security code can be any alphanumeric code up to nine characters as defined by the chairperson. For security and convenience, these security codes can be changed on a per conference basis.

ACCOUNT SETTINGS

The Account Administrator is typically IT or administrative personnel who set restrictions on functions they deem too intrusive or sensitive for employee use. These settings can be changed on a per-user basis or across the account:

Disable Slides
Users will not be able to upload or push slides. This option ensures that users cannot upload company information to the meeting service.

Delete Slides on Exit
Slides uploaded for a conference will automatically be deleted when a user exits the conference. This ensures any uploaded data is destroyed as soon as a user closes the web moderator at the end of a conference. Users will have to re-upload slides the next time they present.

Disable Application and Desktop Sharing
Users will not be able to share individual applications or their desktop with meeting attendees.

Disable Recording
Users will not be able to record the audio or visual portions of their conference.

Disable Remote Control
Users will not be able to pass control of their application or desktop to another participant.

Disable Co-Presenter
Users will not be able to promote participants to allow the participant to push slides or share their applications or desktop.

CHAIRPERSON

The chairperson has several controls available to ensure the security of the conference. These controls allow the chairperson to set access levels, disconnect participants, lock conferences, set view mode, and gather registration information. Chairperson controls list all web and audio attendees. The web attendees are listed by their registration information, which is required to enter the conference.

CO-PRESENTER

Often times a co-presenter will join a chairperson in presenting information. They have the same abilities as a chairperson.

PARTICIPANT

Participants can only see information presented to them through the web browser. They are required to provide a name at the start of the meeting (the chairperson can require additional details). ReadyTalk does not give participants ability to record or share content.

Additional Security Options

PRE-MEETING SECURITY OPTIONS

During meeting setup and scheduling, the chairperson can require specific criteria from participants using these additional security features:

- *Require participants to pre-register and manually confirm each participant.*
- *Set an additional security passcode, which is case-sensitive and must consist of four to nine alphanumeric characters. Participants will be required to enter the passcode before joining the meeting.*
- *Pre-registration criteria—name, company, e-mail, phone number and other criteria—can be set as required registration fields by the chairperson.*

All content can be uploaded to secure servers before the meeting begins or during the meeting and then can be marked for deletion at the end of each conference or on an individual basis.

DURING-MEETING SECURITY OPTIONS

Additionally, the chairperson can control the participants' view at all times. The chairperson can determine if he/she wants to share his/her desktop, applications or only slides. When sharing applications, the chairperson can select the applications he/she wants to share so that any confidential information open in other applications is not viewable by participants.

Participants enter the conference in viewing-only mode. It is at the host's discretion whether they want to promote specific attendees to higher levels of control. Hosts always retain the ability to demote participants as needed back to viewing-only mode.

ReadyTalk also allows chairpersons to monitor and control attendees and their settings:

- *Disconnect: The chairperson can selectively disconnect participants from an audio and/or web meeting as needed or as sensitive material is being discussed. The feature can also be used to disconnect disruptive or unauthorized attendees.*
- *Lock Conference: Locking an audio conference prevents additional participants from entering, which prevents early entrance by non-authorized users. It can also be used when all attendees are present and the chairperson wants to prevent unauthorized entry.*
- *Mute/Unmute All: Mute/Unmute all participants to block out background noise.*
- *Listen Only: Place all participants in "Listen Only" mode so they are silent throughout the conference.*
- *Play Name: Play a selected participant's name.*

Conclusion

Today's fast-paced marketplace requires organizations to open their networks to customers, suppliers, and business partners. This same openness, however, brings security risks that must be properly managed.

ReadyTalk is dedicated to providing a secure and reliable environment and has instituted safe guards at every level of product architecture. Whether it is your PowerPoint file, your proprietary application, or your desktop, the ReadyTalk service will keep your information private. ReadyTalk maintains an ongoing commitment to security and is constantly evaluating new technologies to maintain the future security of customers' data.

About ReadyTalk

ReadyTalk is committed to helping customers conduct successful audio and web conferences of all sizes – from small, ad hoc meetings to large, formal events. Visit www.readytalk.com to learn more about our full range of technology and services including:

Audio + Web Conferencing | Webinars + Professional Services | Recording + Syndication