Connecting and Protecting the Networked World℠

LEVEL 3℠ WEB MEETING

SECURITY GUIDE

JANUARY 2017

DEDICATED TO SECURITY

Meet with confidence with the Level 3 Web Meeting audio and web conferencing services, which are highly reliable and intuitive to use. The Web Meeting services make 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. The Web Meeting service is designed and developed with security as its cornerstone.

This dedication to a secure environment gives you the peace of mind to conduct worry-free conferences — even with your most sensitive information.

Level(3)® COMMUNICATIONS

Connecting and Protecting
the Networked World℠

PHYSICAL SECURITY

Level 3 Web Meeting conferencing services are hosted in next generation data centers. The data centers are monitored and staffed 24/7 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 and multiple diesel backup generators. We 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 allowing data to travel along the shortest route and bypass downed routes and internet connection failures. This intelligent network allows for the 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 other meeting participants. All attendees initiate a Secure Sockets Layer (SSL) connection to the Level 3 Web Meeting 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 supports message privacy and message integrity when a user begins a secure session. The Level 3 Web Meeting 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 using the Level 3 Web Meeting service are 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 Web Meeting service are stored using this same encryption protocol to support data security. The uploaded content is delivered to attendees over an AES encrypted network designed for security.

PERSISTENT CONTENT

At your discretion, your uploaded content can remain in your Web Meeting account and on the 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 Level 3 Web Meeting 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 recordings by providing a passcode that is required each time a playback is requested. This passcode can be changed or disabled at any time. Additionally, recordings can be downloaded from the Web Meeting server entirely and then deleted. Subscriptions can be set up 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 Web Meeting 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 no longer can 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.

Secure

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.

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 with potentially thousands of attendees.

ACCOUNT SETTINGS

Account Administrators are 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 helps ensure 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.

Delete 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 support 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 some of the same abilities as a chairperson, but cannot promote individuals or use the audio controls.

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. The Level 3 Web Meeting service does not give participants the ability to record or share content.

ADDITIONAL SECURITY OPTIONS

Before Meeting

For added security, the chairperson can require participants to:

- Preregister.
- Set an additional security passcode, which is case sensitive and must be four to nine alphanumeric characters. Passcodes are required to join the call if this feature is used.
- Set pre-registration criteria as required registration fields, such as company, email and phone number.

- Content can be uploaded to secure servers before the meeting begins. This content can be deleted.

During Meeting Security

Additionally, the chairperson can control the participants' view at all times. They can determine if they want to share their desktops, applications or only slides. When sharing applications, the chairperson can select the applications to share so 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 back to viewing-only mode, as needed.

The Level 3 Web Meeting service 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

Level(3) COMMUNICATIONS

Connecting and Protecting the Networked World℠

attendees are present and the chairperson wants to prevent unauthorized entry.

Mute/Unmute All: The Mute/Unmute All feature helps block 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.

ABOUT LEVEL 3

We build, operate and take end-to-end responsibility for the network solutions connect you to the world. We put customers and take ownership of reliability and across our broad portfolio.

1.877.2LEVEL3
INFO@LEVEL3.COM
LEVEL3.COM