Level 3 COMMUNICATIONS

Connecting and Protecting the Networked World℠

KEEPING YOUR CONFERENCES SECURE

BEST PRACTICES

OVERVIEW

Today's fast-paced marketplace requires organizations to open their networks to customers, suppliers, and business suppliers. This same openness, however, brings security risks that must be properly managed. At Level 3, the privacy and security of your personal info and within our conferencing systems is a top priority. All of Level 3's Collaboration products are designed and developed with security as its cornerstone. This dedication to a secure and reliable environment gives customers the peace of mind to conduct worry-free conferences with their most trusted information. Level 3 maintains an ongoing commitment to security and is constantly evaluating new technologies to maintain the future security of customers' data.

This document contains recommendations for Level 3℠ Ready-Access®, Level 3℠ Web Meeting, Level 3℠ Connect Solution and Cisco® WebEx® to help minimize potential security exposure.

READY-ACCESS

Level 3℠ Ready-Access® is a reservationless audio conferencing service that provides the foundation for ad-hoc meetings and virtual teaming. With Level 3℠ Ready-Access® you can meet anyone, anywhere, anytime.

Below are some Level 3℠ Ready-Access® features and recommendations that help to keep your conference secure:

1. **Secure Chairperson Passcode**
   - Level 3 strongly encourages the use of secure chairperson PINs. PINs that do not consist of strictly repeated or sequential digits or that do not match common elements (such as access codes or phone numbers) are much more secure than those that do. Level 3 makes it standard practice to limit users from choosing PINs that are "weak" or "intuitive."
2. **Chairperson Passcode Aging**
   - Customers can elect to turn on the Chairperson Passcode Aging feature which requires users to have their Level 3℠ Ready-Access® chairperson passcodes changed on a regular time interval. Customers can elect to change their passcodes every 45, 60, 90, 120 or 180 days.
3. **Disable international dial-outs at the subscription level**
   - Administrators can enabled/disabled this by subscription, so we can leave this feature ON for key subscriptions that you identify — for example, users that reside or travel frequently outside North America.
4. **Enable conference termination for single lines in a conference**
   - The conference termination timer can be set to 5, 10, 15, 30, 60, 120, 240, 360, 480 minutes. When enabled, the meeting can be terminated if only one line is in the conference.
5. **Waiting room feature**
   - Allows the chairperson to set up a waiting room for participants either after the call has started, or after the conference has been locked by the chairperson. Please contact the help desk or your account manager to enable this feature.
6. **Lock conference (*4/*5)**
   - The chairperson has the ability to prohibit anyone else from joining the conference until he or she unlocks the call.
7. **Roll call (*9)**
   - When selected, this feature plays the pre-recorded names of the participants to the chair, to identify who is on the conference. Requires the Name Record feature to be ON.
8. **Participant count (*#)**
   - When selected, this feature plays a message to either the chairperson or the participants indicating the number of people in conference including themselves.
9. **Security passcode (4-9 digits)**
   - This is an added passcode for another layer of security that allows a chairperson to require another string of digits for each party before adding him or her to the conference.
10. **Post conference email summary**
    - Allows the call details to be sent via email immediately after a conference ends to the chair, indicating a conference took place on his or her account.

Level 3 COMMUNICATIONS

Connecting and Protecting the Networked World℠

LEVEL 3℠ CONNECT SOLUTIONS

Level 3's suite of Connect Solutions encompasses a host of user-enablement tools used for the scheduling, management, and handling of a comprehensive set of Unified Communications and Collaboration (UC&C) activities. The design of these is centered around a consistent user experience from mobile to web to desktop and covers moderator experience (on the desktop) and both client and non-client participant support.

Below are some Level 3℠ Web Connect safeguards that are utilized to help keep your conference secure.

1. **CAPTCHA security feature for international participants.**
   - A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) security layer is used to confirm an actual conferencing user is joining the meeting instead of another computer or bot. Before joining the meeting from a location outside of the North American dialing plan, users must type the word or numbers in the image in the field box that is presented.
2. **Call Back Delay feature**
   - The call back delay feature, which will not dial-out to participants outside the North American Dialing Plan until the host starts the web conference, is an additional safeguard that prevents unauthorized use of the Level 3℠ Web Connect "Dial Out" feature.

NOTE: Please keep in mind that since Level 3℠ Ready-Access® is integrated into both Level 3℠ Web Meeting and Cisco WebEx, all of the Level 3℠ Ready-Access® recommendations and features to keep your conference secure should also be used when hosting web conferences.

LEVEL 3℠ WEB MEETING

The Level 3℠ Web Meeting service makes scheduling and conducting online meetings a snap. It eliminates the need for special software installations and supports a wide range of platforms, browsers and devices so you can use what you want, where you want. And with a full set of capabilities at one affordable price, it's never been easier to get the conversation started.

Below are some Level 3℠ Web Meeting features and recommendations that help to keep your conference secure:

1. **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.
2. **Disable Application and Desktop Sharing**
   - Users will not be able to share individual applications or their desktop with meeting attendees.

PRE-MEETING SECURITY OPTIONS

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

1. Require participants to pre-register and manually confirm each participant.
2. 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.
3. Pre-registration criteria—name, company, e-mail, phone number and other criteria—can be set as required registration fields by the chairperson.
4. 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.

Level 3 COMMUNICATIONS

Connecting and Protecting the Networked World℠

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 he or she wants to promote specific attendees to higher levels of control. Hosts always retain the ability to demote participants as needed back to viewing-only mode.

1. **Disconnect**
   - The chairperson can selectively disconnect participants from the Ready-Access 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.
2. **Lock Conference**
   - Locking a Ready-Access 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.

CISCO WEBEX DELIVERED BY LEVEL 3

Keep the conversation going with Cisco WebEx delivered by Level 3. Easily share documents, presentations, applications, data and feedback with other attendees. It's fully integrated with Level 3℠ Ready-Access® audio conferencing for outstanding collaboration capabilities.

Below are some WebEx features and recommendations that help to keep your conference secure:

1. All meetings should be set to require a password. Passwords should be set with "strong" password criteria: For example: eight digits, one capital letter, one number. This will require that hosts assign a "strong" password at the time they schedule their WebEx meetings.
2. We recommend all meetings are set to UNLISTED - i.e., meetings will not be published publicly. This will require that only hosts and invitees have access to details and joining instructions for a scheduled WebEx meeting. Should your business needs require public listings of upcoming meetings, a "strong" password will be REQUIRED for each meeting.
3. Configure your microsite to disallow attendees from joining the teleconference before the host. The host must start the meeting prior to any users having the service dial out to them.

CONCLUSION

Level 3 is committed to protecting your conferencing information and privacy using the proven features, technologies, and security measures laid out in this quick reference guide. Please remember to follow these tips and suggestions for protecting your identity, Level 3℠ Ready-Access® accounts and conferences.

Please contact your Level 3 Collaboration Account Manager if you would like to activate any of these important security parameters within your account. Additionally, our Customer Care team is happy to answer any questions and can be reached at 1-888-447-1119 or conferencingcenter@level3.com

ABOUT LEVEL 3

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

1.877.2LEVEL3
info@level3.com
level3.com

DATA NETWORKS | SECURITY | CONTENT DISTRIBUTION | DATA CENTERS | APPLICATION PERFORMANCE | VOICE | UCC

© 2015 Level 3 Communications, LLC. All Rights Reserved. Level 3, Level 3 Communications, and the Level 3 Logo are either registered service marks or service marks of Level 3 Communications, LLC and/or one of its Affiliates in the United States and/or other countries. Level 3 services are provided by wholly owned subsidiaries of Level 3 Communications, Inc. Any other service names, product names, company names or logos included herein are the trademarks or service marks of their respective owners.

REV. 01/15