RECOMMENDED PROCEDURES FOR
VIRTUAL 12-STEP MEETINGS
USING ZOOM

DISCLAIMER: This guide is a compilation of "best practices" gleaned from other writings on safety for virtual 12-Step meetings, independent research, and Zoom training. Each group is autonomous and has the right to set its own policies and procedures for conducting virtual meetings. The authors make no representations or guarantees regarding the appropriateness of using the Zoom platform for 12-Step meetings or the ability to maintain anonymity in such meetings, and they make no endorsement of the Zoom video conferencing platform. The publisher and/or authors of this guide shall bear no liability or responsibility to any person or entity regarding any loss or damage incurred, or alleged to have incurred, directly or indirectly, by the information contained herein. Use of this guide implies acceptance of this disclaimer.

TABLE OF CONTENTS

APPENDICES

INTRODUCTION

Meetings provide the framework for all 12-Step programs, offering peer support in recovery through shared experience, strength, and hope. From the inception of these programs, most 12-Step meetings have been in-person gatherings, whether large or small, with an emphasis on anonymity. One pandemic in a technological age has changed all that. We are now “zooming” to meetings and learning as we go.

Hosting a virtual 12-Step meeting on the Internet is very different from gathering together in the basement of a church. The structure of the meeting is still somewhat familiar; yet, instead of arriving at a geographic location, we are using software on electronic devices to link ourselves together in one virtual space within the nebulous realm of the Internet.

The Internet itself is not well-understood by most of us, as only a tiny portion (known as the “clear web”) is accessible through standard web browsers. The “deep web” comprises roughly 98% of the Internet and includes anything behind sign-in credentials or a subscription. The “dark web” is a small subset of the deep web and is intentionally hidden, as nearly 60% of its activity is nefarious or illegal. This is where hackers, infiltrators, and disruptors reside.

If someone disrupted our meeting in a church, we would call 911; but this is not possible on the Internet. While meeting virtually, we soon discovered that we were responsible for our own safety and security within this realm; and we became quite resourceful about learning what was available to us and how we could share this knowledge with other 12-Step groups. This guide grew out of the lessons we are learning.

SUMMARY

Those of us who host virtual meetings do so because of our immense gratitude to our programs and our desire to keep them going during these challenging times of social distancing and sheltering in place. This work is some of the most difficult and unprecedented 12-Step service ever, because it combines highly complex computer technology with the psychic welfare of our members. This guide is intended to help those who host virtual 12-Step meetings to navigate the difficult tradeoffs between meeting safety and accessibility.

We suggest the following as a basic approach to meeting safely using the Zoom platform, all of which is covered within this guide in greater detail:

1. If your account has experienced suspicious activity, get a new group account.
2. Use the suggested Zoom settings presented in Appendix B.
3. Develop an approved set of host guidelines, including account sign in and administration.
4. Distribute meeting access instructions to your group members.
5. Develop a short, in-meeting announcement to inform members about key procedures.

BACKGROUND

CONDUCTING 12-STEP MEETINGS IN A VIRTUAL ENVIRONMENT

Under a shelter-in-place order that took effect on March 17, 2020, in response to the COVID-19 virus, many members of 12-Step groups chose to gather together for virtual meetings via Zoom. Originally started by individual members volunteering to host these virtual meetings, access information was quickly distributed to other group members.

Ideally, following 12-Step principles of one ultimate authority, members from each group would have met in person and agreed by group conscience on the parameters of safety and etiquette for these meetings before the first virtual meeting was held. For example, they would have agreed to make changes to the script, to create the positions of host and co-host, to establish the qualifications and scope of authority of such positions, and to determine the safety settings and protocols that would be employed within the software.

Instead, eager members signed up for Zoom accounts and circulated meeting IDs to other members of their groups via email, text, or phone call or by posting this information on a district website. These eager members became the first hosts of virtual 12-Step meetings, and most of them relied on Zoom's default settings. Hosts and their co-hosts, and sometimes safety committees, were left with the responsibility to develop security measures to address the welfare of the group.

Zoom settings are extensive and very complicated. Since the train had left the station on meeting virtually, these individuals found themselves making in the neighborhood of a hundred decisions about security settings and protocols that would impact the safety and anonymity of our members. Feeling as if they were laying track in front of this moving train to sustain these weekly meetings, many hosts were initially making these decisions without consulting the group. Affirmatively making a security setting or leaving it as a default constituted a decision either way, as not to decide is to decide.

Chairpersons, secretaries, and leads modified their scripts — particularly in regard to service, literature, fellowship, and voluntary contributions — to accommodate the fact that meeting participants no longer gathered in the same physical space. Many meeting participants took advantage of Zoom features that were never part of a live 12-Step meeting, including virtual backgrounds, profile pictures, screen sharing, chat messaging, and virtual breakout rooms. Unfortunately, many of these features are potential gateways for hackers to get into the meeting, to gather information on its participants, and to eventually take control of the meeting, usually on a subsequent date. Participants also became more relaxed in the comfort of their own homes and created more video and audio distractions than would normally occur in a live meeting; yet, at the same time, it was a delight to see a gallery of faces while sheltering in place. Sharing became a new experience.

WHAT IS ZOOM?

Zoom is a cloud-based, video-conferencing platform that can be used to bring individuals together in a virtual meeting via video and/or audio, when it is not possible for all of these individuals to meet in person. Zoom is the most popular platform because it is the best in its video and audio quality, its ease of use, and the features it offers for business meetings.

Like most meeting platforms of this nature, Zoom is designed to supplement the communications networks of large corporations and organizations that are equipped with their own cybersecurity systems and technical personnel to shelter Zoom software within a secure structure. Currently, Zoom is being used much more extensively by individuals (including 12-Step members) via their smart phones, tablets, laptops, and personal computers. These users are exposed to vulnerabilities by virtue of not having such security measures in place.

The number of daily participants in a wide range of Zoom meetings jumped from 10 million in December 2019 to more than 200 million in March 2020. That number exceeded 300 million daily Zoom meeting participants[1] before the end of April.

DISRUPTION OF MEETINGS

Almost as soon as they started, Zoom 12-Step meetings nationwide experienced a rash of raids or *Zoombombings*,[2] most of which begin with one or more infiltrators “trolling” or “casing” the meeting (sometimes for several weeks before the prime disruption) to collect names, phone numbers, and the detailed shares of participants to strengthen the impact of their ultimate disruption. Basic hacking techniques were used to gain entry into these 12-Step meetings, but hosts also made it easier for potential infiltrators by posting meeting IDs and passcodes on the Internet and by relying on Zoom’s default settings.

Short of a premeditated raid,[3] there are other types of disruptions that hackers can create within the virtual environment. One is simply entering the meeting and observing, in violation of our tradition of anonymity. Another is when individuals sneak into 12-Step meetings by obtaining meeting IDs and passwords, or by ghosting legitimate members and, once in the meeting, become disruptive or abusive in some way.

[1] Numbers provided by Zoom via the company’s blog.

[2] A “Zoombombing” is an organized and often nefarious attack on a virtual meeting by hackers, infiltrators, and disruptors that is intended to harass, demean, and traumatize regular meeting participants. It is loud, dissonant, verbally abusive, and often involves disturbing images that are pornographic, racist, anti-Semitic, or violent in nature. It is particularly traumatic because we come to these meetings with our hearts open and are highly vulnerable to verbal abuse and disturbing images. All video-conferencing platforms experience these raids; however, the company with the most popular product gets the nickname (e.g., we make a Xerox copy, we ask for a Kleenex, our meeting gets Zoombombed).

[3] Use of terms containing “bomb” will be minimized throughout the remainder of this guide out of respect for those whose emotional, psychic, and physiological sensitivities are triggered by it.

SAFETY COMMITTEES

In response to these disturbing disruptions, a number of 12-Step groups appointed safety committees to aid their hosts in making informed decisions regarding security protocols while balancing the risks of holding a virtual meeting on the Internet with the welcoming openness of a 12-Step meeting. One of the outcomes of these committees has been, and continues to be, to provide guidance for hosts and co-hosts. Groups have persisted in adapting and modifying their safety measures over the past several months, sometimes in response to traumatic disruptions. By maintaining their primary focus on anonymity, unity, the common welfare, service, and leadership, these safety committees have sustained their reliance on the Traditions and Concepts of 12-Step programs to navigate these previously uncharted waters.

Our three legacies of the Steps (recovery), Traditions (unity), and Concepts (service) are sufficiently robust to guide us in making any and all necessary decisions. *There is no reason to abandon our legacies under these circumstances.*

The challenge is to consider and interpret *all* of the Steps, Traditions, and Concepts when such decisions involve tensions and tradeoffs among them and, at the same time, to seek a balance that serves the common welfare. Traditions One (our common welfare should come first, personal progress for the greatest number), Five (the role of meetings in carrying the message), and Twelve (anonymity, principles before personalities) as well as Concepts Three (right of decision), Nine (welfare of the whole may require unpopular actions), and Ten (responsibility and necessary authority) must be considered when deciding what is best for the group.

RECOMMENDATIONS FOR KEY SAFETY MEASURES

To effectively navigate the detail and volume of security settings within the Zoom platform — particularly at a committee level — it is beneficial to distill them into a manageable set of key safety measures. Tools for consideration include passwords/passcodes, waiting rooms, dial-in access, virtual backgrounds, profile pictures, screen share, chat, locking the meeting, breakout rooms, and the ability for participants to rename or unmute themselves, among other features.

A table summarizing key Zoom safety measures, along with the rationale behind these recommendations, is included as Appendix A of this guide. These recommendations are supported by a comprehensive list of settings for the Zoom host account, which can be found in Appendix B.

DIVIDING DIAL-IN FROM VIDEO CALLERS

Among the first safety measures considered was dial-in access to Zoom meetings. While most participants were using devices (e.g., laptops, tablets, smart phones, and personal computers) that enabled full video conferencing access to 12-Step meetings on Zoom, some were dialing in to these meetings through a Zoom toll-free telephone number. This practice created three security risks:

1. Initially, many of these calls were being routed through servers in China, where the government is entitled to claim access to encryption keys[4] generated by these servers and to use them to eavesdrop on callers, even though they live outside of China, or to collect personal information pertaining to these callers. (This situation has since been remedied by Zoom.)
2. Allowing dial-in callers breaks the encryption that is protecting the video conferencing participants in the meeting.[5]
3. Hackers can use the telephone, a comparably mundane device, as a gateway into the virtual realm of video conferencing platforms.

Some 12-Step meetings have chosen to follow our recommendation of requiring members to enter the meeting through the Zoom app and to not allow dial-in access to the meeting. We want to be as inclusive as possible and make it easy for members to attend; yet, we recognize that there are tradeoffs between inclusivity and risk. The following are points to consider in making this decision:

- *The risk of dial-in callers has nothing to do with knowing the person who is coming into the meeting or having a password.* The issue is how they are coming in. The dial-in method does not go through the Zoom app and, therefore, does not bring Zoom's security along with it. In fact, this method disrupts Zoom's video conferencing security.
- Before the pandemic, most face-to-face 12-Step meetings did not allow dialing in, even though the technology is available by simply placing a speaker phone in the middle of the physical room. In most cases, if someone moved out of town, s/he would not be able to continue to attend his/her accustomed meeting.
- "Evidence" that other meetings allowing dial-ins have not been disrupted is equivalent to a false negative. It is possible that such meetings are not targets or just haven't been disrupted yet or that members are not personally aware of past disruptions. Hackers can enter these meeting on the coattails of dial-in callers, which is a highly risky capability within Zoom.

[4] *Encryption* is the method by which information is converted into secret code to hide that information's true meaning. An *encryption key* is a random string of bits created explicitly for scrambling and unscrambling data. Its design intention is to ensure that each key is unpredictable and unique. The longer the key, the harder it is to crack the encryption code. A *bit* (short for "binary data") is the smallest unit of measurement to quantify computer data.

[5] See the second-to-last bullet within the body of the text reached through this link: https://theconversation.com/zoom-security-ive-researched-problems-with-video-conferencing-for-years-heres-what-you-need-to-know-136330

- Tradition Three speaks to “membership” within a 12-Step fellowship and not “attendance” at a particular meeting. Most dial-in callers are accustomed to phone meetings and have other alternatives to access their respective programs. The only added requirements in a virtual meeting are Internet access and the willingness to use it. For the group’s increased security, members can offer encouragement and assistance to one another by using the Zoom app. Also, the telephone experience can be mimicked by using the audio portion of the Zoom app and turning off the video while still maintaining encryption.
- Tradition Twelve addresses anonymity, which is broken when unknown participants enter the meeting on the coattails of dial-in callers.
- Tradition One declares that “our common welfare comes first.” Some large meetings have only a few who wish to dial in, putting the entire meeting at risk. Further, most or all of the dial-in callers have the capability to enter through the app.

HOST / CO-HOST GUIDELINES

PREPARING TO HOST AND CO-HOST A MEETING

Only the scheduled Host of a meeting should start that meeting. It is most secure for the Host to start the meeting through the Zoom app rather than to start or join a meeting using Zoom’s web portal through a browser.[6] Specific instructions for starting a scheduled meeting through the Zoom app are provided in Appendix D.

Each Co-Host should join the meeting through the Zoom app as a regular participant and, once in the meeting, can be made a Co-Host by the Host.

All Hosts and Co-Hosts should close all browsers, documents, and interactive software applications on their devices, because every open file that is brought into a Zoom meeting is a potential gateway for hackers.

HOST: IN-MEETING SETTINGS REVIEW

Under your Security popup menu, the following items should be checked by default — “Enable waiting room” and Allow participants to: “Chat” and “Unmute Themselves.” Participants should not be able to rename themselves. This is also the place where you can later Lock Meeting.

Under Chat, you can determine whether a Participant Can Chat With: No One, Host Only, Everyone Publicly, or Everyone Publicly and Privately.[7] These selections are available under the three dots (meaning “more”) in the lower right hand corner of the Chat box.

[6] As an example, two people were in a locked meeting when a third person suddenly appeared. This individual had bypassed the waiting room and overridden the lock on the meeting by using the Zoom web portal to enter with the email address and passcode.

[7] The option for “Everyone Publicly and Privately” will not appear on the Chat menu when “Private Chat” is turned OFF in Account Management settings, as recommended in Appendix B of this guide.

Set your initial Chat checkmark to “Host Only,” which will allow the Host and Co-Host(s) to Chat privately with each other, with individual participants in the meeting, or with everyone in the waiting room. Individual meeting participants can also Chat with a Host or Co-Host.

After the meeting is locked, you can open Chat to Everyone Publicly. Please note that the Host and Co-Host(s) can continue to Chat privately under this selection. It is best NOT to allow any other participants to Chat privately with one another.

Screen Share should not appear on your Zoom menu bar, and Chat is not designed or intended to be used as a substitute for this feature.

HOST AND CO-HOST(S): MANAGING THE MEETING

IMPORTANT ADVISORY: ***It is recommended that all hosts and co-hosts operate only within the scope of authority given them by their committee or group. These are general, suggested procedures, and each group is autonomous in adopting or not adopting them — take what you like and leave the rest.***

General Duties

The Host is the Secretary’s technical assistant and security chief while the Secretary[8] maintains the flow of the meeting (e.g., readings, announcements, and shares). The Co-Host(s) manage the Waiting Room and rename participants when necessary to first name and last initial. For the most part, the Host focuses on muting/unmuting, addressing the issue of virtual backgrounds, lowering the raised hand after that individual is called upon to speak, turning off the video of various participants to minimize distractions, locking the meeting, and managing Chat. Scanning the gallery for “red flags” that could indicate a potential Disruption are shared Host/Co-Host duties.

The Secretary can also be made a Co-Host to call on individuals for announcements and shares, which enables the Secretary to see the hands in the order they were raised. If the Secretary prefers not to call on those who wish to share, then this duty falls to the Host.

Whether it is the Secretary or the Host who is calling on those who wish to share, this individual is also responsible for ensuring that newcomers have an opportunity to share (if this is part of the meeting’s script by group conscience) and that sharing is brought to a close in a timely manner.

Please remember that the Host and Co-Host(s) can communicate privately with one another using Chat without disrupting the flow of the meeting.

It is essential to the flow and security of the meeting that the Host and Co-Host(s) are clear about the separation of duties between them, as this minimizes any potential for confusion within the meeting itself. For example, the Host should be the one to lock the meeting and to change Chat permissions for participants while relying on the Co-Host(s) to manage the Waiting Room.

[8] In some 12-Step programs, the duties of the Secretary are fulfilled by the meeting Chair or Lead.

Specific Duties

HOST:

- Mute/unmute participants;
- Address virtual backgrounds among participants (see protocols below);
- Turn off the videos of participants who are engaged in distracting activities;
- Call on participants to speak (if Secretary declines) and lower raised hands;
- Lock meeting about 30 minutes in (or at a time agreed upon by the group or committee);
- Open Chat to Everyone Publicly about 15 minutes before the meeting ends and announce it openly or via Chat;
- Routinely scan the gallery, paying particular attention to the end of the gallery where participants have turned off their videos, as this is where a Disruption is likely to start;
- **Remain vigilant, as your primary responsibility is, in the event of a significant Disruption, to END THE MEETING IMMEDIATELY.** Bear in mind that this is a two-click process. If a Disruption occurs, do not restart the meeting. Sign out of the group's Zoom account and shut down your computer. The Zoom account will have to be scrubbed by Zoom's proprietary software before it can be used again to host a meeting. Since this can take a long time given the demands made on Zoom personnel, an alternative is to close the old account and open a new group Zoom account.

CO-HOST:

- Admit known individuals in the Waiting Room one at a time (**NEVER "Admit All"**);
- Communicate with individuals in the Waiting Room using Chat to address duplicates or triplicates, devices as names, and those who are unrecognizable (see detailed protocols below);
- When a participant arrives in the meeting room without video, request via Chat that the video be turned on briefly for identification purposes;
- Change names as necessary to first name and last initial (as participants no longer have the ability to do this in the meeting);
- Assist the Host with virtual backgrounds, turning off videos of those who are distracting, lowering raised hands, and scanning the gallery for potential "red flags."

Division of Duties between Two Co-Hosts: If one Co-Host is primarily responsible for admitting known participants *one at a time*, then a second Co-Host can be relied on (using Chat as a tool) to address the issue of duplicate, triplicate, or unrecognized individuals in the Waiting Room. Other duties can also be divided.

HOST AND CO-HOST(S): ACTIVITIES TO AVOID

Using the web portal (*Zoom.us URL*) to start or join a scheduled meeting can bypass or override security protocols set by the group's Zoom account administrator. For this reason, the following activities should be **AVOIDED**:

- **Sending a meeting invite that includes a link.** Those who use such a link are passing through a browser, which poses a security risk and could bypass or override existing protocols. It is sufficient to send just the meeting ID and passcode without the link and to encourage meeting participants to use the Zoom app to Join a Meeting.
- **Starting a scheduled meeting as a Host through the web portal.** Always use the Zoom app to Sign In for this purpose.
- **Joining a scheduled meeting as a Co-Host through the web portal.** Each Co-Host should Join a Meeting through the Zoom app as a regular participant and, once in the meeting, will then be made a Co-Host by the Host.

DETAILED HOST / CO-HOST GUIDELINES

The following guidelines may aid you in fulfilling your duties as Host and/or Co-Host.

Chat

The Chat feature should be opened at the start of the meeting to "Host Only," which also makes it available to the Co-Host(s). Hosts and Co-Hosts can Chat with each other and with meeting participants privately. They can also send Chat messages to the Waiting Room, but cannot receive Chat messages back from the Waiting Room.

After the meeting is locked, the Chat feature can be opened to Everyone Publicly (never privately) toward the end of the meeting (the last ten or fifteen minutes) to provide phone numbers to newcomers and to post program-related information.

Using Chat for crosstalk is discouraged; and when it occurs, Chat can be closed by the Host. (This is accomplished by checking "No One" instead of "Host Only" on the Chat popup menu.)

Waiting Room

When you activate your "Participants" window, your Waiting Room (when there is someone waiting) will appear above the list of participants.

Always admit each participant in the waiting room one at a time. **NEVER "Admit All."**

If a person comes into the Waiting Room and is duplicated/triplicated (i.e., you see two/three of them with the same name), do not let any of them in, as one of them could be a potential disrupter. Send a Chat message to "Everyone (in Waiting Room)" indicating that (as an example): "Jennifer is duplicated. Please leave meeting, sign out of your Zoom account, and Join meeting without your account, using first name and last initial." You may have to make this request more than once.

***NOTE:** Any participant who uses his/her own Zoom account to enter a meeting is placing that account at risk of being hacked. Before joining a meeting, any participant with a personal or professional Zoom account should enter that account, select "None" for Virtual Background, SIGN OUT of that account, and close their browser before Joining a Meeting through the Zoom app.*

If there is someone with the name of a device (e.g., "iPhone") or a fake or pet name (e.g., "Jet Puff"), send a Chat message to "Everyone (in Waiting Room)" indicating that: "Please leave meeting, change name under meeting ID to first name and last initial, then rejoin."

Please be aware that, for security reasons, no one in the Waiting Room can Chat back. (This prevents infiltrators in the Waiting Room from filling up Chat with derogatory messages or disruptive software code.)

Virtual Backgrounds

Virtual backgrounds are still photographs/illustrations or videos that can be displayed behind the participant in his/her video window during a Zoom meeting. These are digital files that are brought into a Zoom meeting through a participant's device and present a potential security risk.

There is a glitch in the Zoom software that allows participants to bring virtual backgrounds into a meeting even if the Host has disallowed them in the primary Zoom settings.

When this occurs, place the individual in the Waiting Room and request (via Chat) that this person leave the meeting, change the virtual background in his/her Zoom account settings to "None," sign out of his/her Zoom account, and then rejoin the meeting directly through the app (without signing in and joining through a Zoom account).

Simply changing the virtual background to None and remaining in the meeting is not enough — the door has already been opened.

Identification of Participants

Even if a participant name is known to the Host or Co-Host, it is important to see or hear that individual upon arrival in the meeting room, as infiltrators are known to collect names of regular meeting participants and attempt to enter future meetings with those names.

If the meeting hasn't started yet, make voice contact. If the meeting is already underway, ask the individual via Chat to turn on his/her video briefly so s/he can be seen.

If there is no response in either case, place this person in the Waiting Room and send a Chat message to "Everyone (in Waiting Room)" indicating: "Please leave meeting and rejoin with video on." Once you identify this person when s/he returns to the meeting, send a "Thank you!" Chat message.

Remove Participant

If a meeting participant fails to communicate or to cooperate, it is in the best interest of the group (see Tradition One) to remove that individual. To do so, place the person in the Waiting Room and remove him or her from there. This is cleaner than removing the participant directly from the meeting and avoids accidentally clicking something else on the Security menu.

Most Co-Hosts will give this individual the benefit of the doubt by communicating with him/her once more in the Waiting Room via Chat. Remember that this individual cannot Chat back but may be able to leave the meeting, cooperate with your requests, and rejoin. If this does not occur, then Remove the individual from the Waiting Room (and from the meeting).

Please be aware that anyone removed from the meeting (via the Waiting Room or the meeting itself) cannot return to the meeting until that meeting is closed and then reopened by the Host, usually the following week.

Lock Meeting

If it is in keeping with the group conscience, the Host has the prerogative to lock the meeting at any time without notice. Let your Co-Host know via Chat that the meeting is locked (after which participants may leave but cannot return); then, toward the end of the meeting, you can notify participants that the meeting has been locked and that Chat is now open to everyone.

It is not advisable to set a time when the meeting is routinely locked or to announce during the meeting the exact time when it was locked, as this is particularly valuable information for infiltrators who may have slipped in and are “casing” the meeting for future disruption.

Self-Care

Serving as Host or Co-Host is a particularly demanding service position that is likely to prevent you from actually participating in the meeting spiritually, emotionally, or intellectually. Hosts and Co-Hosts are there to ensure, to the best of their collective abilities, the safety and security of the other meeting participants so they can share what is in their hearts and minds. To work your program and practice your own self-care, please attend other meetings where you do not hold these service positions and participate fully at those meetings.

HOST ONLY: ENDING THE MEETING FOR ALL

By clicking the red End button, two more options appear for the Host: “End Meeting for All” (in red) and “Leave Meeting” (in black). *The red “End Meeting for All” is the magic button to be used in the event of a distressing disruption, and* ***only the Host has access to this button****. Understanding the implications of this and being able to act quickly and effectively is the Host’s most important task* (a two-click process). This button is also used to end the meeting normally when everyone else has left this virtual space.

A Host should never leave a meeting without first surrendering his/her Host duties to another participant in the meeting (preferably a Co-Host). In the event that a different Host ends the meeting for all, the original Host who started the meeting will still be responsible for Signing Out of the Zoom account, as this is something that cannot be delegated.

After ending the meeting, **please remember to Sign Out of the Zoom account** (see Appendix D for specific instructions).

ZOOM ACCOUNT ADMINISTRATION

It is important for Hosts, Administrators, and meeting participants to understand the distinction between the Zoom web portal and the Zoom app. Use of the *Zoom web portal* should be limited primarily to maintenance and administration of the group's Zoom account by the group's Virtual Account Administrator. The web portal is also used to download and update the *Zoom app* — an effective tool which Zoom continues to enhance in an effort to increase the availability and flexibility of options and protocols for those of us who lack the cybersecurity infrastructure of a major corporation or large organization. We recommend that only the *Zoom app* be used to start or join a scheduled 12-Step meeting.

ZOOM APP vs. ZOOM WEB PORTAL

In the classic 1939 film *The Wizard of Oz*, the end of the hall where the wizard receives visitors features a magnified image of the wizard's head complete with smoke, flames, and sound effects. This is equivalent to the virtual meeting room created through the use of the Zoom app (replete with its many potential features and presentation tools).

Off to the side in the wizard's hall is a curtained area; and the man behind the curtain — eventually revealed by Dorothy's little dog, Toto, who pulls the curtain aside — is pushing buttons, pulling levers, and shouting into a microphone. The Zoom web portal is the area behind the curtain; and in the corporate world of information technology, use of the web portal would be restricted to the company's on-site systems administrator. We recommend that a similar service position (e.g., Virtual Account Administrator) be created for each 12-Step group, and this person may double as the group's primary Host.

PROPOSED SERVICE POSITION DESCRIPTION

The Virtual Account Administrator would be responsible for:

- Maintaining the group's Zoom account settings in keeping with safety committee recommendations and/or group conscience and updating these settings as necessary.
- Scheduling a recurring meeting when necessary.
- Routinely verifying in a timely manner the availability of a recurring meeting in the Zoom app.
- Checking for updates to the Zoom app, applying those updates to the group's Zoom account, and notifying group members of the availability of each new update.
- Scheduling a rotation of hosts and co-hosts on a timely basis to serve at each meeting, if deemed appropriate by the group's safety committee and/or group conscience.
- Securing and/or providing training to hosts and co-hosts.
- Serving as a host or co-host for the meeting as needed.
- Serving as a member of the safety committee and as the communications hub for the safety committee, hosts and co-hosts, and group members regarding virtual meetings or Zoom-related matters.

- Reporting a meeting Disruption to Zoom and having the group's account scrubbed by Zoom's proprietary software, or alternatively, obtaining a new account (given that Zoom is so overwhelmed and scrubbing may be impractical).

RECOMMENDED ACCOUNT SETTINGS

A detailed list of recommended Zoom account settings for 12-Step meetings is included with this guide as Appendix B. As always, the group conscience can choose to relax or tighten these settings as part of an informed decision-making process.

SCHEDULING A RECURRING 12-STEP MEETING

Open your Zoom app and Sign In. Click on the Schedule icon.

When the Schedule Meeting popup window appears, enter the name of your meeting under Topic and set the start date and time. For the duration, remember to schedule the start 30 minutes before and end one hour after the meeting. Once scheduled within this window, the host can start and end the meeting as desired. We recommend having hosts and co-hosts convene at least fifteen minutes before the scheduled meeting start time to prepare for and address any last-minute issues.

Check the box for "Recurring meeting" and verify the time zone. Allow the Meeting ID to be generated automatically (Zoom discourages the use of the account's Personal Meeting ID). You can change the password to something that includes letters, numbers, and characters; or you can accept the Zoom-generated password. Audio should default to "Computer Audio."

Click the blue Schedule button. If your browser opens to record this meeting to your calendar, simply close it.

In the Zoom app, click on the Meetings button at the top. Your new meeting should appear in the left pane of this window under "Recurring meeting." When a meeting is highlighted, you can Start or Edit it using the right pane buttons.

Remember to *always* SIGN OUT after using the Zoom app.

VERIFYING A SCHEDULED 12-STEP MEETING

Before the next meeting, it is always a good idea to confirm that it is still on the list of recurring meetings in the Zoom app. Meetings expire and can also disappear from the list if you have made changes to the group's Zoom account settings.

If a meeting disappears, SIGN OUT of your Zoom app and close it. Go to the Zoom web portal and Sign In. Select Meetings under Personal in the list to the left. If your meeting does not appear in the Zoom app, it is not likely to appear under "Upcoming Meetings" on this web page. Click on "Previous Meetings" to see a list of what has already been hosted through this Zoom account.

Click on the most recent occurrence of the meeting you wish to reactivate, which is probably in blue. (Do not hit the Delete button.) Details for you to manage this meeting appear on the next screen; and at the bottom of the web page, click the button to "Edit this Meeting" and then click the blue button indicating "Only this meeting."

Under “When,” you can change the date to that of the next scheduled occurrence of this meeting. This should reactivate future occurrences for a specified length of time based on Zoom’s default. Click on the blue “Save” button at the bottom of the screen.

SIGN OUT of the Zoom web portal and Sign In to your Zoom app to verify that your meeting is once again a recurring meeting, then SIGN OUT of your Zoom app.

CHECKING FOR UPDATES

Zoom is constantly updating its app for our benefit. To check for an update, Sign In to the Zoom app and choose Check for Updates on the dropdown menu by clicking on your initials or profile picture in the upper right-hand corner. If an update is available, a popup window will appear and will download. When the “Update” button turns blue, click it. When the Zoom uploader has completed its work, you will be returned to the Sign In popup window for the Zoom app. Sign In to verify that your recurring meeting is still intact, then SIGN OUT.

We recommend advising hosts, co-hosts, and meeting participants of the availability of the Zoom app update at the next meeting or notify them by email.

SCHEDULING HOSTS / CO-HOSTS

In smaller meetings, one person may accept the service position of weekly host and enlist a trained co-host from the group to help with the waiting room for the early part of the meeting. Co-host duties can later be withdrawn so this individual can participate and share in the remainder of the meeting. In larger meetings, however, it may be beneficial to rotate host and co-host duties and to support each host with one or more scheduled co-hosts. For newer hosts/co-hosts, an experienced individual can be made a co-host to provide coaching and guidance using Chat.

The Virtual Account Administrator would be responsible for scheduling hosts and co-hosts on a timely basis and for ensuring that they are effectively trained and adequately supported during the meeting. This Administrator would also serve as a host or co-host.

SAFETY COMMITTEE COMMUNICATIONS

As a member of the safety committee, this Administrator would be primarily responsible for Zoom-related communications among committee members, as well as on behalf of the committee, to hosts and co-hosts, and to the group as a whole. Other committee members may act as service sponsors and/or collaborators to assist with and enhance this responsibility.

REPORTING A DISRUPTION TO ZOOM

If a meeting Disruption occurs, the host will immediately end that meeting for all and notify the group’s Virtual Account Administrator. This individual will contact Zoom at the earliest opportunity to report the incident and to have the group’s Zoom account scrubbed.

In the event that the account cannot be scrubbed in time for the next scheduled meeting, it may be necessary to close that account and open a new one. This responsibility falls to the Virtual Account Administrator in collaboration with whoever else holds responsibility for the group’s email address and Zoom account. In any case, a new meeting ID and passcode will be generated and/or chosen by the Administrator and communicated to the group’s members.

ACTIVITIES TO AVOID

Using the web portal (*Zoom.us URL*) to start or join a scheduled meeting can bypass or override security protocols set by the group's Zoom account administrator. For this reason, the following activities should be ***avoided***:

- **Sending a meeting invite that includes a link.** Those who use such a link are passing through a browser, which poses a security risk and could bypass or override existing protocols. It is sufficient to send just the meeting ID and passcode without the link and to encourage meeting participants to use the Zoom app to Join a Meeting.
- **Starting a scheduled meeting through the web portal.** Always use the Zoom app to Sign In for this purpose.
- **Joining a scheduled meeting through the web portal.** Each participant should Join a Meeting through the Zoom app.

Use of a Host Key should also be avoided. A Host Key can only be used to claim the position of Host for a meeting if the group's Zoom account has been set to allow participants to enter a meeting before the Host; and for security reasons, this practice is strongly discouraged. Participants should not be allowed to enter the meeting before the Host, as this is an open invitation to hackers, infiltrators, and disruptors; and for this reason, "Join Before Host" is OFF in Zoom Account Recommended Settings (Appendix B). The Host Key should (under Zoom's recommendation) continue to be safeguarded even more closely than the passcode.

APPENDIX A

SUMMARY OF KEY ZOOM SAFETY MEASURES

Feature/Benefit	Risk Factor	Recommendation
Password/Passcode: Requires a password or passcode in addition to the meeting ID to enter	Currently a default security setting strongly encouraged by Zoom; risk to meeting increases with public posting on a website or through social media	Require password/passcode and turn off ability to include in a direct meeting link. Rather than posting to the district website, provide the group's email address and, when contacted, request a phone number so the individual can be vetted before receiving the password/passcode. In the event of a disruption, change the password/passcode.
Waiting Room: Serves as a holding area for participants before they are admitted to the meeting room, creating a vetting opportunity. Once in the meeting, a participant can be returned there temporarily to resolve an issue (such as a virtual background) or to be removed from the meeting if deemed necessary.	Currently a default security setting strongly encouraged by Zoom; reduces the risk of admitting a potential hacker, infiltrator, or disruptor	Implement waiting room. When duplicates or triplicates appear, or when a name is not recognized, enables the host or co-host to offer detailed instructions via Chat to remedy the situation. The waiting room also serves as the most efficient area from which to resolve issues or to remove someone from the meeting, if necessary.
Dial-In Access: Allows participants to call into the meeting using a telephone rather than the Zoom app	Gateway for hackers; allowing this audio feature breaks the encryption protecting video conference participants	Do not allow. Phone meetings are available to those who do not have access to devices using the Zoom app.

Feature/Benefit	Risk Factor	Recommendation
Virtual Backgrounds: Allows participants to project an image that hides or masks the physical area behind them	Gateway for hackers; favored tool for disrupters; indicates that an open Zoom account has been brought into the meeting; unnecessary distraction for other meeting participants	Do not allow. A participant who arrives with a virtual background should be asked to leave the meeting, to change the virtual background in his/her Zoom account to "None," to sign out of that account, and to join the meeting through the Zoom app.
Profile Pictures: Allows participants to select a picture to appear when they turn off video	Gateway for hackers; security risk; indicates that an open Zoom account has been brought into the meeting	Turn on ability to hide profile pictures.
Open Zoom Account: Used to schedule, start, and host a meeting	Participants bringing their own open Zoom accounts into a 12-Step meeting create gateways for hackers and can override or bypass security protocols set for that meeting	Instruct participants to enter a 12-Step meeting only after signing out of their personal Zoom accounts on all devices, closing their browsers, and joining the meeting using the Zoom app.
Other Open Software: Most commonly used for Screen Share but also a habit for many users of electronic devices	Gateway for hackers; security risk	For each participant, including and especially a host or co-host, all browsers, documents, files, email, and other interactive software should be closed before starting or joining a meeting through the Zoom app.
Screen Share: Enables documents, presentations, or a desktop to be displayed for all participants to view during portions of the meeting	Favored tool for disruptors who often use this feature to display disturbing images	Do not use. Ask participants to read from program literature that is available to them at their respective locations.

Feature/Benefit	Risk Factor	Recommendation
Chat: Enables participants to send and receive messages; file sharing is also available as part of this feature	Favored tool for disruptors; care should be taken not to overwhelm Chat by using it as a substitute for the Screen Share feature	Disable Private Chat, File Sharing, and the ability to save Chat contents. For most of the meeting, Chat should be set to “Host Only,” enabling the host and co-host(s) to communicate privately with one another as well as with other participants (by typing, not cutting and pasting). During the last ten to fifteen minutes of the meeting, Chat can be opened to “Everyone Publicly” to provide phone numbers for newcomers and to post program-related information.
Lock Meeting: Enables the host to lock a meeting in progress as an added safety measure	In-meeting security feature added by Zoom; once the meeting is locked, no other participants can enter through the “front door”	The host should lock the meeting before opening Chat to “Everyone Publicly.” The exact time should vary and should not be announced. Rely on a Higher Power for intuitive guidance.
Breakout Rooms: Enables host to create separate rooms for smaller meetings within the larger 12-Step meeting	Gateway for hackers; huge security risk	Do not use.
Rename: The host can allow or disallow participants to rename themselves	Favored tool for disruptors to rename themselves as seemingly legitimate members or to hide their authorship of disruptive Chat messages	Do not allow. The host or a co-host should change existing names to first name and last initial.

Feature/Benefit	Risk Factor	Recommendation
Turn Off Video: Allows video to be turned off, leaving the white letters of the participant’s name against a black screen	Minimizes distractions during the meeting but creates some risk if video is off, not working, or unavailable on a device when a participant arrives; efforts should be made by the host/co-host(s) to verify the identity of this individual	Encourage participants to enter the meeting with video on for identification purposes; audio or Chat confirmation may suffice if video is unavailable. Video can only be turned on by the participant, even if a host or co-host turned it off to minimize distractions.
Screenshots: Enables participants to electronically record information in Chat or the Zoom window	Violation of anonymity, the spiritual foundation of all 12-Step Traditions	Discourage screenshots. A pen and paper should suffice to record a phone number or program-related information.
End Meeting: Only the host can end the meeting, not the co-host(s)	The only viable (and Zoom-recommended) method of responding to a disturbing disruption; also used to end the meeting when all other participants have taken their leave	The Host must remain vigilant. In the event of a disturbing disruption, the host should end the meeting for all *immediately*; and the meeting should not be resumed until the following week.

APPENDIX B

ZOOM ACCOUNT RECOMMENDED SETTINGS

Use of the Zoom web portal should be limited primarily to maintenance and administration of the group's Zoom account by the group's Virtual Account Administrator. These settings should be locked under Account Management and then double-checked in the account's Personal Settings.

ADMIN ACCOUNT MANAGEMENT SETTINGS

Sign into the Zoom web portal and select "Account Management" under the ADMIN section to the left, then select "Account Settings." Click to toggle a setting on (blue) or off (gray), and click the ***Lock*** icon for settings that you do not wish a Host to change.

ACCOUNT SETTINGS FOR MEETING

Security

ON: Require a password when scheduling new meetings

ON: Require a password for instant meetings

ON: Require a password for participants joining by phone

ON: Require a password for Personal Meeting ID (PMI)

ON: Waiting Room = highlight open dot beside ***Everyone***

OFF: Embed password in invite link for one-click join

OFF: Only authenticated users can join meetings

OFF: Only authenticated users can join meetings from Web client

Schedule Meeting

ON: Host Video

ON: Participants Video

ON: Audio Type = highlight open dot beside ***Computer Audio***

OFF: Join Before Host

ON: Enable Personal Meeting ID

OFF: Use Personal Meeting ID (PMI) when scheduling a meeting

OFF: Use Personal Meeting ID (PMI) when starting an instant meeting

OFF: Add audio watermark

OFF: Always display "Zoom Meeting" as the meeting topic

OFF: Require a password for Room Meeting ID (Applicable for Zoom Rooms only)

OFF: Bypass the password when joining meetings from meeting list (Zoom Rooms)

ON: Mute participants upon entry

OFF: Calendar and Contact Integration

OFF: Office 365 users can consent to enterprise applications accessing company data

OFF: Upcoming meeting reminder

OFF: Enforce to use OAuth 2.0 only for authenticate Office365 calendar integration

In Meeting (Basic)

OFF:	Require Encryption for 3rd Party Endpoints (applies to dial-in callers)
ON:	Chat = check “Prevent participants from saving chat”
OFF:	Private chat
OFF:	Auto-saving chats
ON:	Sound notification when someone joins or leaves = ***Host and co-hosts only***
OFF:	File transfer
OFF:	Feedback to Zoom
OFF:	Display end-of-meeting experience feedback survey
ON:	Co-host
OFF:	Polling
ON:	Always show meeting control toolbar
ON:	Show Zoom windows during screen share
OFF:	Screen sharing
ON:	Disable desktop/screen share for users
OFF:	Annotation
OFF:	Whiteboard
OFF:	Remote control
ON:	Nonverbal feedback
OFF:	Allow removed participants to rejoin
OFF:	Allow participants to rename themselves
ON:	Hide participant profile pictures in a meeting

In Meeting (Advanced)

ON:	Report participants to Zoom
OFF:	Breakout Room
OFF:	Remote support
OFF:	Closed captioning
OFF:	Save Captions
OFF:	Far end camera control
OFF:	Group HD video
OFF:	Virtual background
OFF:	Identify guest participants in the meeting/webinar
OFF:	Auto-answer group in chat
OFF:	Peer to Peer connection while only 2 people are in a meeting
OFF:	Only show default email when sending email invites
OFF:	Use HTML format email for Outlook plugin
OFF:	DSCP marking
OFF:	Allow users to select stereo audio in their client settings
OFF:	Allow users to select original sound in their client settings
OFF:	Select data center regions for meetings/webinars hosted by your account
OFF:	Show a “Join from your browser” link
OFF:	Allow live stream meetings
OFF:	Allow Skype for Business (Lync) client to join a Zoom meeting

Email Notification

ON:	When a cloud recording is available
ON:	When attendees join meeting before host
ON:	When a meeting is cancelled
ON:	When an alternative host is set or removed from a meeting
ON:	When someone scheduled a meeting for a host
ON:	When the cloud recording is going to be permanently deleted from trash
ON:	When the meeting duration exceeds the limit = [***4***] hours

Admin Options

OFF:	Blur snapshot on iOS task switcher
OFF:	Display meetings scheduled for others
OFF:	Use content delivery network (CDN)
OFF:	Allow users to contact Zoom's Support via Chat
OFF:	Show one person meetings on Reports

ACCOUNT SETTINGS FOR RECORDING

OFF:	Local recording
OFF:	Cloud recording
OFF:	Automatic recording
OFF:	IP Address Access Control
OFF:	Prevent hosts from accessing their cloud recordings
OFF:	Cloud recording downloads
OFF:	IP Address Access Control
ON:	Only authenticated users can view cloud recordings = ***Signed-in users in my account***
ON:	Require password to access shared cloud recordings
ON:	Auto delete recordings after [***30***] days
OFF:	Allow recovery of deleted cloud recordings from Trash
OFF:	Recording disclaimer
OFF:	Multiple audio notifications of recorded meeting

ACCOUNT SETTINGS FOR TELEPHONE: *All should be OFF*

PERSONAL SETTINGS

Select “Settings” under the Personal section to the left to *verify* the following.

PERSONAL SETTINGS FOR MEETING

Security

ON: Require a password when scheduling new meetings
ON: Require a password for instant meetings
ON: Require a password for participants joining by phone
ON: Require a password for Personal Meeting ID (PMI)
ON: Waiting Room = highlight open dot beside ***Everyone***
OFF: Embed password in invite link for one-click join
OFF: Only authenticated users can join meetings
OFF: Only authenticated users can join meetings from Web client

Schedule Meeting

ON: Host Video
ON: Participants Video
ON: Audio Type = ***Computer Audio***
OFF: Join Before Host
ON: Enable Personal Meeting ID
OFF: Use Personal Meeting ID (PMI) when scheduling a meeting
OFF: Use Personal Meeting ID (PMI) when starting an instant meeting
ON: Mute participants upon entry
OFF: Upcoming meeting reminder

In Meeting (Basic)

OFF: Require Encryption for 3rd Party Endpoints
ON: Chat = ***Prevent participants from saving chat***
ON: Private chat
OFF: Auto-saving chats
ON: Sound notification when someone joins or leaves = ***Host and co-hosts only***
OFF: File transfer
OFF: Feedback to Zoom
OFF: Display end-of-meeting experience feedback survey
ON: Co-host
OFF: Polling
ON: Always show meeting control toolbar
ON: Show Zoom windows during screen share
OFF: Screen sharing
ON: Disable desktop/screen share for users
OFF: Annotation
OFF: Whiteboard
OFF: Remote control
ON: Nonverbal feedback
OFF: Allow removed participants to rejoin
OFF: Allow participants to rename themselves
ON: Hide participant profile pictures in a meeting

In Meeting (Advanced)

ON: Report participants to Zoom
OFF: Breakout Room
OFF: Remote support
OFF: Closed captioning
OFF: Save Captions
OFF: Far end camera control
OFF: Group HD video
OFF: Virtual background
OFF: Identify guest participants in the meeting/webinar
OFF: Auto-answer group in chat
OFF: Only show default email when sending email invites
OFF: Use HTML format email for Outlook plugin
OFF: Allow users to select stereo audio in their client settings
OFF: Allow users to select original sound in their client settings
OFF: Select data center regions for meetings/webinars hosted by your account
OFF: Show a “Join from your browser” link
OFF: Allow live stream meetings

Email Notification

ON: When a cloud recording is available
ON: When attendees join meeting before host
ON: When a meeting is cancelled
ON: When an alternative host is set or removed from a meeting
ON: When someone scheduled a meeting for a host
ON: When the cloud recording is going to be permanently deleted from trash

Other

OFF: Blur snapshot on iOS task switcher

PERSONAL SETTINGS FOR RECORDING

OFF: Local recording
OFF: Cloud recording
OFF: Automatic recording
OFF: IP Address Access Control
ON: Only authenticated users can view cloud recordings = ***Signed-in users in my account***
ON: Require password to access shared cloud recordings
ON: Auto delete recordings after [30] days [Host can delete cloud recordings is disabled]
OFF: Recording disclaimer
OFF: Multiple audio notifications of recorded meeting

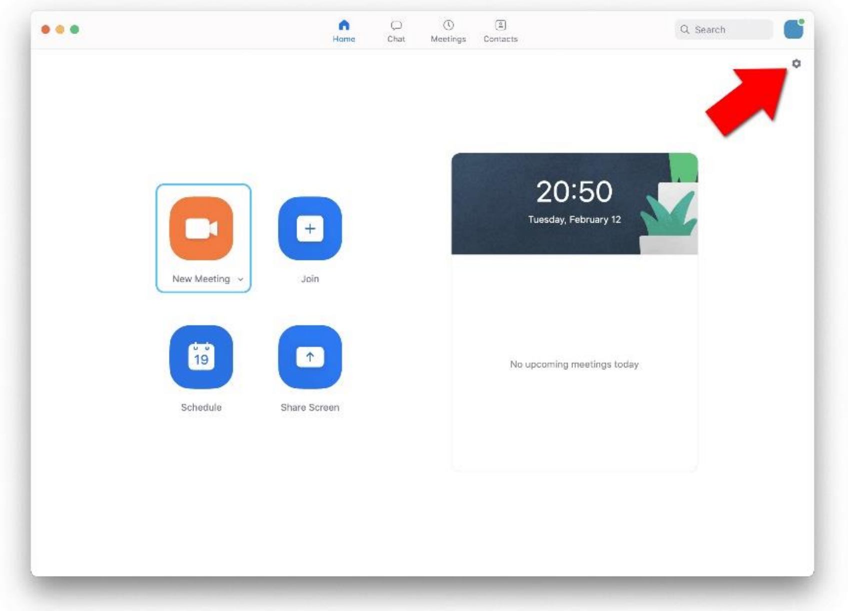
PERSONAL SETTINGS FOR TELEPHONE: *All should be OFF*

NOTE: *Some of the “ON” settings are in place for both Account Management and Personal Settings in the event that a meeting is accidentally recorded to the Cloud or someone hacks in and either joins a meeting before the host or schedules a meeting without the host’s prior knowledge. “Show Zoom windows during screen share” is ON in the event that screen share is activated. A password is required for participants joining by phone as a precaution.*

SIGN OUT of the group’s account in the Zoom web portal.

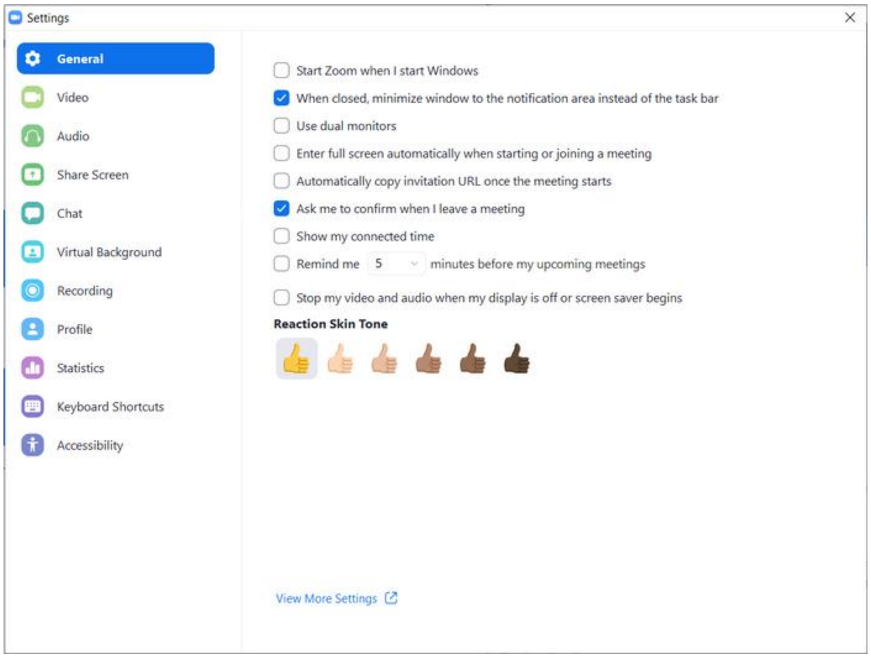
ZOOM APP SETTINGS

When you first Sign In to the Zoom app, a screen similar to the one below will appear. Click on the Settings icon to which the giant red arrow is pointing.



Your initials or your profile picture are directly above the Settings icon. Click on your initials or profile for a dropdown menu; and at the end of that menu is where you SIGN OUT.
Remember to SIGN OUT every time you leave a meeting!
Never leave your Zoom account open.

This will bring you to your General Settings page. Check "When closed, minimize window to the notification are instead of the task bar" and "Ask me to confirm when I leave a meeting."



□ Start Zoom when I start Windows
☑ When closed, minimize window to the notification area instead of the task bar
□ Use dual monitors
□ Enter full screen automatically when starting or joining a meeting
□ Automatically copy invitation URL once the meeting starts
☑ Ask me to confirm when I leave a meeting
□ Show my connected time
□ Remind me 5 minutes before my upcoming meetings
□ Stop my video and audio when my display is off or screen saver begins

Reaction Skin Tone

View More Settings

Recommended settings for each category listed in the left pane, beginning with Video, are as follows. [***NOTE:*** *Defaults of video and audio are determined by your device.*]

VIDEO

My Video

Blank: Enable HD
CHECK: Mirror my video
CHECK: Touch up my appearance

Meetings

CHECK: Always display participant names on their video
Blank: Turn off my video when joining meeting
CHECK: Always show video preview dialog when joining a video meeting
Blank: Hide non-video participants

Advanced

CHECK: Enable de-noise
CHECK: Enable hardware acceleration for video processing
CHECK: Enable hardware acceleration for sending video
CHECK: Enable hardware acceleration for receiving video
NOTE: Video rendering and capturing should all be set to Auto.

AUDIO

Microphone

CHECK: Automatically adjust volume

Other [No Subtitle]

Blank: Use separate audio device to play ringtone simultaneously
CHECK: Automatically join audio by computer when joining a meeting
CHECK: Mute my microphone when joining a meeting
CHECK: Press and hold SPACE key to temporarily unmute yourself
CHECK: Sync buttons on headset

Advanced

Blank: Show in-meeting option to “Enable Original Sound” from microphone
NOTE: Audio Processing suppression and cancellation should all be set to Auto.

SHARE SCREEN *(precautionary settings)*

My Video

Blank: Enter full screen when a participant shares screen
Blank: Maximize Zoom window when a participant shares screen
CHECK: Scale to fit shared content to Zoom window
CHECK: Show Zoom windows during screen share
Blank: Enable the remote control of all applications
Blank: Side-by-side mode
CHECK: Silence system notifications when sharing desktop

Advanced

CHECK: Enable hardware acceleration for screen sharing
Blank: Limit your screen share to [10] frames-per-second
CHECK: Show green border when I select the shared content
NOTE: Screen capture mode should be set to Auto.

CHAT

Chat Settings

Blank: Show “Code Snippet” button

CHECK: Include link preview

CHECK: Change my status to “Away” when I am inactive for [30] minutes

NOTE: Left sidebar theme should be set to Dark.
Ignore blocked users

Unread Messages

Blank: Keep all unread messages on top

Blank: Show unread message badge (1) for channels

Blank: Move messages with new replies to the bottom of the chat

NOTE: When viewing unread messages in a channel, select Start at the first unread.

Push Notifications

NOTE: Select All messages.
Ignore “With exception for Channels…” and “Receive notifications for Keywords.”

Blank: Notify me about new replies on messages I am following

Blank: Do not disturb from:

CHECK: Play sound when I receive a new message

CHECK: Mute notifications while I am in a meeting or on a call

Blank: Show notification banner on screen until dismissed

Blank: Show message preview (uncheck this option for privacy)

VIRTUAL BACKGROUND

NOTE: You should receive a message that “Setting has been turned off.”

RECORDING

NOTE: All boxes should be Blank.

Your **PROFILE** is personal, and **STATISTICS** are informational. Feel free to explore and select **KEYBOARD SHORTCUTS**.

ACCESSIBILITY

Closed Caption

NOTE: Closed Caption Font Size should be set to Normal.

Meeting Controls

CHECK: Always Show Meeting Controls

NOTE: Chat Display Size should be set to 100%.

APPENDIX C

PARTICIPANT GUIDELINES

We recommend that only the Zoom app be used to start or join a virtual 12-Step meeting. This is the tool that Zoom is continuing to enhance in an effort to increase the availability and flexibility of options and protocols for those of us who lack the cybersecurity infrastructure of a large corporation.

Participants should only use the Zoom web portal to download or update the Zoom app.

MEETING PREPARATIONS

Close all browsers, documents, and interactive software applications on your device, as every open file you bring into a Zoom meeting is a potential gateway for hackers. Just as we do in a live meeting, we bring only ourselves to a virtual meeting without distractions.

You do not need your own Zoom account to join a 12-Step meeting, just the Zoom app on your device.

If you do not have the app yet, you can download it at https://zoom.us/download, or you can get the free Zoom app from the App store.

If you do not have a Zoom account, please skip to "Using Your Zoom App To Join A Meeting."

If you do have a Zoom account:

1. First, be sure you are signed out of your Zoom account on all of your devices (laptop, desktop, tablet, smart phone). Go to Zoom.us and, if you see your account information, then select "SIGN OUT" from the dropdown menu in the upper right-hand corner (by clicking either your picture or a gray head and shoulders). If you see a "SIGN IN" option, you are already signed out. Then, *close that browser window*.
2. Sign In through the Zoom app, change your Virtual Background[1] to "None," then SIGN OUT of your account.

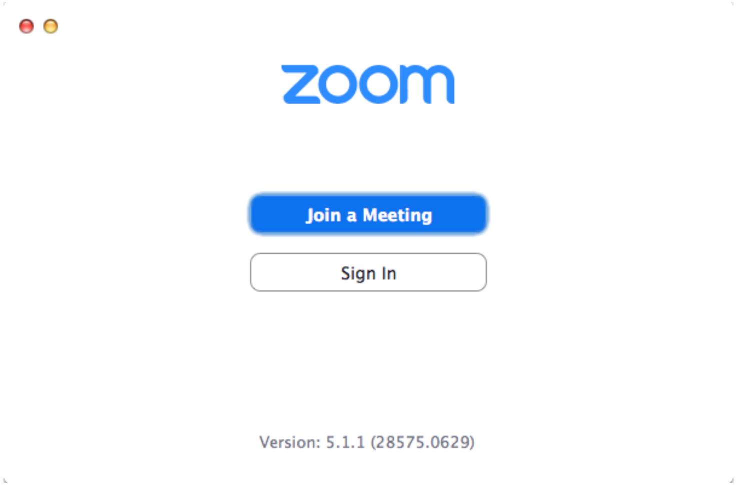
You are now ready to Join a Meeting.

[1] Virtual backgrounds are discouraged in most 12-Step meetings, as they create a security risk and are an unnecessary distraction for other participants.

USING YOUR ZOOM APP TO JOIN A MEETING

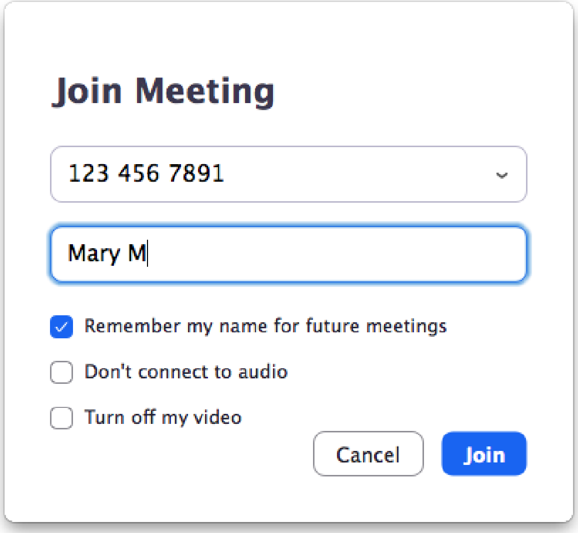
Open your Zoom app.

On the popup window, select “Join a Meeting.”



On the next popup window, manually enter the meeting ID and your first name and last initial.[2] The down arrow will also allow you to choose the meeting ID if you have used it before.

[***NOTE:*** *The only box checked on this popup window should be “Remember my name for future meetings.”*]



Join Meeting

123 456 7891

Mary M

☑ Remember my name for future meetings

☐ Don't connect to audio

☐ Turn off my video

Click the blue “Join” button.

On the subsequent popup window, enter the meeting password/passcode.

[2] In some 12-Step meetings, participants are not able to rename themselves; so it is best to do it here.

Click the blue “Join Meeting” button, and the Host will let you in shortly.

Always join with video.

While you are in the Waiting Room, the Host or a Co-Host may send you a message via Chat. Even though you will not be able to reply, please follow the instructions carefully. Any delay in admitting you to the meeting room itself can be attributed to safety concerns, so please do not take it personally.

IN-MEETING ETIQUETTE

In preparation for the meeting, gather your reading materials. As we do in a live meeting, we will be reading from one or more books, pamphlets, and/or other printed resources.

Once you enter the meeting room, please ensure that your video is on so you can be seen by the Host and Co-Host(s), at least long enough for them to identify you as a legitimate participant. If you enter the meeting with your video off, you are likely to receive a Chat message from the Host or Co-Host(s) asking you to turn on your video briefly; and now that you are in the meeting room, you will be able to reply via Chat.

If you do not respond to the request to show video, you may be returned to the Waiting Room where you will receive another Chat message request. Some meetings will remove participants who are unwilling to show video for identification. If you are removed, you will not be able to return to the meeting until the following week.[3]

To minimize distractions for other participants in the meeting, please sit as still as you would in a live meeting. If it is necessary for you to do something other than sitting attentively, please turn your video off.

Please remain muted throughout the meeting unless you are reading or sharing.[4]

At some point, and at the Host’s discretion, the meeting may be locked without notice. You are free to leave after the meeting has been locked, but you will not be able to return.

IN-MEETING FEATURES

The Zoom menu bar appears at the bottom of the Zoom window; and from left to right, you can mute/unmute your audio, stop/start your video, view a list of participants, send and receive chat messages (when the Host opens Chat), and leave the meeting.

In Gallery View on a desktop or laptop,[5] the Zoom window displays up to 25 video thumbnails of meeting participants per gallery screen (through which a participant can scroll with left and right arrows) and up to 49 video thumbnails in Full Screen mode. In Speaker View, the participant sees in the Zoom window only the individual who is speaking at that time.

[3] If you are removed accidentally, it may be possible for you to return to the same meeting while it is underway by using a different device.

[4] Some 12-Step meetings may not allow participants to unmute themselves.

[5] On a smart phone, iPad, or tablet, as few as four participants at a time can be viewed.

By clicking on “Participants” in the Zoom menu bar, a list of all meeting participants appears to the right of the Zoom window. At the bottom of this list is a “Raise Hand” button that you can use if you would like to speak. When clicked, a blue hand icon will be positioned next to your name on the Participants list. The Host and Co-Host(s) will see the names attached to these blue hands in the order that they were raised.

By clicking on “Chat” in the Zoom menu bar, this feature will appear. Using this feature, you will be able to Chat privately with the Host or Co-Host(s). During the last ten or fifteen minutes of the meeting, Chat may be opened for “Everyone Publicly” so that phone numbers can be provided to newcomers and information can be posted for all participants regarding literature, Tradition Seven, and program-related announcements.

LEAVING A MEETING

To leave the meeting you are attending, click on “Leave” (in red to the far right on the Zoom menu bar), then click the confirmation “Leave the Meeting” button that appears (also in red).

If you wish to return to that same meeting after leaving, and the meeting has not been locked, you can do so by following the instructions for “Using Your Zoom App To Join A Meeting.” If you do this more than once or twice, however, you may be placed in the Waiting Room and then removed from the meeting by the Host or Co-Host(s), as this scenario typically indicates a security concern.

APPENDIX D

HOST SIGN IN / SIGN OUT INSTRUCTIONS

PREPARING TO START A MEETING

Only the scheduled Host of a meeting should start that meeting. It is most secure for the Host to start the meeting through the Zoom app (see instructions below), rather than to start or join a meeting using Zoom's web portal through a browser.[1]

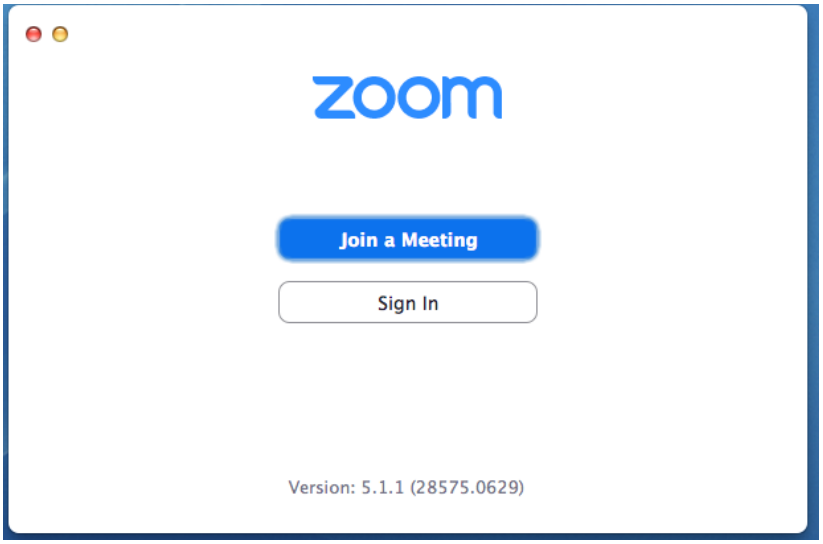
Each Co-Host should join the meeting through the Zoom app as a regular participant and, once in the meeting, can be made a Co-Host by the Host.

All Hosts and Co-Hosts should close all browsers, documents, and interactive software applications on their devices because every open file that is brought into a Zoom meeting is a potential gateway for hackers.

USING YOUR ZOOM APP TO SIGN IN AND START A SCHEDULED MEETING

Open your Zoom app.

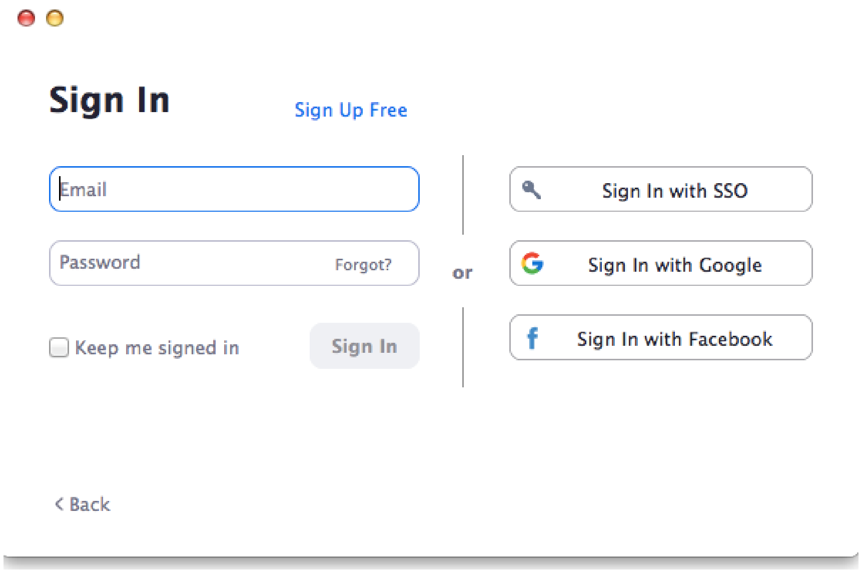
As the Host of this meeting, Sign In. (All other participants, including the Co-Host(s), are to select "Join a Meeting.")



Version: 5.1.1 (28575.0629)

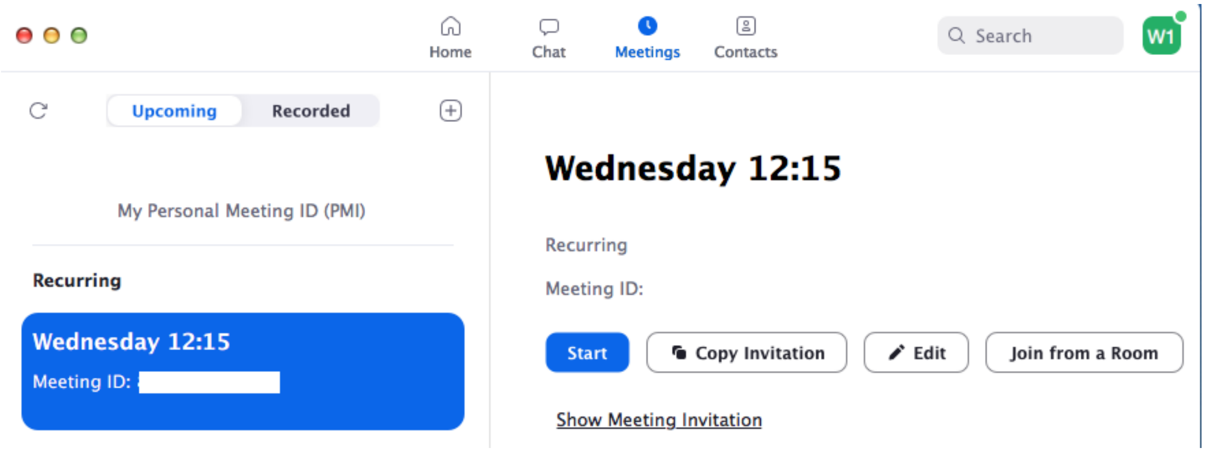
[1] As an example, two people were in a locked meeting when a third person suddenly appeared. This individual had bypassed the waiting room and overridden the lock on the meeting by using the Zoom web portal to enter with the email address and passcode.

On the “Sign In” popup window, enter the group’s email address and Zoom password (which will become known as a *passcode* in the future). The blue “Sign In” button will light up — click it to complete Sign In. Do not check the “Keep me signed in” box.



The “Meetings” popup window will appear (see below).[2] “My Personal Meeting ID (PMI)” is situated at the top of the list in the left pane of the window, followed by recurring meetings. (NOTE: Meeting ID is crossed out in the example below for safety.)

When you click on the meeting you are hosting from the list of recurring meetings, it will be highlighted in blue. Move to the right pane of the popup window and click Start (which is also highlighted in blue).



Wednesday 12:15

Meeting ID: [redacted]

Wednesday 12:15

Recurring

Meeting ID:

You are now in the meeting.

[2] If a different popup window appears than the one above, please sign out of the account using the dropdown menu on this “different” window, exit the Zoom app, and begin again. This ensures a clean Host entry into a meeting.

Click on “Participants” on the Zoom menu bar so the Waiting Room will become visible as participants arrive, then review your in-meeting settings.

IN-MEETING SETTINGS REVIEW

Under your Security popup menu, the following items should be checked by default — “Enable waiting room” and Allow participants to: “Chat” and “Unmute Themselves.” Participants should not be able to rename themselves. This is also the place where you can later Lock Meeting.

Under Chat, you can determine whether a Participant Can Chat With: No One, Host Only, Everyone Publicly, or Everyone Publicly and Privately.[3] These selections are available under the three dots (meaning “more”) in the lower right hand corner of the Chat box.

Set your initial Chat checkmark to “Host Only,” which will allow the Host and Co-Host(s) to Chat privately with each other, with individual participants in the meeting, or with everyone in the waiting room. Individual meeting participants can also Chat with a Host or Co-Host.

After the meeting is locked, you can open Chat to Everyone Publicly. Please note that the Host and Co-Host(s) can continue to Chat privately under this selection. It is best NOT to allow any other participants to Chat privately with one another.

Screen Share should not appear on your Zoom menu bar, and Chat is not designed or intended to be used as a substitute for this feature.

SIGNING OUT

Always be sure to Sign Out of the group’s Zoom account after Ending the Meeting for All. To Sign Out, click on the icon in the upper right-hand corner of the “Meetings” popup window (the green “W1” in the previous example), which will display a pulldown menu. At the bottom of this menu, select “Sign Out.”

[3] The option for “Everyone Publicly and Privately” will not appear on the Chat menu when “Private Chat” is turned OFF in Account Management settings, as recommended in Appendix B of this guide.

APPENDIX E

SAMPLE INSERT TO MEETING SCRIPT

[***NOTE:*** *The following script insert is designed to be read by the Secretary after the Suggested Welcome and the Serenity Prayer. This text can be shortened as the group grows accustomed to safety protocols and etiquette, and please remember that many of these requests rely on the honor system. The purpose of having the Secretary provide this information is to allow the Host to recede into the background as much as possible, as the meeting itself is managed by the Secretary.*]

We would like to remind you that joining this meeting through the Zoom app strengthens our security.

There will be no screen sharing during this meeting, so please grab whatever you have at home so you can read to the rest of us from your program literature.

Please remain muted unless you are reading or sharing, sit as still as you would in a live meeting, and turn off your video if what you are doing could be distracting to others.

Dial-in phone calls and virtual backgrounds are not allowed; and no participant can change his or her name while in the meeting, so your hosting team will do that for you.

In the interest of anonymity, please refrain from recording, photographing, or taking screenshots of any portion of this meeting; and please introduce to the group anyone who is in the room with you.

This meeting will remain open for 15 minutes after the closing prayer for fellowship.

Chat is now open to the Host only and could be closed at any time. The Host also holds the prerogative to lock the meeting without notice, after which you can leave but you cannot re-enter. Chat will be opened for everyone during the last ten or fifteen minutes of the meeting.

There is no longer an "Unmute All" button, so please unmute yourself at the end of the meeting to join in the closing prayer.

If there is a major Disruption, the meeting will be ended immediately by the Host and will not resume until next week.