



WHY ARE WE HERE? (updated) Over the last several months Zoom has stated that on September 28, 2020, certain mandatory practices would be enacted on all meetings set up through a paid subscription: each meeting would have to have utilize either a Waiting Room or a Passcode. To be clear, Zoom is using the word *passcode* to describe the entrance code to join a room; this is not the same as an individual's *password* to log into Zoom. for purposes of this memo and workshop, we will follow the Zoom vernacular and use passcode to describe the mandatory code to enter a meeting room on Zoom.

Because this change may affect how many AA meetings on resume platforms operate. This guide and workshop are were designed to explain these changes, and offer solutions based on the experiences of groups to ensure this transition runs smoothly and the virtual doors of AA remain open. Without exception, any meeting that lasts an hour or longer is connected to a paid subscription, in turn, affected by these changes.

Last week, Zoom decided to hold off implementing these mandatory changes until November and added a third alternative to Waiting Rooms and Passcodes. This third alternative is Authentication. It is uncertain whether these changes will be implemented in November, however, our experience has shown that many AA group are using one or more of these measures already and we wanted to explain them to you.

WAITING ROOMS

What types of meetings will the affect: This requirement of having a waiting room will affect all meetings that do not currently have a passcode. As a practical matter, this will also affect meetings that use the following tools and options:

- 1) meetings without passcodes that allow people to join before the host
- 2) meetings without passcodes that utilize host codes to transfer between multiple chairs and secretaries
- 3) virtual spaces that are shared and utilized consecutively by various meetings
- 4) all meetings without passcode where people arrive late (in other words, all meetings)

What is a waiting room on Zoom?



As the name suggests, a waiting room on Zoom is simply a place where all persons who seek to enter the meeting are held before passing through the virtual doors into a meeting. In order to pass through the waiting room an administrator, post, or cohost, must let the person in. Entrance can either be granted on an individual basis or on a group basis when there are multiple persons in the waiting room. *It is impossible for persons in the waiting room to see or talk to each other in the waiting room.*

Operational Note: Please remember it is currently impossible to have private conversations and/or two-way conversations with persons in the waiting room. Currently, a host or cohost can only send messages to all people in the waiting room.

In order to effectively utilize these new functions, it may be helpful to be aware of certain terms as applied in Zoom:

Administrators – refers to persons who initially “start” the meeting usually from the website portal (rather than the application). For our purposes, those who login with the “Administrator Login Information” (described below) are administrators. By default, Zoom makes them the initial host upon entry¹. They have all the same powers as a host (including transferring) and is the initial host. Unlike a host, anyone who is administrator or logs in with the administrative login information can reclaim host and has power to enable tools via the portal.

“Administrator login information” – as used in this handout, refers to the email address and password used to establish the Zoom meeting room in which a group meets.

Hosts –have access to all the same utilities that administrators and cohosts have, including security features, lower all hands, chatting controls, etc. Unlike a cohost, a host has the ability to transfer hosting to another person and to designate or undesignated cohosts in a meeting. There is no limit to the amount or number of cohosts one has in the meeting.

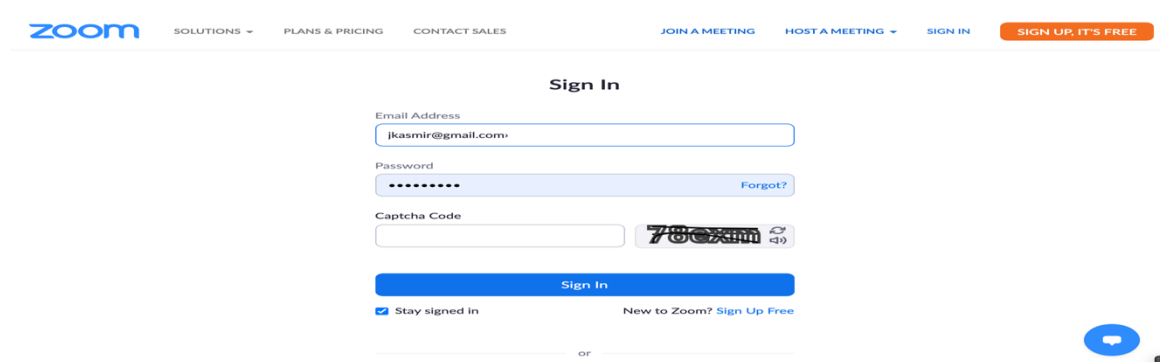
Cohosts - have access to all the same tools as a host except does not have the abilities to transfer or name a host, nor can they designate or undesignated another cohost.


¹ It is possible for more than one person to login using the administrative login information. When that happens, the first person who logged in with the administrative login information becomes a cohost, and the most recent person to login with the administrative login information is the host.

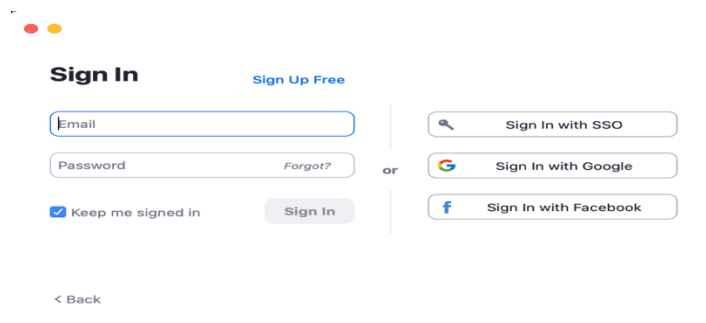
Host Keys – prior to this recent change in Zoom, host keys were used in some meetings with certain entrance rules to allow someone to assume the hosting role. With this change, host keys take on a slightly different role and will necessitate also having a password. ***If your meeting used host keys, it is important to please read the section below on Host Keys***

Website Portal and Application Access:

All users can access their Zoom accounts in at least two ways: 1) via the website portal and 2) via the application. Accessing Zoom through the **Website Portal** involves going to <https://zoom.us/signin> and following the prompts to sign in. **Signing in as an administrator will be covered below**) The Website Portal sign in looks like:



By contrast, accessing the Zoom Application, usually begins by clicking on an icon that looks like this:  Then the sign in looks like:



As referenced above, in both of these logins, you may be asked to enter your password (**again, this refers to your personal login code that you created when you signed up.**)

ADMINISTRATIVE LOGIN INFORMATION

In Zoom, every meeting is tied to an email address and password. We are referring to this information in this handout as the Administrative Login Information because *this is the information needed to login as an administrator.*

In many instances, a group will create an email address for purposes of creating a Zoom meeting space. Using a group email address is suggested for three reasons:

- 1) Protecting Personal Information: There have been instances of Zoom hacking where infiltrators hack (or break into) an account. By using a group email address instead of an individual's personal email address, each person's individual emails and personal information is protected
- 2) Many different individuals may need Administrative Login: As described below, groups that use waiting rooms that have multiple meetings or numerous chairs will need to have the Administrative Login Information in order to become the host of a meeting.
- 3) Anonymity: As with many things in our program, any time that personal information is used, there is a risk to anonymity. Using a personal email address or Personal Zoom account creates a risk to anonymity.
- 4) A note about Enterprise Service and Anonymity: Admittedly, this is a little technical, however, it is worth explaining here. Zoom allows for the creation of enterprise accounts – which is one of many tools Zoom offers so that multiple meetings can occur simultaneously and independently of each other by other Zoom account holders. In an enterprise system, members are added to the enterprise.

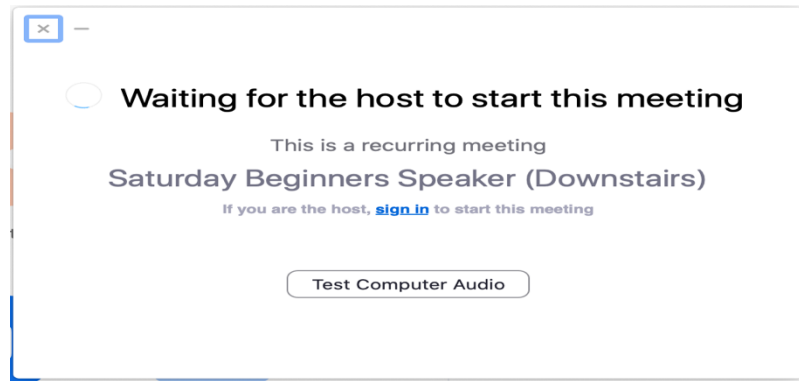
The issue arises that an enterprise intertwines with a personal zoom account and disables its independence. Every use of the personal account will include the enterprise information.

Example: Bill W has a personal zoom account with his personal email that he uses to set up a group meeting. The group then transfers onto an enterprise account. Since Bill W's personal zoom account was used, any time Bill W uses Zoom, for any purpose, including non-AA related events, the enterprise information will appear and can therefore compromise his anonymity.

If a group uses an email account only for the group meeting on Zoom, then the only time the enterprise information is seen is in recovery related information.

IMPORTANT PRACTICAL MATTERS REGARDING THE USE OF WAITING ROOMS

- I. **WAITING ROOMS PREVENT PERSONS FROM ENTERING THE ROOM BEFORE THE HOST/ADMINISTRATOR:** Use of a waiting room prevents anyone from entering a virtual meeting space before the host/administrator. Absent a host opening the room, attendees will be stuck in a waiting room. They will just see a window that looks like this:



- II. **WITH WAITING ROOMS HOST KEYS MUST BE ACCESSED WITH THE ADMINSTRATOR LOGIN INFORMATION**

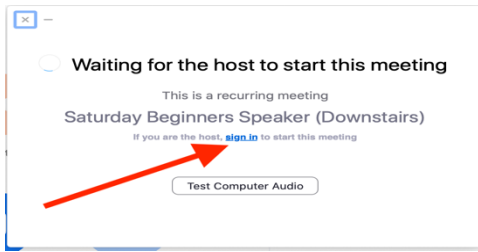
HOST KEYS DO NOT WORK without the administrator login and passcode, no one can become a host.

The “old” system: Often times AA groups that met frequently or had several different chairs utilized the *host key* option. In this situation, anyone could enter the room without a passcode. Then the chairs could “claim host” (i.e., become host in name and with all the powers that come with that title) once inside the room by pressing a button and entering a “host key” (a special numeric code). Host codes effectively eliminated the need for an Administrator to be present and open up the room.

Waiting rooms (as currently offered on Zoom) prevent such a simple process. Unless someone has the administrator login information, they cannot override the waiting room. Therefore, they cannot access the button to claim the host.

Two possible solutions: Given the way Zoom currently operates, there are two means of using host keys.

Solution One: Give all the chairs the administrative login information. As shown above, if a meeting chair tries to enter the room before the host, there is a link that can be pressed for them to log in as host.



When this link is pressed, the application login window reappears. They will need to enter the administrative login information (again, this is the email address and password used to create the room, not the individual host's personal login information).

Solution Two: Use Passcodes. As discussed, *passcodes* are an alternative to waiting rooms altogether. Many meetings use passcodes, that are distributed to all attendees and allow them to enter the room. *If passcodes are in effect, then the "old" system can still be utilized.*

III. **WAITING ROOMS CANNOT BE TURNED OFF ONCE A ROOM IS OPEN, IT IS THERE THROUGHOUT THE ENTIRE MEETING**

Waiting rooms are in effect throughout the duration of the meeting, therefore an administrator, host or cohost must monitor the waiting room to allow latecomers to enter. When someone enters the waiting room, notifications appear on the screens and in the participant lists of anyone designated as a host or cohost.

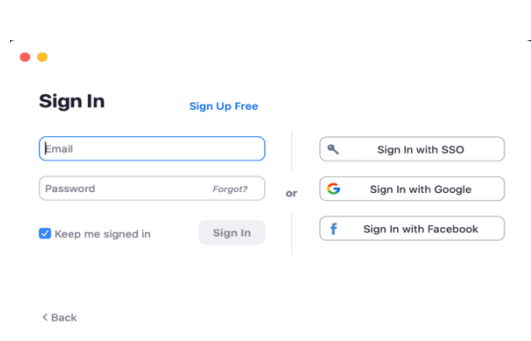
Solution: Experience has shown that it is a good idea to have a designated person or persons throughout the meeting to monitor the waiting room. It is a simple function, and another opportunity for a fellow to do service. It is further suggested, that the waiting room monitor (aka spiritual door person or maitre d') not have responsibilities for monitoring the room for trolls, Zoom bombers, etc.

Like a greeter, experience suggests that the spiritual door person arrive well before the meeting begins to serve this purpose.

IMPORTANT PRACTICAL MATTERS REGARDING THE USE OF PASSCODES

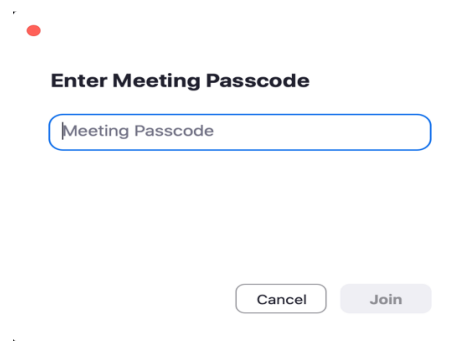
To reiterate, PASSCODE refers to the code that is used to enter a meeting room. A PASSWORD is used by an individual to log into zoom either via web portal or application.

PASSWORD:



The screenshot shows the Zoom Sign In page. It features a 'Sign In' header with a 'Sign Up Free' link. Below the header are input fields for 'Email' and 'Password', with a 'Forgot?' link next to the password field. There are three social sign-in options: 'Sign In with SSO', 'Sign In with Google', and 'Sign In with Facebook'. A 'Keep me signed in' checkbox is checked. A 'Sign In' button is located at the bottom right of the form. A '< Back' link is visible at the bottom left.

PASSCODE:

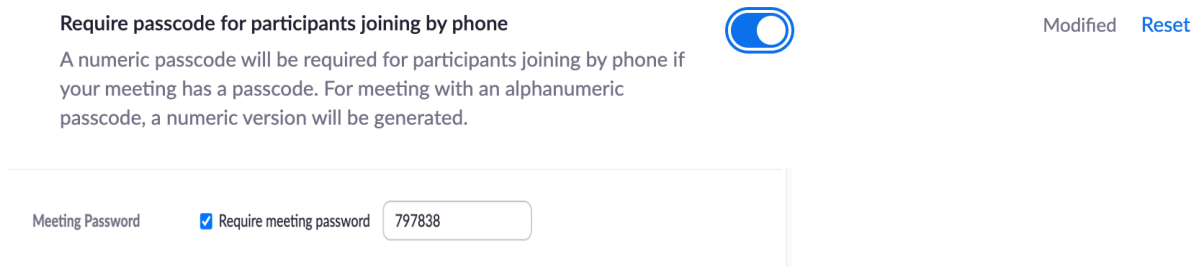


The screenshot shows the Zoom 'Enter Meeting Passcode' page. It features a single input field labeled 'Meeting Passcode'. Below the input field are two buttons: 'Cancel' and 'Join'.

I. Setting Up passcodes

Among the most effective ways to protect a meeting is using a passcode, it need not be a complicated one. Many groups have enacted passcodes to prevent zoom bombers and trolls. In my experience, a zoom bombing can interrupt any serenity gained in a meeting and traumatize a newcomer.

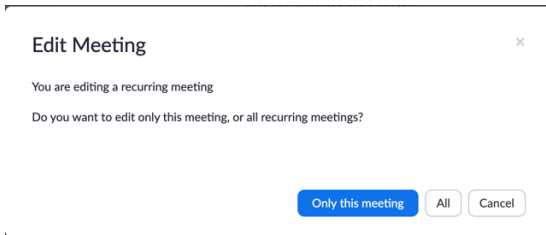
Enacting passcode for a scheduled meeting merely requires the administrator to log into the **portal** and select the meeting. Then edit the meeting and check the box that indicates “require meeting passcode.” ***Where you have a recurring meeting, it is easy to edit all meetings and ensure the same passcode is used consistently.***



The screenshot shows the Zoom meeting settings page. It features a toggle switch for 'Require passcode for participants joining by phone', which is currently turned on. Below the toggle is a text box with the following text: 'A numeric passcode will be required for participants joining by phone if your meeting has a passcode. For meeting with an alphanumeric passcode, a numeric version will be generated.' To the right of the toggle are the words 'Modified' and a 'Reset' link. Below this is a section for 'Meeting Password' with a checked box for 'Require meeting password' and an input field containing the number '797838'.

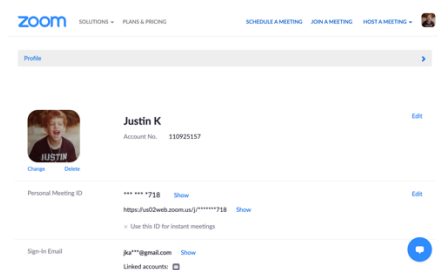
REMINDER PLEASE REMEMBER THAT WHEN YOU ARE MAKING A CHANGE YOU WANT TO AFFECT ALL YOUR MEETINGS EITHER SELECT A MEETING FROM THE MEETING LIST

AND USE EDIT ALL MEETINGS OR GO TO SETTINGS (Note: depending on the nature of the change may dictate which method is to be used.

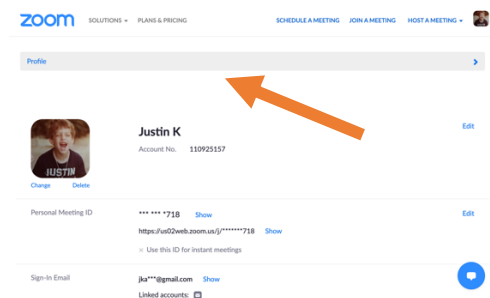


To get to Settings from the Portal Login:

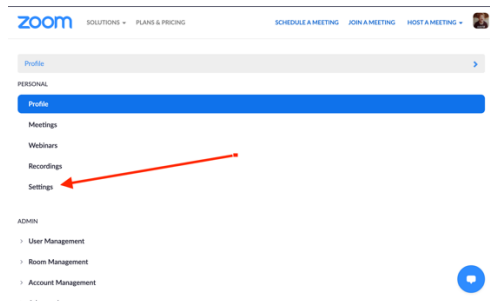
After you sign in at the portal you will be on the "Profile Page"



To access the "Settings" merely click the shaded bar that says profile and a drop down menu will appear with settings, click settings.



Click the shaded bar and end up at:



NOTE! ZOOM CHANGE IN PASSCODES

When a meeting is set up to require passcodes for entry, by default, Zoom also creates a passcode for those persons who dial in via telephone. The Dial In passcode can be disabled without disabling the passcode for people who Zoom into the meeting.

To disable this dial-in passcodes, log into with the administrative login information and edit the scheduled meeting(s).

Require passcode for participants joining by phone



A numeric passcode will be required for participants joining by phone if your meeting has a passcode. For meeting with an alphanumeric passcode, a numeric version will be generated.

Accessibility issues -- auto-reply: The accessibility question can be easily overcome by setting up a group email account with an autoreply giving out the passcode and/or a passcode embedded link. It is my experience with groups that zoom bombers will not put that much effort into trolling a meeting. Many groups also place a suggestion into the email requesting that this information not be posted on social media.

To protect the virtual meeting space, many groups do not post a passcode embedded link on Intergroup or other AA Meeting Website. Instead they direct inquirers to send an email to the group email.

A *passcode embedded link* will contain the letters “pwd” in the link. For example:

Invite Link

<https://us02web.zoom.us/j/85638080077?pwd=UUZYeDNxbUg1cjhQZ2ZVYVh4YnR4UT09>

Copy Invitation

To generate a passcode embedded link for a password protected meeting, the administrator via the **portal** would go into settings and toggle the section for password embedded link. Then, once enacted, the meeting link for a particular meeting should contain the password.

Embed passcode in invite link for one-click join



Modified [Reset](#)

Meeting passcode will be encrypted and included in the invite link to allow participants to join with just one click without having to enter the passcode.

Only occasionally do queries for passcodes end up in a spam or junk mail folder. Again, this can be overcome by creating a service position to monitor the junk mailbox periodically

IMPORTANT PRACTICAL MATTERS REGARDING THE USE OF AUTHENTICATIONS

As referenced above, in late September 2020, Zoom reversed its prior decision to mandate either passcodes or waiting rooms on September 27, 2020. According to their latest email, in November, all meetings on paid Zoom accounts will now have to employ one (or more) of three options: waiting rooms, passcodes, or authentications. Waiting rooms and passcodes are described above. This section describes authentications.

AA Note: Several meetings in Manhattan have already activated the authentication requirement as a security measure for their meetings, and it has been fairly effective in prevented unwanted intruders. **Zoom is in the process of enhancing this feature.**

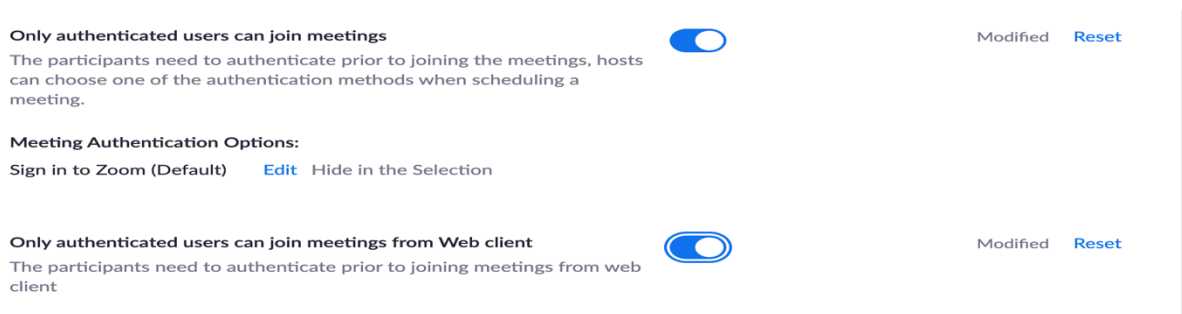
WHAT IS AUTHENTICATION: Authentication in Zoom simply means that anyone who wishes to join a Zoom meeting (other than by dialing in) must have a Zoom account. As most of you know, setting up a Zoom account is free. When a person has set up a zoom account, the authentication requirement is satisfied.

Note on a misconception on free Zoom accounts: **Participation in meetings lasting longer than 45 minutes do not require paid accounts.** It is true that according to Zoom, a free account appears to limit the length of a Zoom meeting to 45 minutes. However, this is *only true* if the free account creates the meeting. Meetings set up on paid accounts can last any length of time and anyone with any account (free or paid) may join for the length of the entire meeting.

Benefit to Authentication: the primary benefits to authentication are that it prevents anyone who finds a list of meetings from just hacking into or zoom bombing the meeting. With authentication, the unwanted guest can be removed from the meeting and prevented from rejoining. Moreover, with Zoom's reporting feature, these persons can also be prevented from invading other places and causing havoc.

Activating Authentication:

In order to activate authentication, the administrator logs into zoom with the administrative login information and then modifies the meeting settings at the following points:



The screenshot shows two settings for authentication in Zoom. The first setting, "Only authenticated users can join meetings", is currently turned on (indicated by a blue toggle switch). Below this setting, there is a description: "The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting." To the right of the toggle are links for "Modified" and "Reset". Below this is the "Meeting Authentication Options:" section, which lists "Sign in to Zoom (Default)" as the selected option, with "Edit" and "Hide in the Selection" links next to it. The second setting, "Only authenticated users can join meetings from Web client", is also turned on. Its description is "The participants need to authenticate prior to joining meetings from web client". It also has "Modified" and "Reset" links to its right.

Based on this screen it appears that more authentication methods will be offered by Zoom. As such, we will just have to see what happens more will be revealed! Stay Tuned!!