→ COVID-19 Information and Vaccine Requirements
(https://www.riohondo.edu/student-health-services/coronavirus/)

About Information Technology Services

For updates about our online instruction, remote student services and other resources during this time, please go to this link: https://www.riohondo.edu/student-health-services/coronavirus/#students (https://www.riohondo.edu/student-health-services/coronavirus/#students)

The Information Technology Services department (ITS) supports the College's IT services such as e-mail, telephone, internet access, Wi-Fi, website maintenance, Banner, Access Rio, SARS-Anywhere, tech training, etc.

We are dedicated to providing quality and timely support to the campus community.

If you need assistance with your account, network access, telephone system, moving your computer, or anything IT related please contact us through the help desk. (/its/helpdesk/)

Help Desk

(http://www.riohondo.edu/its/helpdesk/)

✓ Training

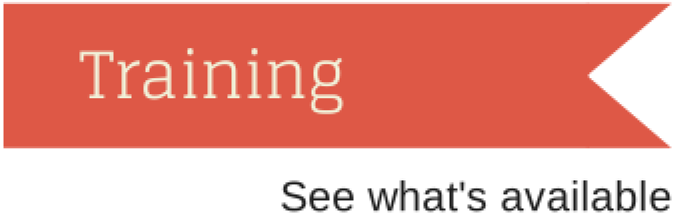
(http://www.riohondo.edu/its/technology-training/)

Audio / Visual

(http://www.riohondo.edu/its/av/)

→ COVID-19 Information and Vaccine Requirements
(https://www.riohondo.edu/student-health-services/coronavirus/)

Technology Training



We support you! Training is available for individuals or groups by appointment for Canvas, SARS Anywhere, SARS Anywhere Admin, SARS TRAK, Blackboard Connect, InformaCast, Office 365 (Word, Excel, PowerPoint, and Outlook), Microsoft Windows, WordPress, 25Live Pro, Cranium Cafe, Adobe Spark, and other campus software.

Setting Up Multi-factor Authentication in Microsoft 365

The first half of the video is an explanation about our MFA requirement for accessing your Microsoft 365 account. The second half of the following video is a short set of instructions on configuring SMS (text messaging) with your account as a second factor.

Video transcript

More information is available from Microsoft in the help article: Set up your Microsoft 365 sign-in for multi-factor authentication (https://support.microsoft.com/en-us/office/set-up-your-microsoft-365-sign-in-for-multi-factor-authentication-ace1d096-61e5-449b-a875-58eb3d74de14)

Banner Navigation Training – Banner 9

Banner Navigation Training is required for new staff users and is available upon request. Please obtain and complete a *Banner security form* from Human Resources prior to scheduling training. Banner Navigation Training usually takes ninety minutes to complete.

> *All training will be provided online using ConferZoom or MS Teams.*

SARS Software Products

We provide configuration and training support for the following SARS Products:

- SARS Anywhere
- SARS Admin
- eSARS Online Scheduling
- SARS Trak

Training for SARS Anywhere is available in three phases: appointment schedulers, office admin, and counselor.

SARS Anywhere (https://appointments.riohondo.edu/SARSAnywhere)

SARS Anywhere Admin

(https://appointments.riohondo.edu/SARSAdmin)

Campus and Faculty WordPress Training

Training is available for authorized faculty and staff to update their department or area's website. Please contact training using the form below to schedule WordPress training. Faculty, please use the request form here to obtain a faculty website (https://faculty.riohondo.edu/request-a-faculty-w ebsite/).

Microsoft/Office 365

Training is available for Microsoft/Office 365 products. Please contact training with your request and we will customize a presentation for your office and/or staff including Word, Powerpoint, Excel, One Drive, Teams, Sharepoint, and more.

- Login to Office 365 here. (https://portal.office.com)

TechConnect Zoom

Training is offered online when appropriate using CCC ConferZoom (http://conferzoom.org). ConferZoom is a collaboration and online meeting software provided by the CCCCO. It is available for all community college faculty and staff.

(https://conferzoom.org/ConferZoom/SignUp)

TechConnect Cloud – File and Media Storage

Faculty and staff have access to virtually unlimited file and media storage through the grant-funded 3C Media Solutions (http://3cmediasolutions.org) website. File and media can be made available publicly and linked to on websites or within the canvas LMS.

(https://3cmediasolutions.org/)

TechSmith Products

We have access to TechSmith Snagit, Camtasia, a (https://w w w.techsmith.com/)nd Knowmia (formerly Relay) (https://riohondo.techsmithrelay.com/) through the Distance Education office.

More Resources

The 3CSN Wayfinding Series (http://3csn.org/) is on-going daily training in many areas that faculty are requesting. This is a state-level resource.

(http://3csn.org/)

The Vision Resource Center (https://visionresourcecenter.cccco.edu/) is an online learning and collaboration platform for all professionals in the California Community Colleges.

(https://visionresourcecenter.cccco.edu/)

@ONE provides training and professional development (https://onlinenetworkofeducators.org/) to support the effective use of digital tools and platforms to make California Community Colleges a nationally recognized leader in online teaching and learning.

(https://onlinenetw orkofeducators.org/)

→ COVID-19 Information and Vaccine Requirements (https://www.riohondo.edu/student-health-services/coronavirus/)

Avoid The ZoomBomb

(March 26th, 2020) – tldr;

Open your ConferZoom account settings page and change the following

- https://cccconfer.zoom.us/profile/setting (https://cccconfer.zoom.us/profile/setting)
- Join before host – OFF
- Mute participants upon entry – ON
- Private chat – OFF
- File transfer – OFF
- Allow host to put attendee on hold – ON
- Screen sharing – ON with “Host Only”
- Disable desktop/screen share for users – ON
- Annotation – OFF
- Remote control – OFF
- Allow removed participants to rejoin – OFF
- Waiting room – ON

Download a formatted PDF of these instructions here. (https://s3-us-west-1.amazonaws.com/files.3cmedia/u_673/4136/How_to_avoid_the_zoombomb.pdf)

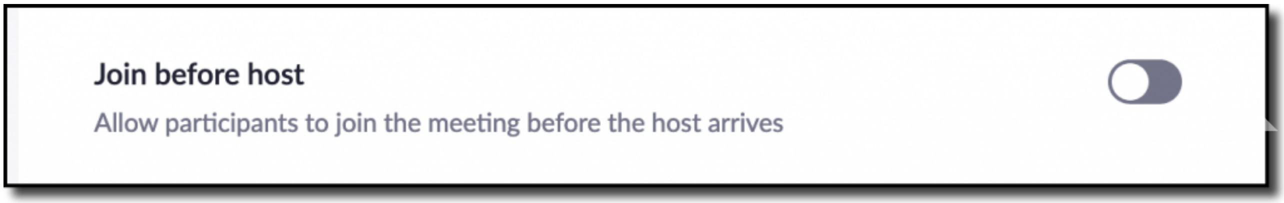
How to Avoid the “ZoomBomb”

These changes to the default settings are recommended for anyone who is hosting Zoom conferences open to the public or with children attending. Changing these settings will help you keep control of your meeting and focus on your content.

Join before host

The participants could be having a party without you there to monitor.

Recommendation: Turn it off



Join before host

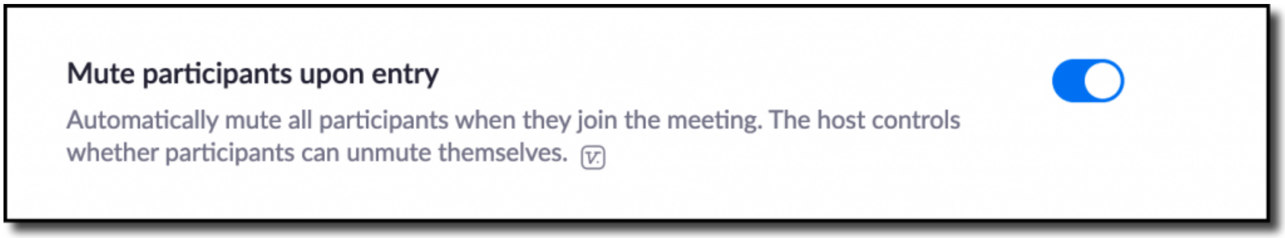
Allow participants to join the meeting before the host arrives

Mute participants upon entry

Barking dogs and crying babies can take over your meeting unintentionally. So can the participant who is singing their favorite heavy metal song at the top of their voice.

You might also consider disallowing participants to unmute themselves. In that case participants can use the “Raise hand” feature or the chat room to indicate when they want to speak. You can manually unmute them.

Recommendation: Turn on



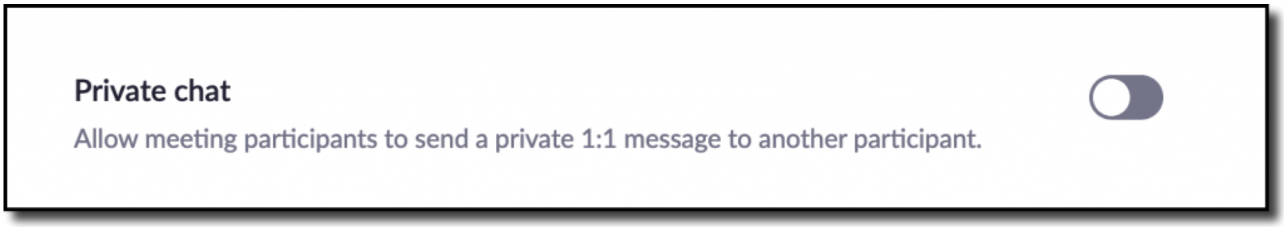
Mute participants upon entry

Automatically mute all participants when they join the meeting. The host controls whether participants can unmute themselves.

Private chat

The chatroom is one of the key ways to get live feedback and participation with your participants. We want to see all the communication that is happening. Disabling private chat will help tamp down any possible bullying or harassment during your meeting. They can use discord or text messages if they need a backchannel.

Recommendation: Turn off



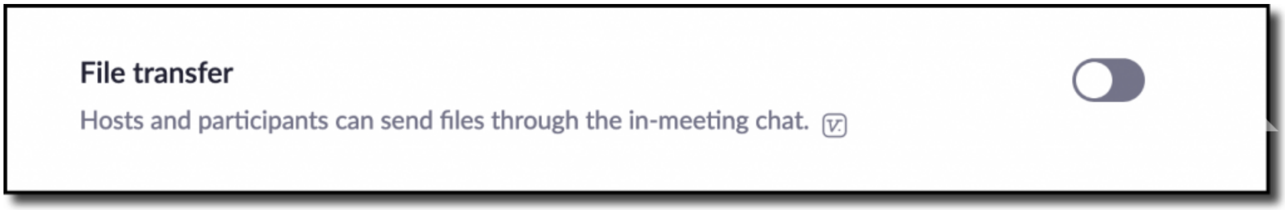
Private chat

Allow meeting participants to send a private 1:1 message to another participant.

File transfer

The ability to send files to your participants is very handy for you. Not so helpful if the participants are sending inappropriate (even unintentionally) files/gifs/images to the group. Put your files on Google Drive, Dropbox, 3C Media, etc. and give them download links.

Recommendation: Turn off



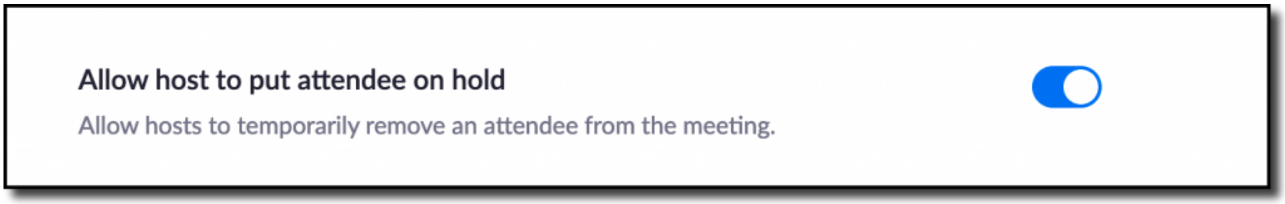
File transfer

Hosts and participants can send files through the in-meeting chat.

Allow host to put attendee on hold

Sometimes participants have environmental consideration that require you to step in and pause them. The participant could have someone enter the room. They could have a TV running behind them. They might have forgotten to dress appropriately…

Recommendation: Turn on



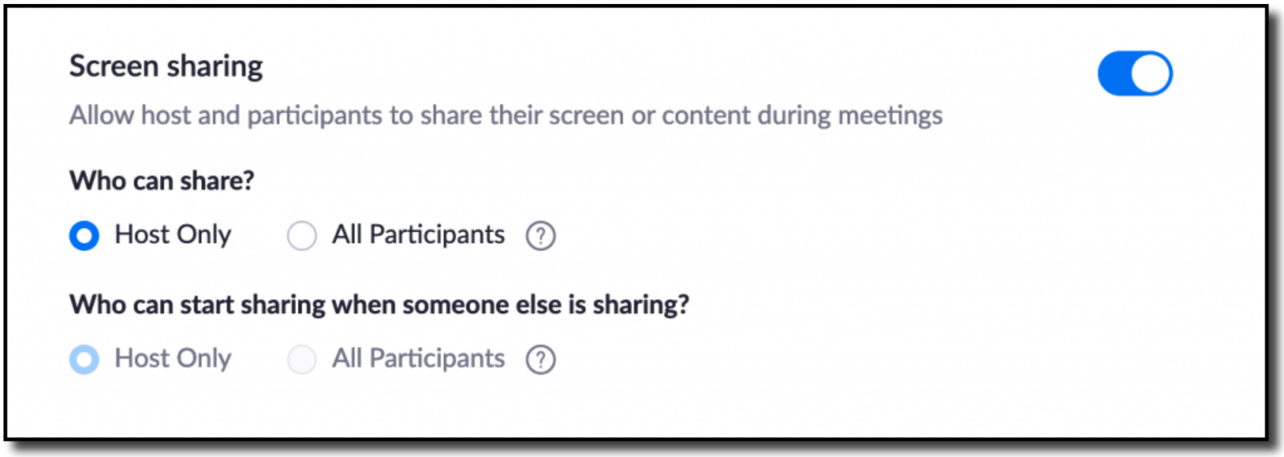
Allow host to put attendee on hold

Allow hosts to temporarily remove an attendee from the meeting.

Screen sharing

Your company department meeting is a great place for colleagues to share their business work with the group. Your classroom might not be. Participants can take over the session share and put anything they would like on screen for all in attendance. You can make a participant a co-host if you would like someone else to share their screen.

Recommendation: Turn on "Host Only"



Screen sharing

Allow host and participants to share their screen or content during meetings

Who can share?

● Host Only ○ All Participants

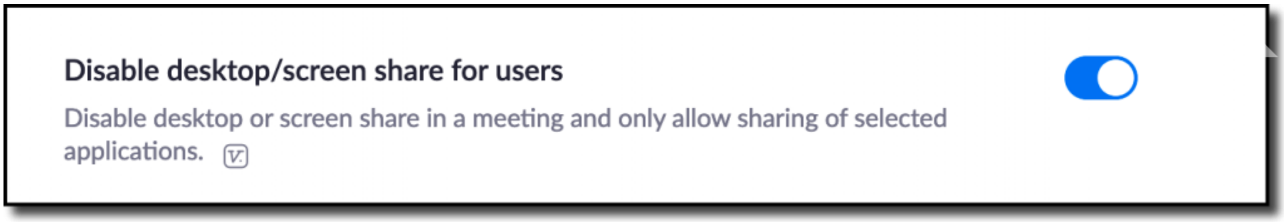
Who can start sharing when someone else is sharing?

● Host Only ○ All Participants

Disable desktop/screen share for users

We don't need to see the personal photos and information of your co-host when they share. This setting will enable them to share an Application (Powerpoint, Firefox, Chrome, Powershell, etc.) only. You should consider only sharing applications yourself.

Recommendation: Turn on



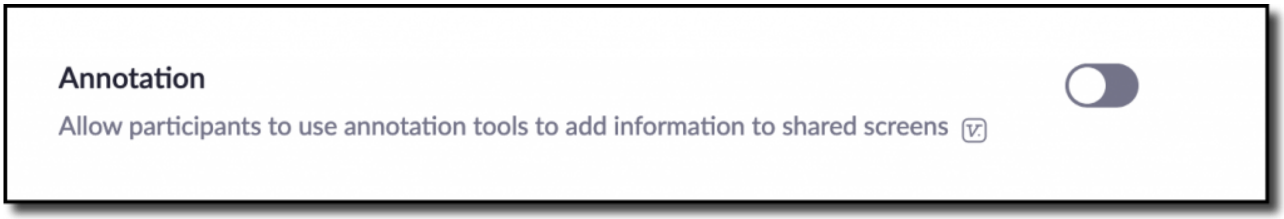
Disable desktop/screen share for users

Disable desktop or screen share in a meeting and only allow sharing of selected applications.

Annotation

Annotation gives you the ability to “draw” over the screen. It also gives that to your participants. They can draw anything that comes to mind over your presentation, your face, or anything else.

Recommendation: Turn off



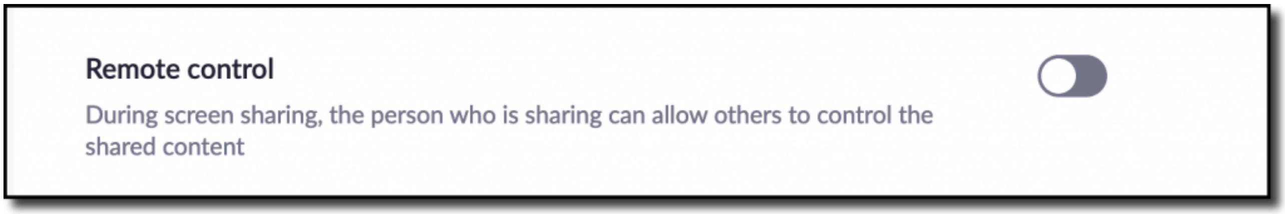
Annotation

Allow participants to use annotation tools to add information to shared screens

Remote control

This is a handy support feature in a 1:1 session. You don’t want participants constantly requesting remote control of your desktop during meetings.

Recommendation: Turn off



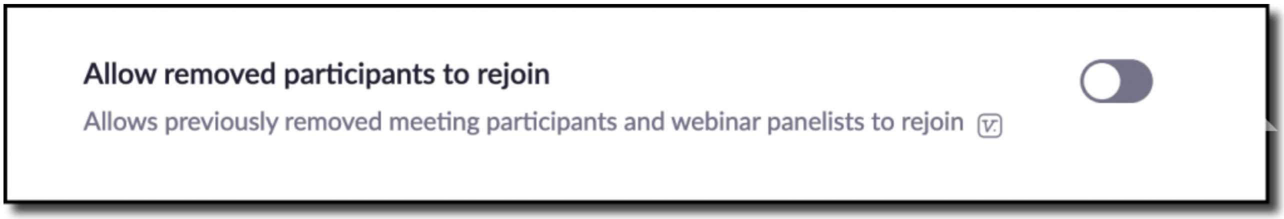
Remote control

During screen sharing, the person who is sharing can allow others to control the shared content

Allow removed participants to rejoin

When you kick someone out of your meeting for any reason, they shouldn’t be able to come back.

Recommendation: Turn off



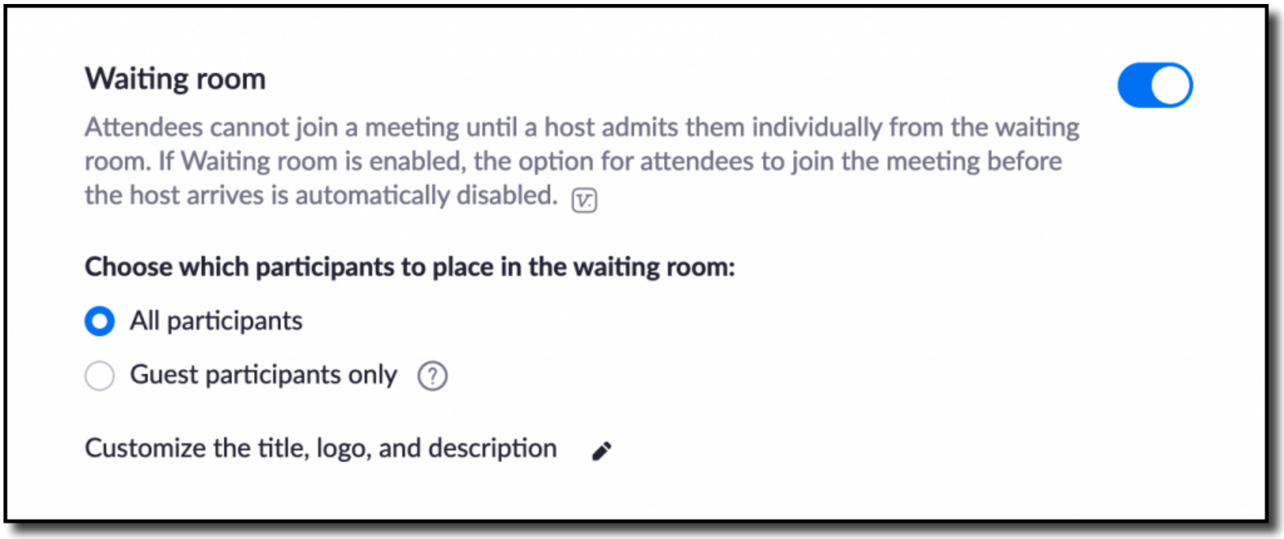
Allow removed participants to rejoin

Allows previously removed meeting participants and webinar panelists to rejoin

Waiting room

This is perhaps the most useful feature to help control your meeting or classroom. All participants will enter the waiting room before joining the main session. This allows you to let participants in as you are ready to receive them.

Recommendation: Turn on and customize



Waiting room

Attendees cannot join a meeting until a host admits them individually from the waiting room. If Waiting room is enabled, the option for attendees to join the meeting before the host arrives is automatically disabled.

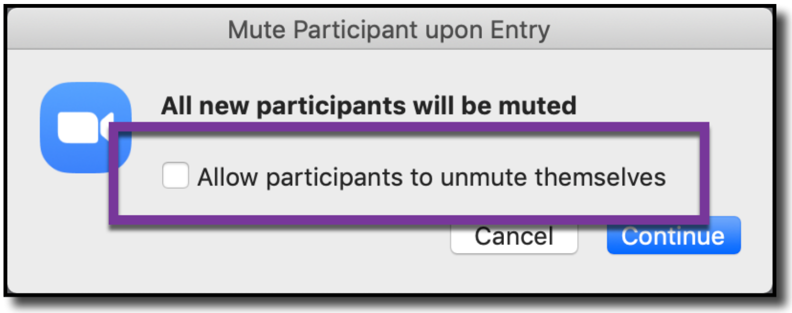
Choose which participants to place in the waiting room:

● All participants

○ Guest participants only

Customize the title, logo, and description

Optional – Consider locking your meeting once everyone is in attendance.



Mute Participant upon Entry

All new participants will be muted

□ Allow participants to unmute themselves

→ COVID-19 Information and Vaccine Requirements (https://www.riohondo.edu/student-health-services/coronavirus/)

Submit A Grant Request Using Adobe Sign

October 9th, 2020

> *Note: Please have your Staff Development Grant request paperwork completed and ready to upload prior to beginning this process. You will not be able to edit your application or make changes using this service.*

This tutorial will walk you through the steps of submitting your completed Staff Development grant request via Adobe sign.

Adobe Sign

Adobe sign is a software service that is avaialable to Rio Hondo college employees in order to obtain digital signatures. If you do not have an Adobe Sign account, please submit a request to the IT Help Desk first. Click here to visit the IT Help Desk (https://helpdesk.riohondo.edu)

Once you have activated your account you may login to Adobe Sign and begin your signature request.

Login to Adobe Sign

First, please login to your Rio Hondo Adobe Account:

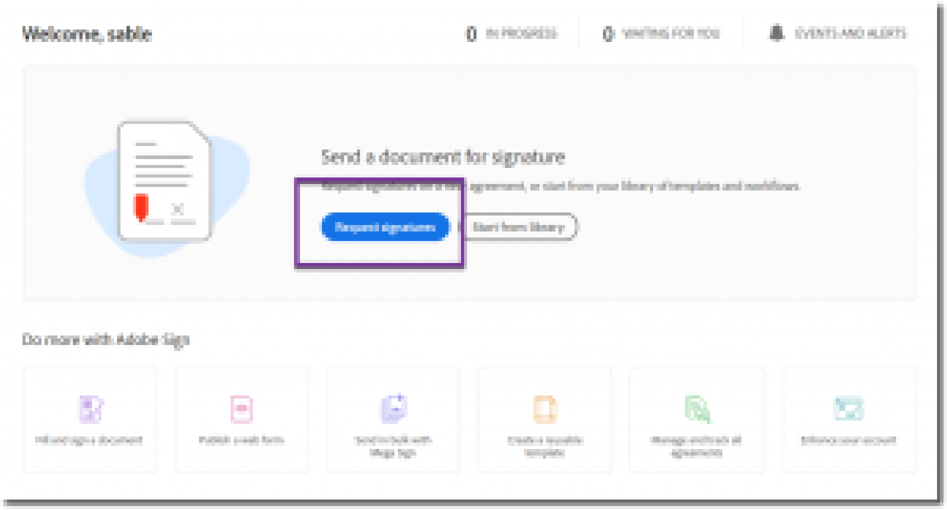
Login to Adobe.com (https://account.adobe.com)

Second, open a new tab and navigate to Adobe sign:

Click here to login to Adobe Sign (https://na1.documents.adobe.com/account/homeJS)

Send a Document for Signature

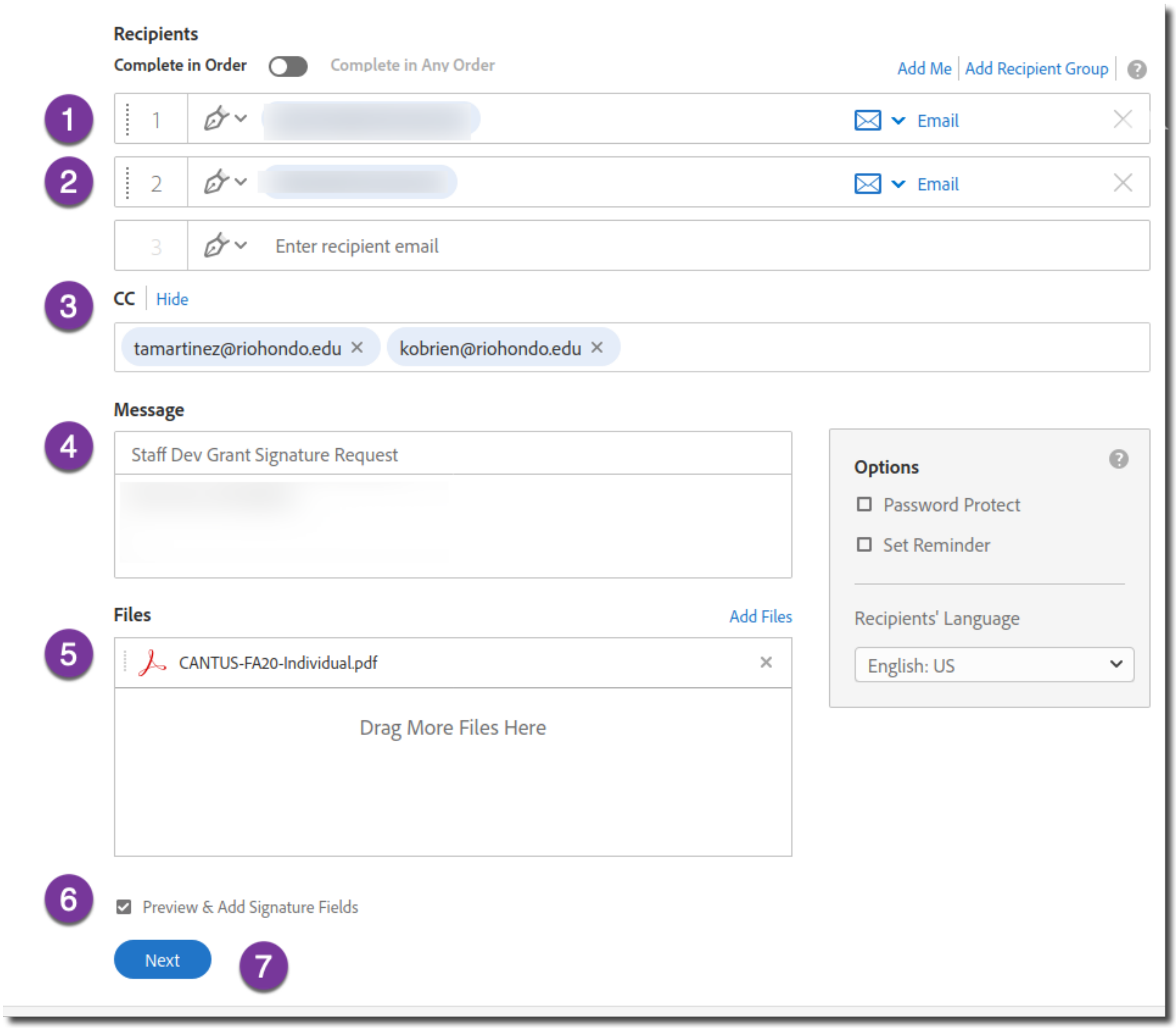
Select “Request Signatures” button from the page to begin your request.



Compose Your Signature Request

We are using Adobe Sign to send email to our Supervisor and then to our Vice President to sign. We will perform the following steps:

1. Input your Supervisor’s email address
2. Input your Vice President’s email address
3. Add Staff Dev as a CC
4. Compose your email message
5. Drag the **completed** application from your computer to Adobe Sign
6. Check the box to “Preview and Add Signature Fields”
7. Click Next



Recipients

Complete in Order ○ Complete in Any Order

1. 1 [redacted] Email
2. 2 [redacted] Email
3. Enter recipient email

CC | Hide

tamartinez@riohondo.edu ×
kobrien@riohondo.edu ×

Message

Staff Dev Grant Signature Request

[redacted]

Options

□ Password Protect

□ Set Reminder

Recipients' Language: English: US

Files

CANTUS-FA20-Individual.pdf ×

☑ Preview & Add Signature Fields

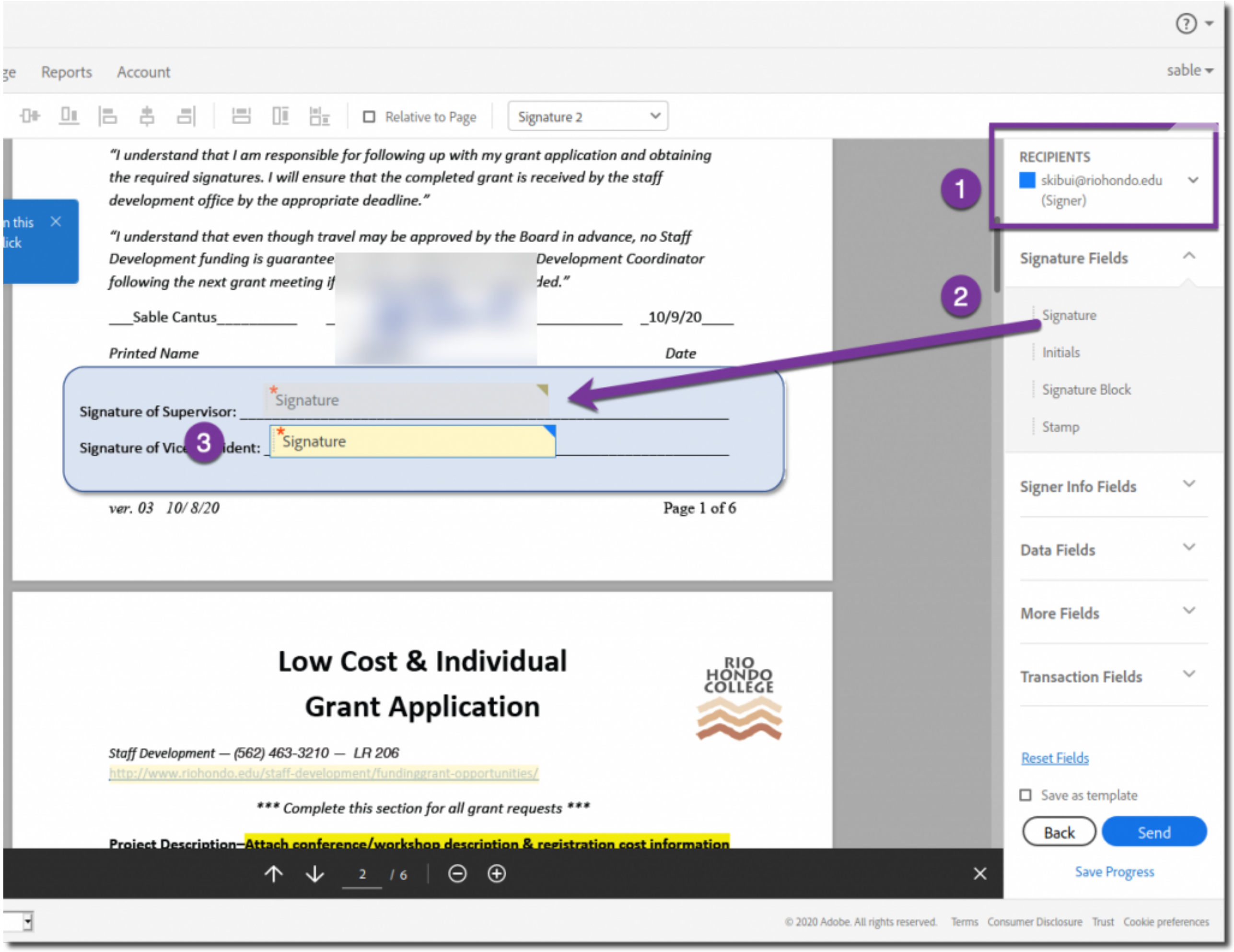
(https://www.riohondo.edu/its/wp-content/uploads/sites/2/2020/10/2-create-request.png)

Add Signatures

In this step we will add a signature block for your Supervisor and Vice President.

1. Check the recipient field
2. Drag the “Signature” from the “Signature Fields” block onto the grant request form

Do those steps again for the next recipient by using the dropdown arrow in the recipients field (#1).



"I understand that I am responsible for following up with my grant application and obtaining the required signatures. I will ensure that the completed grant is received by the staff development office by the appropriate deadline."

"I understand that even though travel may be approved by the Board in advance, no Staff Development funding is guarantee [redacted] *Development Coordinator following the next grant meeting if* [redacted] *ded."*

___Sable Cantus__________ _ [redacted] __________ _10/9/20____

Printed Name *Date*

Signature of Supervisor: ___ Signature ______________________________

Signature of Vic ident: _ Signature ______________________________

ver. 03 10/ 8/20 Page 1 of 6

Low Cost & Individual Grant Application

RIO HONDO COLLEGE

Staff Development — (562) 463-3210 — LR 206

http://www.riohondo.edu/staff-development/fundinggrant-opportunities/

****** Complete this section for all grant requests *****

Project Description–Attach conference/workshop description & registration cost information

RECIPIENTS

skibui@riohondo.edu (Signer)

(https://www.riohondo.edu/its/wp-content/uploads/sites/2/2020/10/3-add-signatures.png)Double check your work and hit Send. Please notify Staff Development when both signatures are complete.

Good luck!

→ COVID-19 Information and Vaccine Requirements (https://www.riohondo.edu/student-health-services/coronavirus/)

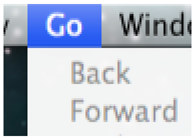
How To: Connect To A Network Shared Folder With Mac OS X

Your campus Macintosh machine is able to connect to campus resources using your network ID and password.

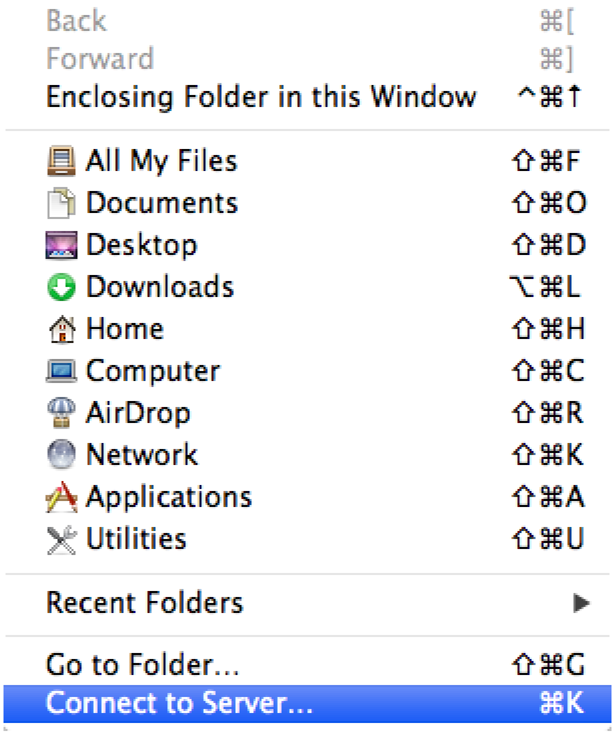
To connect to a networked share drive such as your “H drive” (the home folder) or the “P drive” (the public folders) your Mac must be connected to the campus network in one of two ways.

- Connected to the Rio-Secure wireless network
- Connected to a wired ethernet port on campus

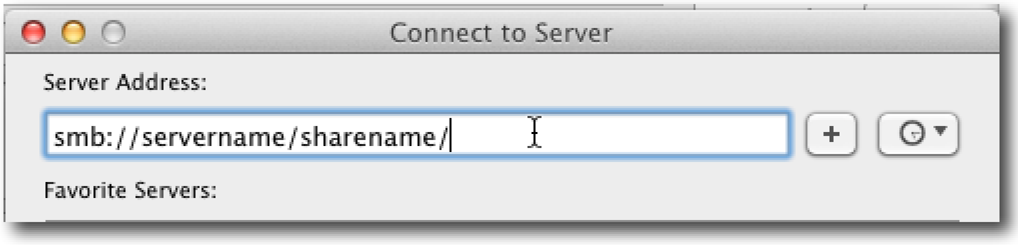
From the Finder, select Go in the Menu bar.



Select Connect to Server…



Enter the address of the network share



Server Address: smb://servername/sharename/

Windows network shares use the **Server Message Block** protocol and therefore begin with

smb://

followed by the name of the server you are connecting to.

smb://home880/users$/jfaculty

→ COVID-19 Information and Vaccine Requirements (https://www.riohondo.edu/student-health-services/coronavirus/)

Safe Email Tips

Our email inbox is a “lifeline” of sorts to the world. Email is what we use to communicate with our peers and students. It’s how we send proposals and request. And how we receive assignments.

Avoiding email is not a realistic proposition as email is often our primary focus when computing. Email is a primary attack vector to our personal data and computer systems. Email based computer attacks can be especially devastating whether the attacker is a malicious person or program (virus, worm, etc.).

We would like to offer a few tips on how to email safely.

Never Share Your Password

Email administrators should not ask for your password. Email administrators can reset your password if they need access to your account for trouble-shooting or problem solving. As a rule, never give out your email password.

Scan Your Unopened Messages

Take a moment to look through the list of messages. Note strange looking sender names or odd subject lines. Look for random-looking numbers, too much space, or anything out of the ordinary.

Don’t open any suspicious email – not even with the preview pane. Just delete it.

Opening malicious email (even with the preview pane) will often download images and scripts from the internet. That is a powerful vector of attack.

Avoid Clicking on Links

Outlook displays email formatted as HTML by default. This makes for beautiful newsletters, but can also hide the target URL (universal resource locator) of text.

For example, the email message may state “Click Here to enroll with the early bird savings!!!!” The words you see in email are “Click Here” but when you click it may take you to a malicious site (e.g., steal-my-identity-please.com).

Be wary of email messages about services you use. Malicious sites are often similar to URL’s you may know or expect: Amazzon, Wllamart, Yahooo, Chaase, etc. The malicious sites can compromise your computer when they load code in your browser that takes advantage of exploits in the browser, the computer, or plugins (java, flash, adobe reader, etc.).

One way to protect against this is simply to not click on any links you aren't expecting and are not from someone you know. You can hover your mouse cursor over links to see the target URL. You can right-click on the hyper-text and copy the link, then paste it into your browser if you are sure it's OK.

You can also view all of your email as plain-text.

Avoid Opening Unexpected Attachments

Do not open an attached file that you aren't expecting even if it is from someone that you know. Attachments must always be opened with care.

Opening a file on your computer allows malicious code to execute directly on your system with your level of privileges. A malicious person can have immediate access to your computer and all of your files.

For example, if you ask your students to email in Word attachments for their term paper, open those attachments from those students.

You can avoid attachments altogether by using an online service and asking students to send you the link (see above for best practices about links).

Using Google Drive

You can create documents on Google Drive and use the "Share" button to send a link to that document.

Using Dropbox

Students using dropbox (or any number of other file storage services) can upload their word document and send you a "share" link that you can then copy from your email and paste into your browser to download.

Sending links to documents instead of attaching them to messages helps keep your inbox faster as well.

The prominent security firm, RSA, was attacked and many costly secrets were lost when someone opened a malicious excel file.

Avoid Sending Personal or Private Information

Avoid sending user names and passwords in email messages, especially with the accompanying URL. One approach is to send the URL and username via email and then send the password from another system (not email). You could call the person, send them an instant message, or a text message.

Never send unencrypted documents that contain your personally identifiable information. This includes your SSN, address, etc.

Email sent off campus is stored on external servers and may be viewed by people you aren’t expecting to view them.

It is safe to consider that any email message you send is a public document and any attachments are for the world to see. This is not hyperbole. The campus can only control email within our own systems.

→ COVID-19 Information and Vaccine Requirements (https://www.riohondo.edu/student-health-services/coronavirus/)

Audio And Video File Storage

3C Media SOLUTIONS

(http://www.3cmediasolutions.org)

3C Media Solutions is a CCCCO grant-funded institution that offers multiple digital services to community college faculty and staff. With your free account, you can upload and share many types of files including documents, powerpoint, PDF, mp3’s, and all types of video. See the 3C website for a full list.

3C also offers “share links” a-la dropbox for your files. This makes putting large files into blackboard a matter of sending students the share link.

There are a number of How-To videos and FAQ’s on the 3C site. Click here to visit the 3C Media Solutions support site. (http://www.3cmediasolutions.org/support#How To)

You can read more about 3C on their About page (http://www.3cmediasolutions.org/user/register).

Register for an account and Get Started

(http://www.3cmediasolutions.org/user/register)

What would I use 3C Media Solutions for?

There are many uses of this service. Here are a few scenarios that may be applicable.

Sending large files in an LMS

The Rio Hondo LMS application has a file size limit. This is fine for most office documents but doesn’t suffice for large PDF’s, audio, or video files.

You can upload individual files or a folder of files to your 3C account and send a download link via blackboard.

You can upload audio or video and send students a link to view or listen to the media in their browser.

⊞ I don't want everything on Youtube

3C is offering an alternative to youtube. You upload your videos and send students the links. There is no fear of sending them advertisements or getting caught up “browsing” the follow-up recommendations.

⊞ I use CCC Confer and would like to share my recorded presentation.

3C has a relationship with CCC Confer and they are able to automatically post your presentation upon request.

→ COVID-19 Information and Vaccine Requirements (https://www.riohondo.edu/student-health-services/coronavirus/)

Setup Zoom Two-Factor Authentication

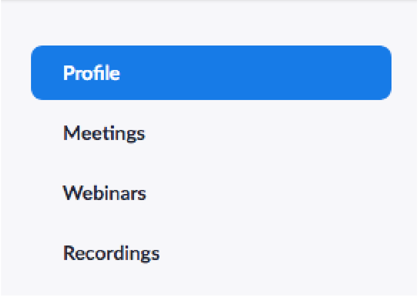
Using two factor authentication is a proven method to increase the security of your account and/or data. Zoom now has the option of using an authenticator application (something you have) to produce a Time-based One-Time Password (TOTP) that will be provided when you login to ConferZoom with your regular username and password (something you know).

Login to ConferZoom

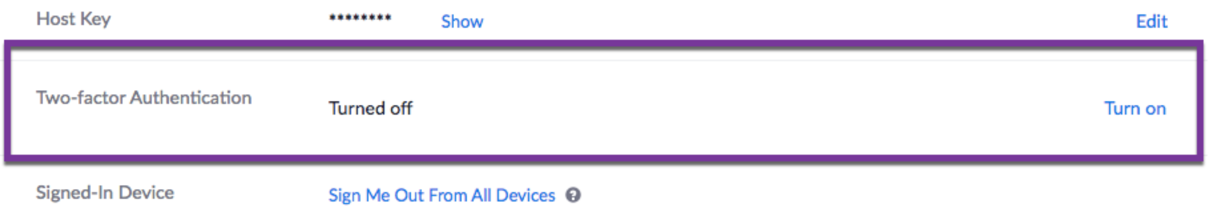
Navigate to ConferZoom (https://conferzoom.org) and select Sign in. Login with your existing credentials.

Turn on Two-factor Authentication

Navigate to your Profile in the left hand menu and scroll down towards the bottom.



Select “Turn on” next to Two-factor Authentication.



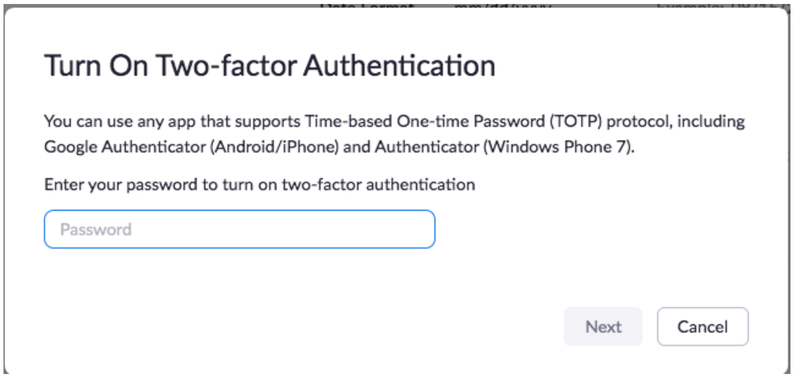
Setup Authentication App

Now that we have enabled two-factor for your account we will need to setup an application to manage your TOTP’s. I do not recommend using SMS as a login method. SMS has proven to be an unreliable security method.

You will need an authenticator application on your mobile phone. There are several to choose from including:

- Google Authenticator (https://w w w.google-authenticator.com/)
- Microsoft Authenticator (https://w w w.microsoft.com/en-us/account/authenticator)
- Authy (https://authy.com/)
- OTP Auth (https://cooperrs.de/otpauth.html) *ios only

When you have an authenticator app installed on your device, navigate back to your profile and select Set Up next to Authenticator App.

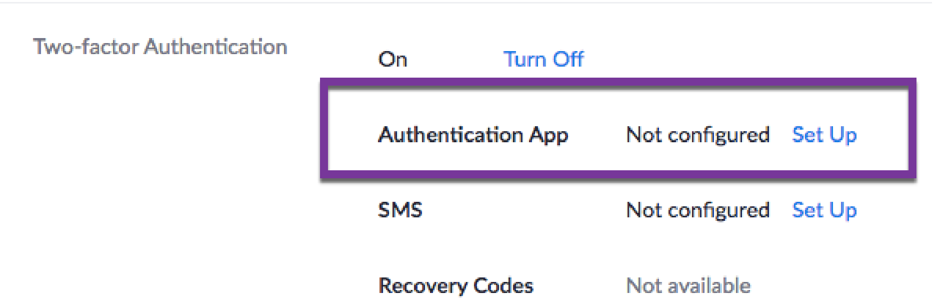


Turn On Two-factor Authentication

You can use any app that supports Time-based One-time Password (TOTP) protocol, including Google Authenticator (Android/iPhone) and Authenticator (Windows Phone 7).

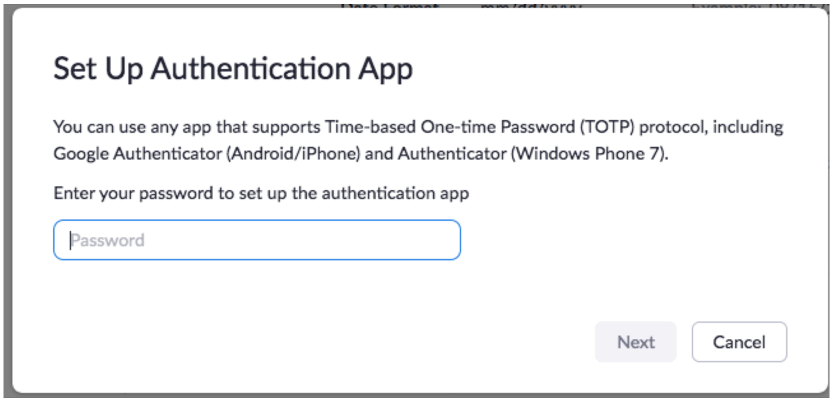
Enter your password to turn on two-factor authentication

Enter your ConferZoom password when prompted.



Two-factor Authentication	On	Turn Off	
	Authentication App	Not configured	Set Up
	SMS	Not configured	Set Up
	Recovery Codes	Not available	

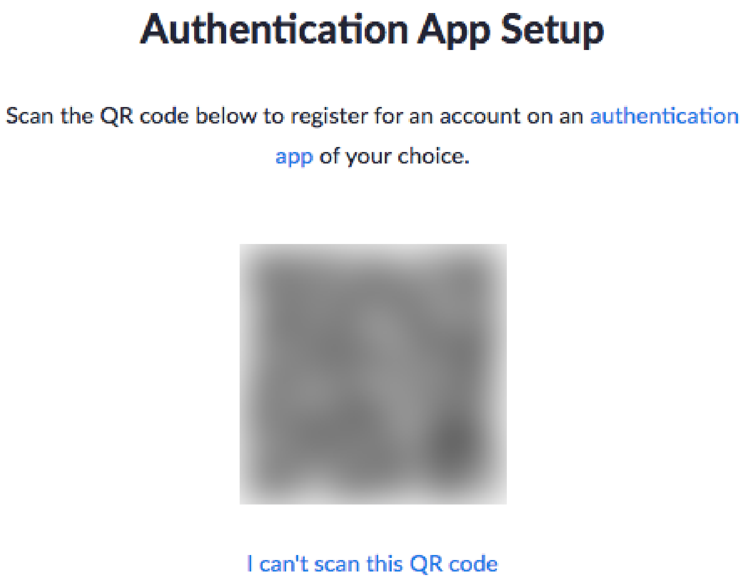
Open your authentication app and add a new site. Select “Scan barcode” and scan the QR code presented. Keep this code private. It is your SECRET key and should not be shared with anyone. I make a copy of the QR code and store that securely for future recovery in case I lose access to my phone.



Set Up Authentication App

You can use any app that supports Time-based One-time Password (TOTP) protocol, including Google Authenticator (Android/iPhone) and Authenticator (Windows Phone 7).

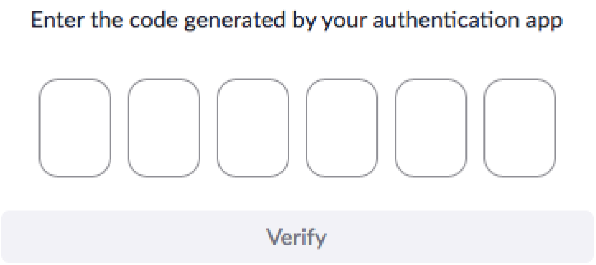
Enter your password to set up the authentication app



Authentication App Setup

Scan the QR code below to register for an account on an authentication app of your choice.

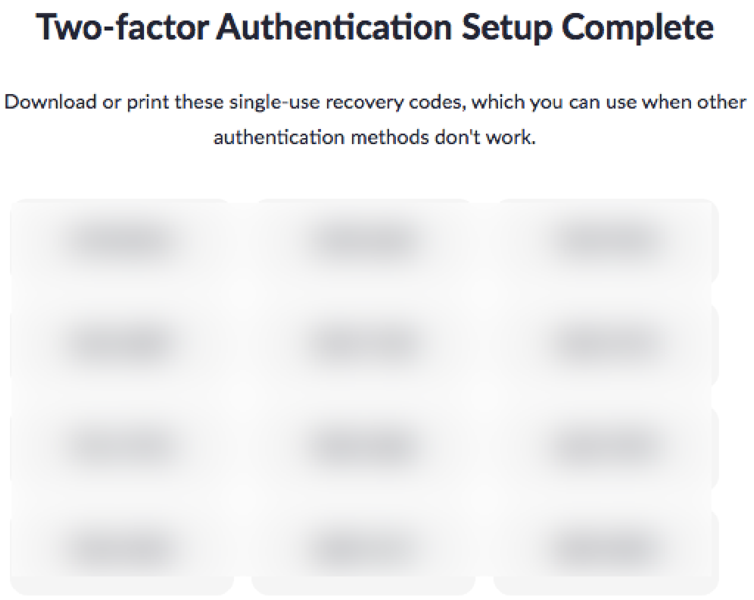
You will be prompted to enter the 6 digits from your authentication app in order to confirm that it is paired correctly.



Enter the code generated by your authentication app

You will then be given a set of 10 recovery codes that can be used in times when your authentication app is not convenient to access. These codes are available to be used 1 time each.

Keep them private in a safe place.

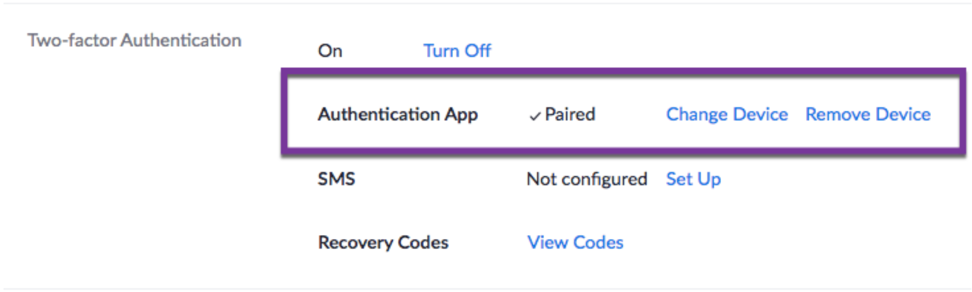


Two-factor Authentication Setup Complete

Download or print these single-use recovery codes, which you can use when other authentication methods don't work.

Congratulations, your ConferZoom account is now secured. You will be prompted to enter the code from your authentication app the next time you login to your ConferZoom account.

You can check the Two-factor Authentication status in your Profile.



Two-factor Authentication	On	Turn Off		
	Authentication App	✓ Paired	Change Device	Remove Device
	SMS	Not configured	Set Up	
	Recovery Codes	View Codes		