# K12 Onboarding Guide

Education Guide

zoom

Part I - Account Configuration (IT Team)

Add Zoom Deployment team, Configure Vanity URL, Associated Domains & Single Sign On.

1. Create a Zoom Deployment Team.

   a. The core admin team will oversee the Zoom deployment and manage the day to day operations. These users can help install important integrations such as SSO, Learning Management Systems, and other applications.

   b. Add the deployment team by clicking **Add users** via the User Management portal: **zoom.us/account/user**.
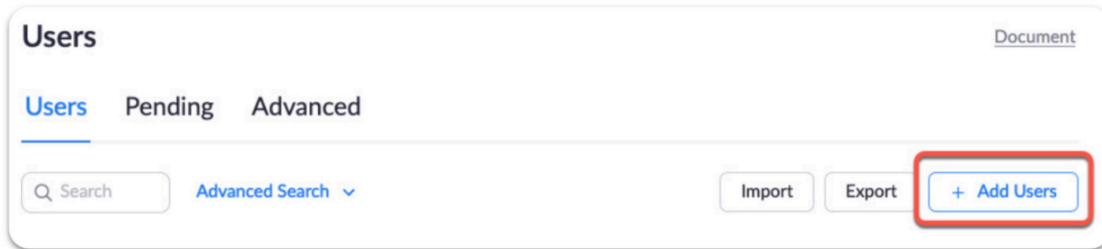

   c. Once the team accepts the email invitation that is sent by Zoom, the owner can promote these users to an **Admin** role by editing the user type on the right-hand side of the user. **Only** the Account Owner can add Zoom **Admins** by editing the user's role.
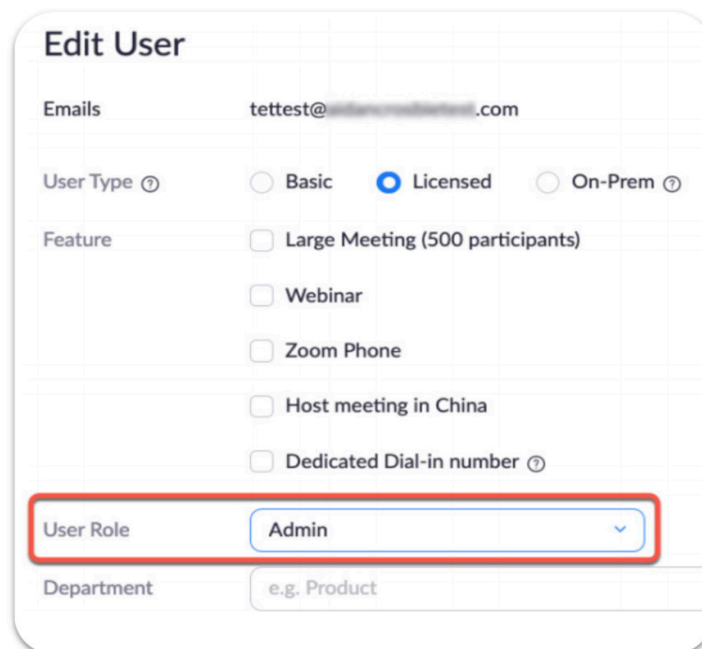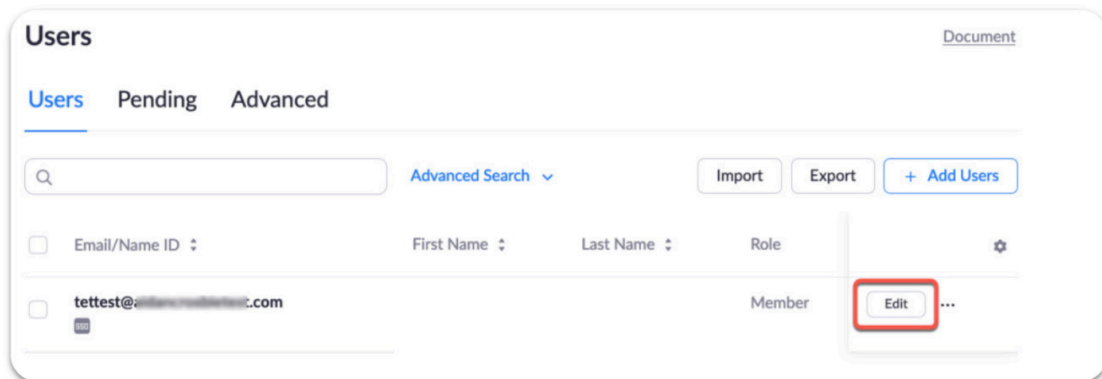
d. It is recommended to utilize **Role Management** to ensure that Admins who are installing specific integrations only have access to those options in the portal. You can create custom roles and assign it to the deployment team depending on their responsibilities. (*ie: SSO, Branding/Webmaster, LMS Admin, etc.*).

- Create custom roles here: **zoom.us/role#/**.
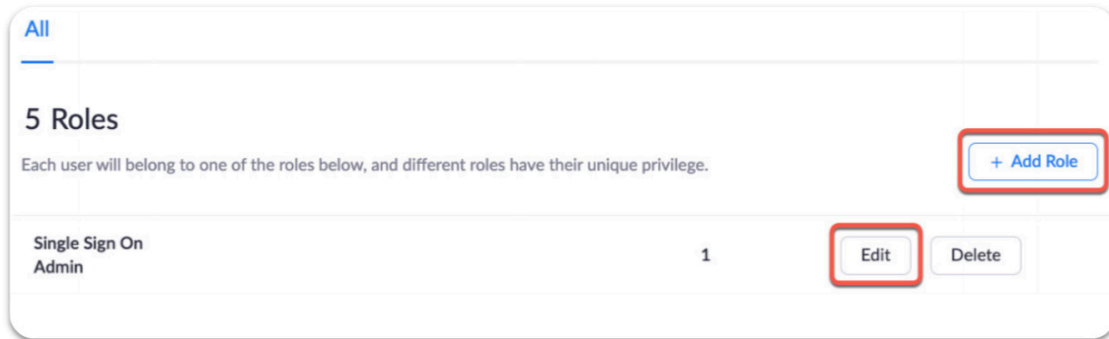
2. Apply for a **Vanity URL**.

    a. The Vanity URL serves as a landing page for users to sign into their Zoom accounts.

    b. This is required for Single-Sign-On and Branding.

    c. Important resources and school information can be added to this landing page for informational purposes via the Branding section of the account. Learn more **here**.

    d. Add a Vanity URL here: **zoom.us/account**.
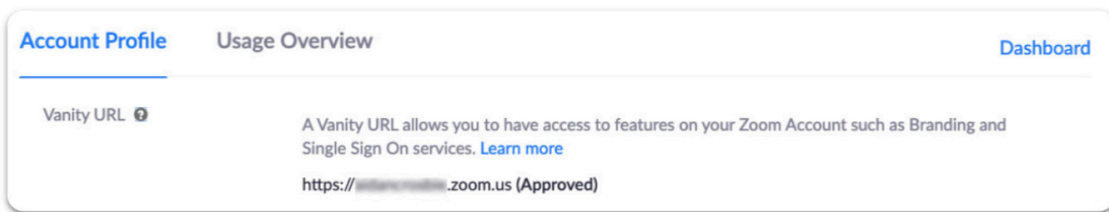
3. Apply for **Associated Domains**.

    a. Associated domains will provide the Account Owner/Admins full rights to the school domain. This helps consolidate new users by domain and/or restricts new users from creating a Zoom account with the school domain.

    b. Associated domains can be found here: **zoom.us/account**.

    c. If applicable, apply for both the faculty/staff and student domains.

    d. Once the Associated Domains are approved, **do not check** any of the 3 options found below **Manage users with the same domain**, **Allow users with the same domain to consolidate into this account**, and **Allow users with the same domain to sign up for Zoom** until **Part IV** is reviewed.
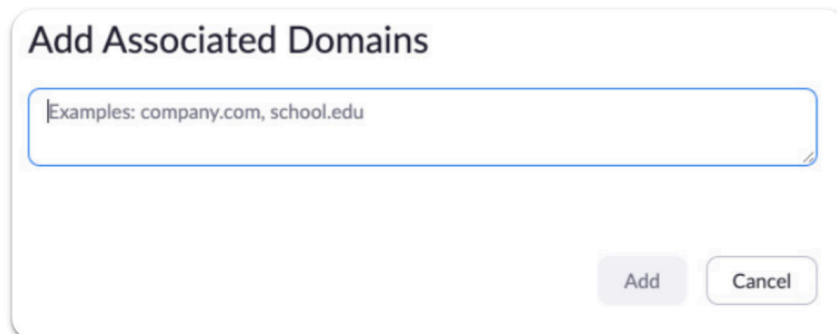
4. Configure SSO External Authentication.
   a. External authentication will require any participant/students joining a meeting to authenticate via the school's SSO Identity Provider. This process will not create accounts for students but will verify the student's name and email address for the meeting. This will provide an accurate attendance report and ensures that only authorized users have access to the meeting.
   b. Configure External Authentication via the following **documentation**.
   c. This setting is configured via the Account Settings **here**.
   d. Enable the option **Only authenticated users can join meetings** and click on **Add Configuration**.
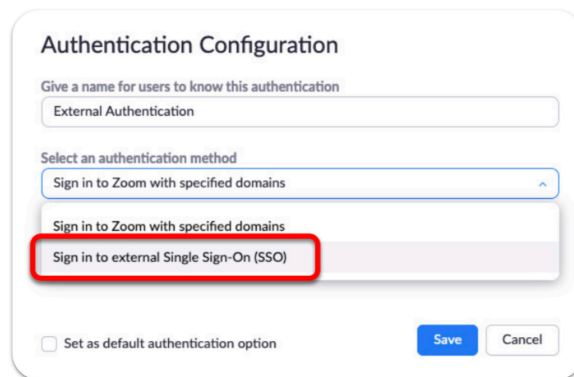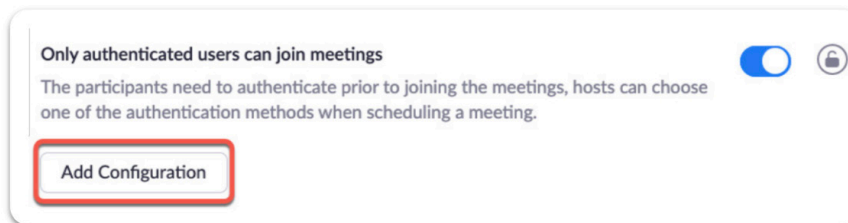
e. Once this is successfully configured, hosts/teachers scheduling meetings will need to select the authentication profile for this to work properly.
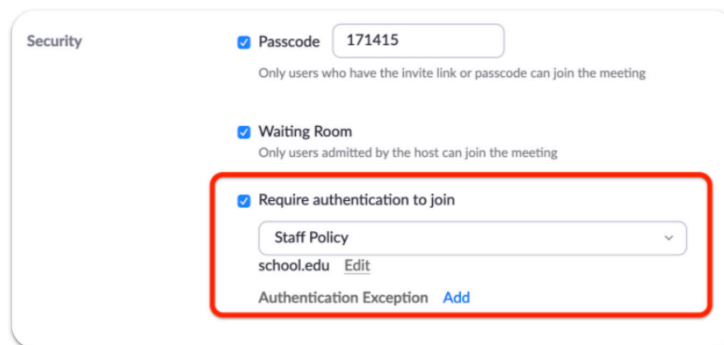
f. The Zoom administrator/owner can lock the authentication profile setting on the account or group level to force users to utilize the profile that has been configured.
   - ie: Instructor groups, K - 10 groups, etc.
   - If this setting is locked, the host cannot disable the authentication profile and will not be able to meet with participants who do not have the appropriate SSO credentials unless they add them as an **Authentication Exception**.
   - To add an **Authentication Exception** select **Add** and enter the guest/s name and email.
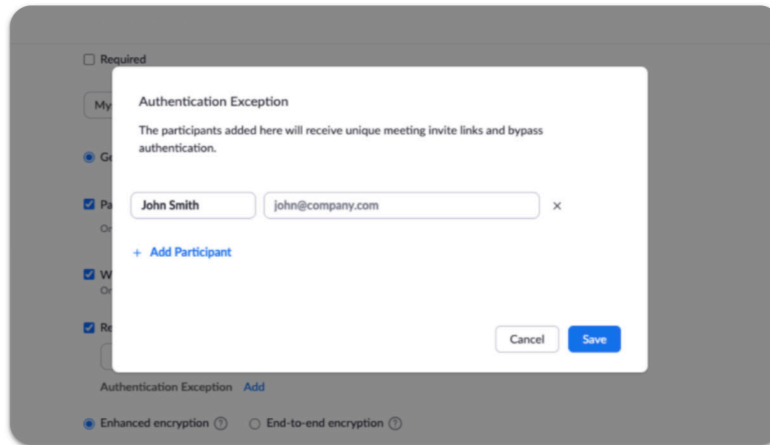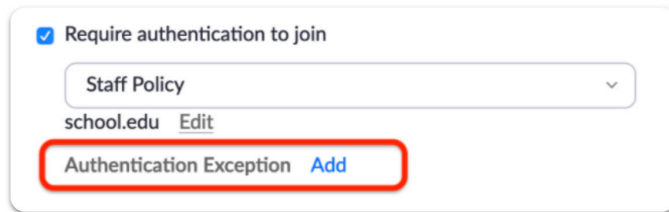
5. Configure Single-Sign-On (*If applicable, otherwise skip to Step 6*):

- **Clever Integration**
- **G Suite Integration**
- **Azure Integration**
- **Shibboleth Integration**
- **Okta Integration**
- **ADFS Integration**
- **Custom SSO Integration**
    a. Single-Sign-On is configured via the following page: **zoom.us/account/sso**.
    b. Recommended **SAML Basic Information Mapping**:
        1. Default user type
            i. Can provision all new users with a standard or basic license.
        2. Email address
            i. Zoom's primary attribute is to authenticate via an email address.
        3. First name
            i. Update each SSO Login to help catch name changes (*marriages, gender changes, etc.*).
        4. Last name
            i. Update each SSO Login to help catch name changes (*marriages, gender changes, etc.*).
        5. Display name
            i. Update each SSO Login to set preferred name/nickname via the IDP if applicable.
        6. Employee Unique ID
            i. Unique IDs can be mapped to users when authenticating via SSO. If a user changes their email address, Zoom will tie the new email address to the same account via the Employee Unique ID.
            ii. This is useful for name changes, marriages, and etc.
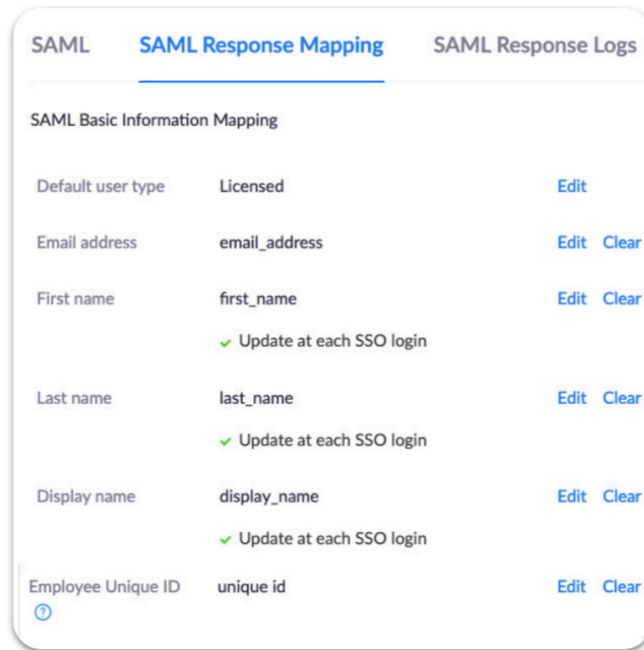
c. Recommended SAML Advanced Information Mapping:

1. User type - **None**:
   i. This is only applicable if students are utilizing the **same** IDP that is configured for staff and faculty. Students can be restricted from creating accounts by identifying a SAML attribute and value that they all have in common. When Zoom sees this value, that user/student will be denied access to the product.

2. User type - **Licensed/Basic**:
   i. Staff/Faculty can be provisioned with a license or basic license per a common/shared SAML attribute and value.
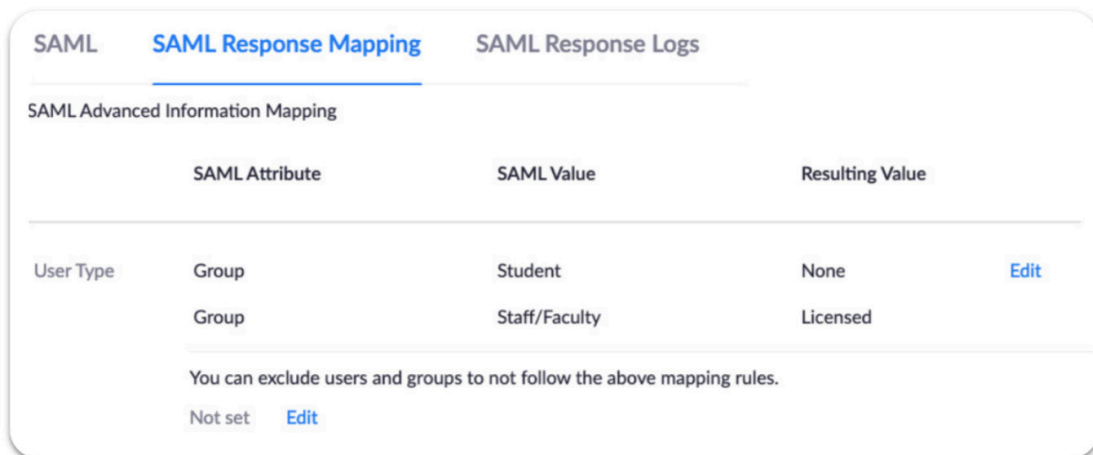
6. Manual Creating & Adding Users (*No Single Sign-On*).

a. Add staff and faculty via **User Management**.

b. Users can be imported in mass via a CSV file with our import feature found **here**.

c. Students should **not** be added unless they are 16 years of age or older.

Part II - Account Management

Configuring Account Settings, Security Settings and Creating Groups.

Configure Account Settings

1. Meeting Settings
   a. These settings will apply to all users in the account and will provide hosts with more meeting features. The following options are a few of Zoom's recommended settings to empower educators and administrators to have a better experience with Zoom:
      1. **Security**:
         i. Waiting Room (*Enable*)
         ii. Require passcode when scheduling meetings (*Enable*)
         iii. Require a passcode for instant meetings (*Enable*)
         iv. Require a passcode for Personal Meeting ID (*PMI*) (*Enable*)
         v. Embed passcode in invite link for one-click join (*Enabled*)
         vi. Only authenticated users can join meetings (*Configured in Part I of this documentation*) (*Enable*)
      2. **In Meeting** (*Basic*):
         i. Chat (*Enable*)
         ii. File transfer (*Enable*)
         iii. Co-host (*Enable*)
         iv. Polling (*Enable*)
         v. In-Meeting (*Basic*) (*Enabled*)
         vi. Screen sharing (*Enable*)
            a. Who can share? Host Only (*Enable*)
            b. This will limit any unwanted screen sharing from participants and let's the host control who can share within the meeting.
         vii. Annotation (*Enable*)
         viii. Whiteboard (*Enabled*)
         ix. Allow participants to rename themselves (*Disable*)
      3. **In Meeting** (*Advanced*):
         i. Breakout room (*Enable*)
            a. Allow hosts to assign participants to breakout rooms when scheduling.
         ii. Closed captioning (*Enable*)
            a. Enable live transcription service to show transcript on the side panel in-meeting.
         iii. Virtual background(*Enable*)
            a. Allow use of videos for virtual backgrounds. (*Enable*)
            b. Allow users to upload custom backgrounds. (*Disable*)
            c. Admins can **Manage virtual backgrounds** by uploading their own custom virtual backgrounds pertinent to their school/district so there is uniform branding for hosts.
            d. Immersive View. (*Enable*)

2. Record Settings
   a. Record active speaker with shared screen (*Enable*)
   b. Record an audio only file (*Enable*)
   c. Save chat messages from the meeting/webinar (*Enable*)
      1. Retains audit logs to hold participants accountable.
      2. Saves any important information shared in the meeting.
   d. Audio transcript (*Enable*)
      1. This will transcribe the cloud recording audio from speech to a text transcript. This serves any accessibility requirements, but it is not ADA compliant.
   e. Automatic recording (*Disable*)
   f. Require passcode to access shared cloud recordings (*Enable*)
   g. Auto delete cloud recordings after _ days (*Enable*)
      1. This will automatically delete cloud recordings after a set amount of days. This will help clean up recordings from being stored too long and will free up storage space.
      2. Most common retention policy is 365 days, but every organization may vary depending on their needs.
   h. Recording disclaimer (*Enable*)
      1. Several states and locations have two-party consent laws that prohibit people from being recorded without their knowledge or consent.
      2. This helps with any privacy concerns from participants.
3. For additional support regarding Account and Recording settings, contact your Zoom CSM or the Zoom support team via this **webform**.

Create Groups for Faculty and Staff

1. Review **Group Management** documentation to create groups for Faculty and Staff.
2. Groups provide access, or restrict certain features for a subset of users on the account. ie: Disable cloud recording on groups, enforce cloud recording retention policies, etc.
3. Consult with your Zoom CSM or reach out to the Zoom support team via this webform for common use-cases regarding group settings.

Review **Security Settings**

1. Disable Google/Facebook/Apple ID logins (*Optional*).
   a. This will remove the ability for users to authenticate with methods that are not approved by the school district/org.
   b. If Single-Sign-On is not integrated, Google authentication and work email are alternative solutions.
2. Only account admin can change users' name, profile picture, sign-in email, and host key.
   a. Name (*Enable*)
      1. This will ensure the correct name is being used for Zoom hosts.
   b. Profile picture (*Enable*)
      1. This will disable hosts from uploading inappropriate pictures or utilizing material that is not approved.
   c. Sign-in email (*Enable*)
   d. Host key (*Enable*)

Meeting   **Recording**   **Telephone**

Security

Waiting Room 🔵 🔒
When participants join a meeting, place them in a waiting room and require the host to admit them individually. Enabling the waiting room automatically disables the setting for allowing participants to join before host.

Waiting Room Options
The options you select here apply to meetings hosted by users who turned 'Waiting Room' on

✓ Users not in your account will go in the waiting room

✓ Host and co-hosts only can admit participants from the waiting room

Edit Options   Customize Waiting Room

Require a passcode when scheduling new meetings 🔵 🔒
A passcode will be generated when scheduling a meeting and participants require the passcode to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

☐ Require a passcode for meetings which have already been scheduled
ⓘ

Require a passcode for instant meetings 🔵 🔒
A random passcode will be generated when starting an instant meeting

Require a passcode for Personal Meeting ID (PMI) 🔵 🔒

◯ Only meetings with Join Before Host enabled
◉ All meetings using PMI

Only authenticated users can join meetings 🔵 🔒
The participants need to authenticate prior to joining the meetings, hosts can choose one of the authentication methods when scheduling a meeting.

Meeting Authentication Options:
External Authentication **Edit**
(Default) ⬇ SP metadata XML

[Add Configuration]

In Meeting (Basic)

Chat 🔵 🔒
Allow meeting participants to send a message visible to all participants

File transfer 🔵 🔒
Hosts and participants can send files through the in-meeting chat. ⓥ

☐ Only allow specified file types ⓥ

Co-host 🔵 🔒
Allow the host to add co-hosts. Co-hosts have the same in-meeting controls as the host.

Polling 🔵 🔒
Add 'Polls' to the meeting controls. This allows the host to survey the attendees. ⓥ

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 ⓘ

Annotation 🔵 🔒
Allow host and participants to use annotation tools to add information to shared screens ⓥ

☑ Allow saving of shared screens with annotations ⓥ

☑ Only the user who is sharing can annotate ⓥ

Whiteboard 🔵 🔒
Allow host and participants to share whiteboard during a meeting ⓥ

☑ Allow saving of whiteboard content ⓥ
☐ Auto save whiteboard content when sharing is stopped

Allow participants to rename themselves 🔵 🔒
Allow meeting participants and webinar panelists to rename themselves. ⓥ

In Meeting (Advanced)

Breakout room 🔵 🔒
Allow host to split meeting participants into separate, smaller rooms

☑ Allow host to assign participants to breakout rooms when scheduling

Closed captioning 🔵 🔒
Allow host to type closed captions or assign a participant/third party device to add closed captions

Virtual background 🔵 🔒
Customize your background to keep your environment private from others in a meeting. This can be used with or without a green screen.

☑ Allow use of videos for virtual backgrounds ⓥ

☐ Allow users to upload custom backgrounds ⓥ

Meeting   **Recording**   **Telephone**

Local recording 🔵 🔒
Allow hosts and participants to record the meeting to a local file

☑ Hosts can give participants the permission to record locally

Cloud recording 🔵 🔒
Allow hosts to record and save the meeting / webinar in the cloud

☑ Record active speaker with shared screen
☐ Record gallery view with shared screen ⓘ
☐ Record active speaker, gallery view and shared screen separately
☑ Record an audio only file
☑ Save chat messages from the meeting / webinar

Advanced cloud recording settings

☑ Add a timestamp to the recording ⓘ
☑ Display participants' names in the recording
☑ Record thumbnails when sharing ⓘ
☐ Optimize the recording for 3rd party video editor

☑ Audio transcript ⓘ
☑ Save panelist chat to the recording ⓘ

Automatic recording ⚪ 🔒
Record meetings automatically as they start

Only authenticated users can view cloud recordings 🔵 🔒
The viewers need to authenticate prior to viewing the cloud recordings, hosts can choose one of the authentication methods when sharing a cloud recording.

Auto delete cloud recordings after days 🔵 🔒
Allow Zoom to automatically delete recordings after a specified number of days

Specify a time range (days): [365]

Recording disclaimer 🔵 🔒
Show a customizable disclaimer to participants before a recording starts ⓥ

☑ Ask participants for consent when a recording starts
Customize
☐ Ask host to confirm before starting a recording

Security

| Security |

Only account admin can change users' name, profile picture, sign-in email, and host key 🔵

☑ Name (first name and last name)
☑ Profile picture
☑ Sign-In email
☑ Host key

Sign-in Methods

Allow users to sign in with work email ⚪
Enable to give users permission to sign in with entering work email address

Allow users to sign in with Single Sign-On (SSO) 🔵
Enabling this requires you to configure your account's SSO settings. This will allow users to sign in with SSO through your company's vanity URL.

☐ Require users to sign in with SSO if their e-mail address belongs to one of the domains below

Allow users to sign in with Google ⚪
Enable to give users permission to sign in with Google

Allow users to sign in with Facebook ⚪
Enable to give users permission to sign in with Facebook

Allow users to sign in with Apple ID ⚪
Enable to give users permission to sign in with Apple ID

Mass Installations by IT (*Recommended Settings for Student Machines***)**

Students under 16 **cannot create Zoom accounts and the following switches will disable students from logging in.**

These options should be enforced for the following operating systems:

1. Chrome OS
    a. DisableGoogleLogin
    b. DisableFacebookLogin
    c. DisableLoginWithSSO
    d. Turn **OFF** Google play if Android apps are not needed (*this may cause very high CPU usage at any time to download/ check applications*)
    e. Turn **OFF** Bluetooth if it is not needed (*high CPU usage may be experienced via Bluetooth backend services*)
2. Windows OS
    a. Disable Google login option: nogoogle, 1
    b. Disable Facebook login option: nofacebook, 1
    c. Disable Email login option: DisableLoginWithEmail, 1
    d. Disables logging in via SSO: nosso, 1
3. Mac
    a. Disable Google login option: nogoogle, false
    b. Disable Facebook login option: nofacebook, false
    c. Disable Email login option: disableloginwithemail, false
    d. Disable SSO login option: nosso, false

Part III - Associated Domains & Meeting Scheduling

Configure Associated Domains, Learning Management System Integration & Calendar Solution.

Configuring Associated Domains

1. **Ensure that all staff & faculty are added to the account via SSO or User Management before continuing**.
    a. If there are any existing users with separate paid accounts, it is recommended to have them join the deployment before configuring associated domains to ensure they receive any applicable refunds and that their consolidation can be completed successfully.
2. To configure Associated Domains, visit the following page: **zoom.us/account**.
3. If faculty/staff share the same domain with students:
    a. Enable the option **Manage users with the same domain** to require existing students to change their current email address with Zoom.
        1. This will require faculty & staff to change their email address if they have not been added to the deployment.
    b. Do **NOT** enable **allow users with the same domain to consolidate into this account** as this will consolidate all existing students.
4. If students are on a different email domain:
    a. Staff & faculty can be consolidated into the Zoom deployment when they log into their own accounts via Zoom. This will help capture any existing users who have not yet been added to the deployment and they will not need to change their email address.

a. To do this, enable the option **allow users with the same domain to consolidate into this account** next to the staff/ faculty domain.

    1. If enabled, all users in that domain will be prompted to join the Zoom deployment upon their next login.

    2. This will not pull students into the account as long as students have a different email domain.
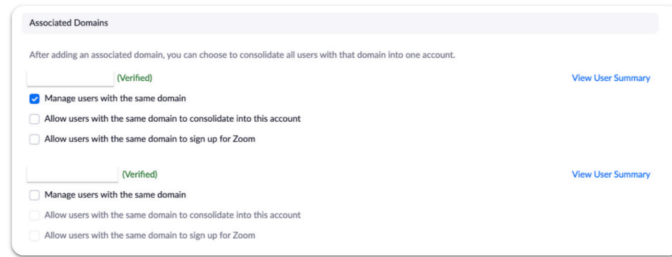
Learning Management System Integration (*Optional*)

1. Zoom can integrate with most LMS systems via the LTI Pro application found via the Zoom Marketplace **here**.

2. The app must be pre-approved in order to install it.

3. It is recommended that a generic service/helpdesk user who has Admin rights install LTI Pro as the integration will be tied to the person that installs it.

    a. ie: helpdesk@school.edu

    b. If the user who installs the integration leaves the Zoom deployment or is downgraded to a member, it will cause the integration to stop working correctly.

    c. If a named user has already installed LTI Pro, the installer can be changed. Contact the CSM or technical support team via this **webform** for further instructions on how to do this.

    d. The integration requires the instructor's email address in the LMS to match their email address in Zoom. If they do not match, this can cause issues with the integration such as duplicate accounts, error messages, etc.

    e. Follow the **documentation** to install the LTI Pro Integration.

Calendar Integration (*Optional*)

For Users that Want to Schedule Zoom Meetings Directly from Their Calendar

1. **O365 Add-in**
2. **OL Plug-in** (*Deprecated on Mac OSX*) .
3. **G Suite Add-in**
4. **Chrome Extension**

Offboarding/Downgrading Users

1. Once you run out of licenses, we will only provide users with a basic license. To help minimize the number of licenses being utilized, it is recommended that you first run an Inactive Host report **here**.

2. From that point, please use that list to determine which users are not actively logging in.

3. Once you have that list, you can do a bulk update via your User Management to downgrade those users in one single shot.

4. Please learn more about bulk updating users via the following **documentation**.

5. You can also do this via SSO by utilizing SAML Mapping. Please learn more about that option **here**.

6. Lastly, you can also utilize our API calls to programmatically downgrade or delete users:

    a. Learn more: **API user update**, **API user delete**.