



Advanced Security
Configurations & Tips

The ultimate guide to secure Zoom



hello@cytex.io

cytex.io



Zoom security best practices

This guide outlines the best practices and security configurations for securing Zoom, ensuring your organization remains protected from breaches, unauthorized access, and data leaks. These steps are tailored for administrators managing Zoom at an organizational level.



1

Zoom role management

Each Zoom account user has a system role: owner, administrator, or member. Account owners and admins can view other users' roles through user management. Role-based access controls (RBAC) in Zoom minimize the risk of accidental or malicious changes to the environment.

You can assign group admins for groups under your account without altering account roles. Group admins manage members and settings, and can check if their group is the primary group for users. They do not need to be account admins or have role permissions to edit user groups.

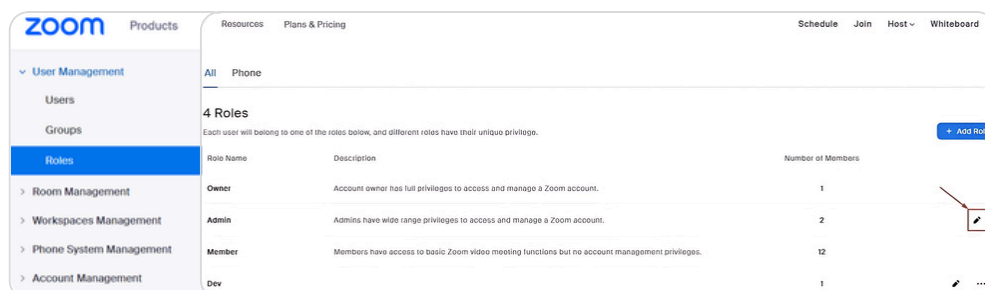
Prerequisites for role management:

- An Enterprise, Business, Education or Pro plan
- For setting the initial role, you must be the account owner
- Account owner or admin with the privileges or user with role management permissions

Note: Since only the owner can initially add a user role, Zoom recommends that the owner adds a role that allows at least one other person to manage user roles.

To add initial user '**role management**' permissions:

- Sign in to the Zoom web portal as the account owner > <https://zoom.us/signin>
- Navigate to User Management > Roles, then click Add Role.
- Enter a name and description, then click Add.
- Click the checkbox for Role Management.
 - Note: This enables users in this role to create and manage user roles so that the Owner is not the only person who can perform this task. You can also click additional checkboxes if you want users in this role to see or edit additional pages.
- Scroll down > click Save Changes > click Back to Roles to return the main Role Management page.
- Click Edit to the right of the role > click the Role Members tab > click Add Members.
- Enter the email address of the user (if adding multiple, add a comma between email addresses, to separate them) > click Add.

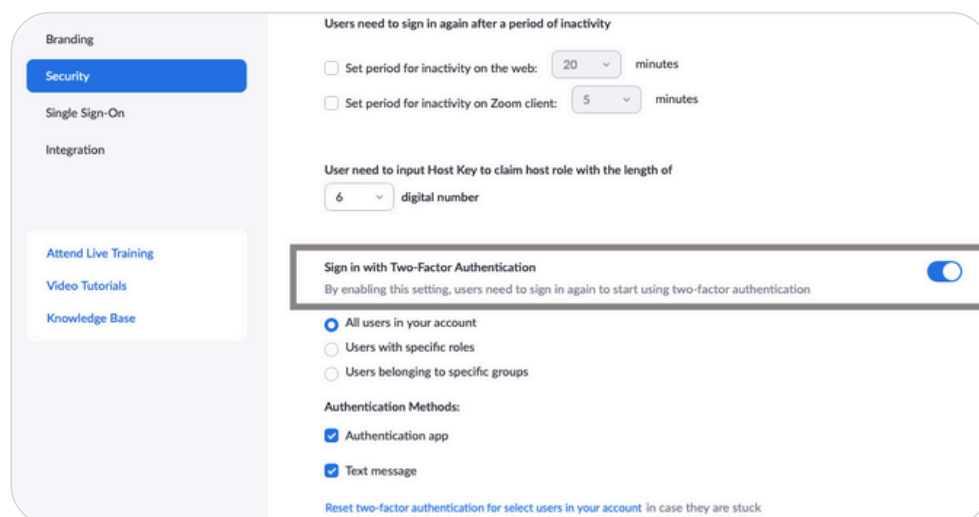


2

Enforce two-factor authentication (2FA)

2FA adds an additional layer of security to prevent unauthorized access to user accounts. Users will need access to their phone to sign in to the Zoom web portal, desktop app, mobile app, or Zoom Room.

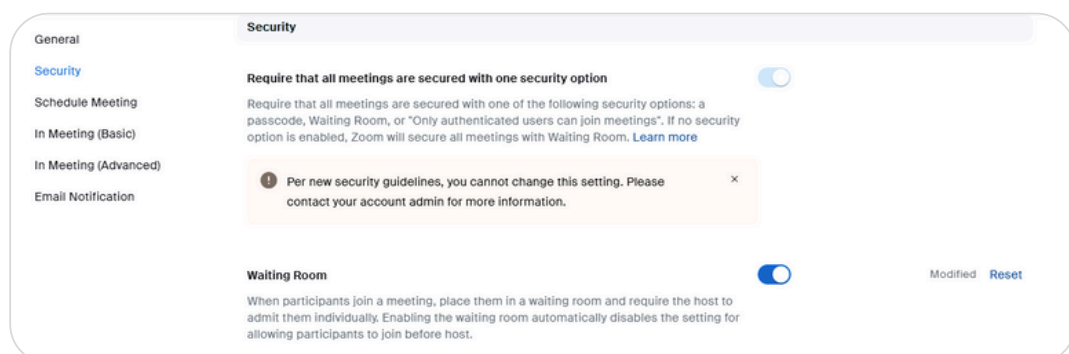
- Sign in to the Zoom Admin Portal.
- Navigate to Advanced > Security.
- Under Security > click Sign in with Two-Factor Authentication toggle to enable or disable it.
- Select one of these options to specify users to enable 2FA for:
 - All users in your account: Enable 2FA for all users in the account.
 - Users with specific roles: Enable 2FA for roles with the specified roles.
 - Click the pencil icon > select roles > click OK.
 - Users belonging to specific groups: Enable 2FA for users that are in the specified groups.
 - Click the pencil icon > select roles > click OK.
- Under Authentication Methods, enable one of the following authentication methods.
 - Authentication app: Use a third-party authentication app to generate login codes. (Example: Google Authenticator, Microsoft Authenticator, and FreeOTP).
 - Text message: Use Text message or SMS to send login codes.
- Click Save to apply your changes.



3

Lock down meeting settings

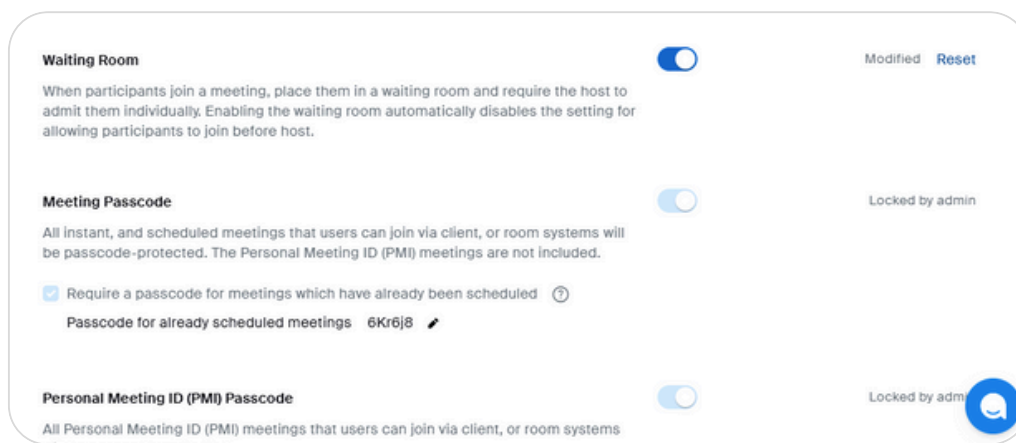
Prevent unauthorized access, Zoombombing, and meeting disruptions.



3

Lock down meeting settings

- Navigate to Settings > Meetings > Security in the Admin Portal.
- Enable the following options:
 - Waiting Room: Ensure all participants are vetted before entering.
 - Passcode Protection: Set unique passcodes for all meetings.
 - Only Authenticated Users Can Join: Restrict access to users signed in with a verified Zoom account.
 - Disable Join Before Host: Prevent participants from joining without the host.
- For recurring meetings, use a unique meeting ID instead of the personal meeting ID (PMI).

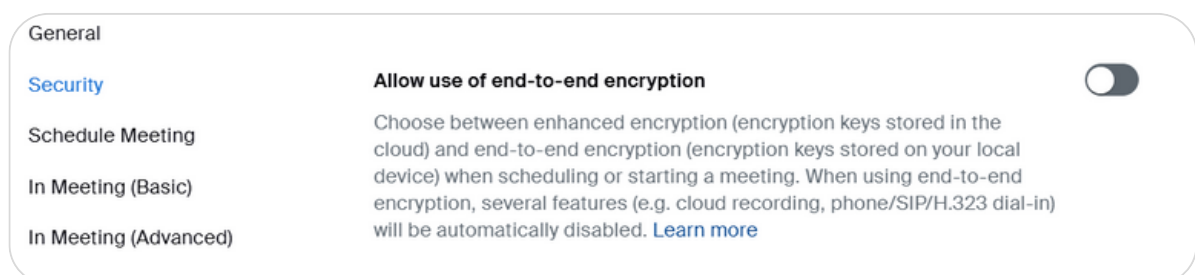


4

Enable data encryption for meetings

Encryption ensures sensitive communications remain private and protected from interception.

- Navigate to Settings > Security > Encryption.
- Enable End-to-End Encryption (E2EE) for meetings.
- Inform participants that certain features (e.g., polling, cloud recording) may not work with E2EE enabled.



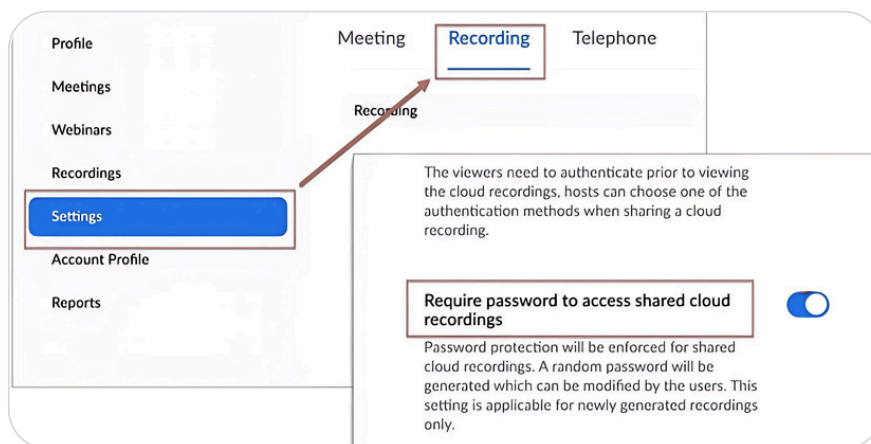
5

Implement advanced recording controls

Protect sensitive meeting recordings from unauthorized access or data leaks.

5 Implement advanced recording controls

- Navigate to Settings > Recordings.
- Enable the following options:
 - Require Passcode for Recording Access: Ensure only authorized users can view recordings.
 - Disable Downloading of Recordings: Restrict users from downloading shared recordings.
 - Cloud Recording Expiration: Set an expiration date for stored recordings to limit long-term exposure.
- Regularly review and delete old recordings that are no longer needed.

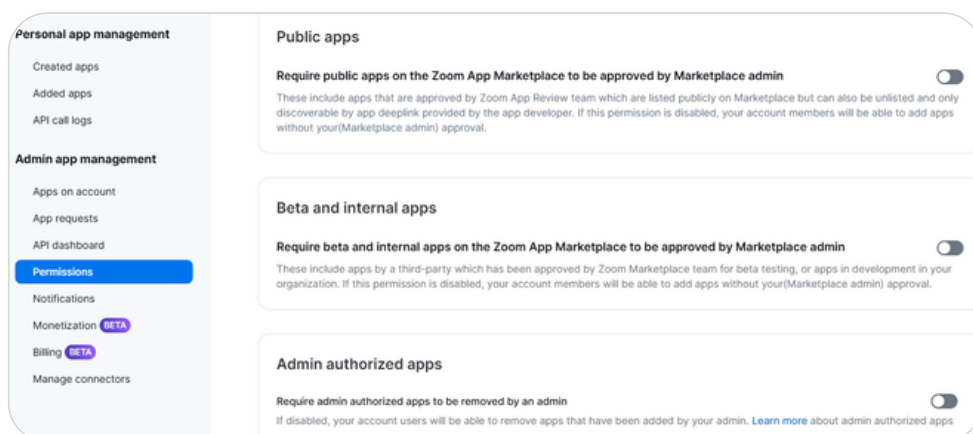


6 Monitor and restrict third-party integrations

Unvetted third-party apps can introduce vulnerabilities to your Zoom environment.

- Navigate to Zoom Marketplace Management.
<https://marketplace.zoom.us/user/permissions>
- Under Permissions enable 'Require public apps on the Zoom App Marketplace to be approved by Marketplace admin'
- Enable 'Require beta and internal apps on the Zoom App Marketplace to be approved by Marketplace admin'
- Enable 'Show only approved apps', so that the users only see approved apps in the Apps tab in the Zoom client.

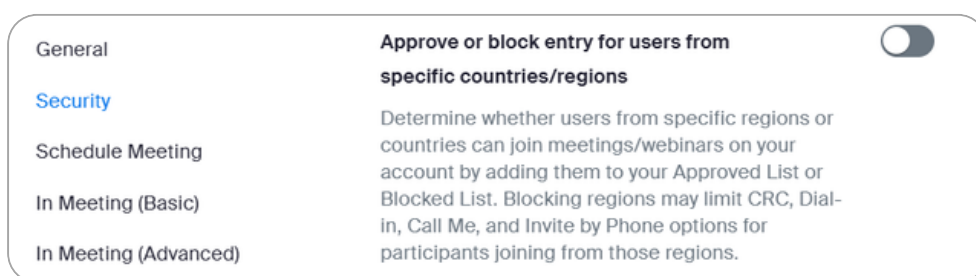
Additionally, perform a regular review and audit of installed apps for security compliance.



7 Set Up Conditional Access Policies

Conditional access policies ensure only trusted devices and users can access your Zoom environment.

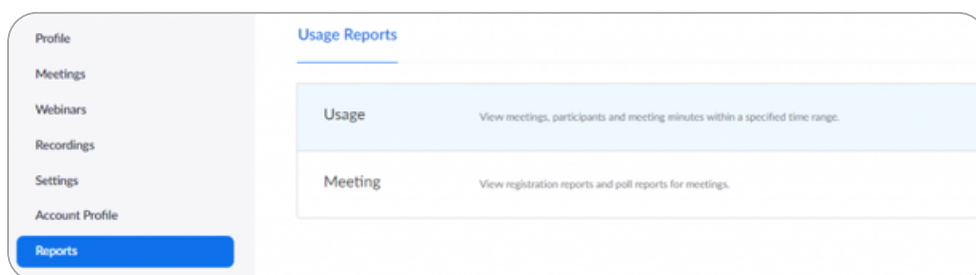
- Navigate to Settings > Security > Access Control.
- Define policies such as:
 - Restricting access based on geographic locations or IP ranges.
 - Blocking access from untrusted devices or browsers.
- Enforce device compliance checks for mobile and desktop clients.



8 Implement Real-Time Monitoring and Alerts

Early detection of suspicious activity can prevent security incidents.

- Navigate to Reports > Activity Logs in the Admin Portal.
- Enable alerts for unusual login attempts, multiple failed logins, and account lockouts.
- Integrate Zoom logs with your Security Information and Event Management (SIEM) system for centralized monitoring.



9 Configure Zoom Customer Managed Key (CMK) Hybrid

CMK Hybrid allows organizations to manage their own encryption keys for Zoom's cloud services. This ensures sensitive data is protected, even from Zoom itself, by giving customers complete control over their encryption keys.

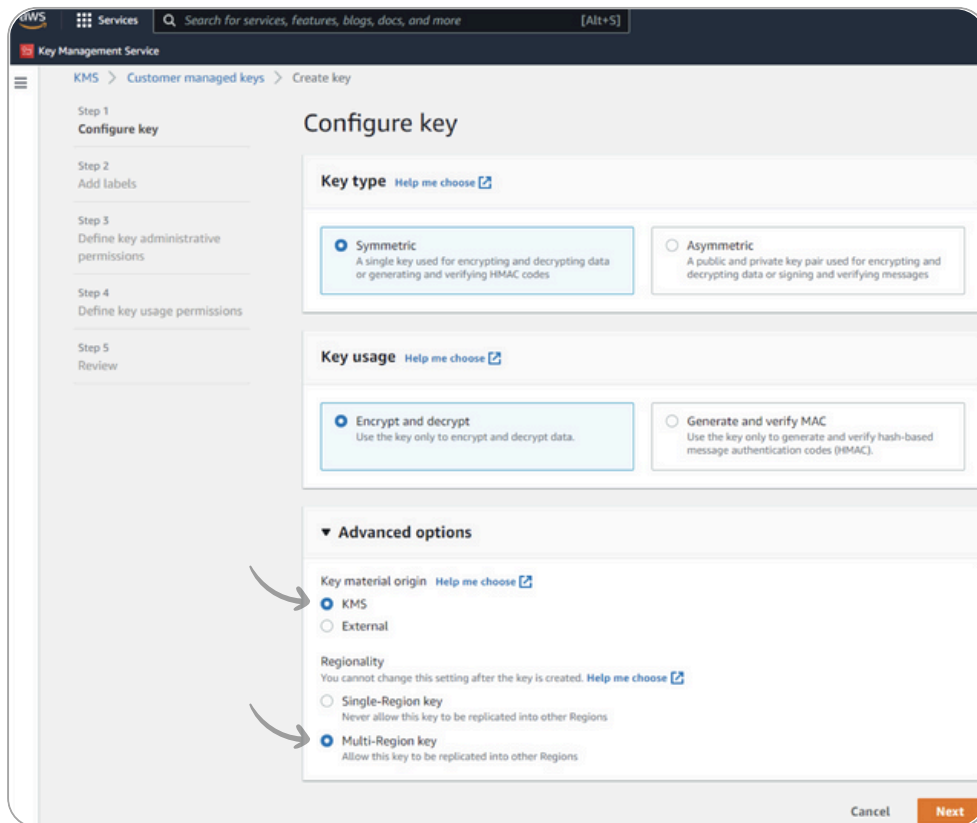
Pre-Requisites:

- Ensure your organization has an active subscription to Zoom's CMK Hybrid service.
- Set up a Key Management Service (KMS) such as AWS KMS, Oracle OCI Vault, or Azure Key Vault.
- Confirm that your KMS is compatible with Zoom's CMK Hybrid architecture.

9

Configure Zoom Customer Managed Key (CMK) Hybrid

AWS KMS (and OCI Vault) already replicate each key to multiple availability zones, we encourage AWS customers to **use AWS' multi-region key (MRK) option** to replicate the key across multiple regions in some of the data centers in which Zoom operates for extra fault tolerance. Next, the organization needs to add the Zoom key broker to the key policy to give the Zoom key broker access to the keys. While most organizations will rely on AWS's Automated key management for key rotation, organizations that need more control over key rotation and revocation can also use Manual key management or External hardware security module. OCI Vault provides similar options.



Customer Managed Keys are KMS keys in your AWS account that you create, own, and manage. Before you get started with Customer Managed Key service in the Zoom cloud, follow the steps below:

- Create a KMS key with the following configuration:
 - Key type: Symmetric
 - Key usage: Encrypt and decrypt
 - Key material origin: KMS
 - Regionality: Multi-Region key
- Replicate the KMS key to other AWS regions you wish to host the key in, for redundancy.
- Configure your key policy and IAM (Identity access management) policy appropriately in all of your AWS regions to specify access to your keys by copying and editing the template below into your AWS console.

9 **Configure Zoom Customer Managed Key (CMK) Hybrid Configuring your key's policy:**

In order to configure your key's policy, go to the Customer Managed Key page in the Encryption Keys section of the AWS KMS management console. The policy needs to include the following:

- Allow-list the Zoom Key Broker AWS account number
- Specify which AWS KMS methods are permitted.

There are two ways to add these:

- The recommended way is to select the Add other AWS accounts found in the Key policy tab.
 - Include the Account number# 409910850980 as the Zoom Key broker account to allow access to your KMS key. This creates the JSON policy with the account and IAM role (arn:aws:iam::409910850980:root) as well as all the required valid key operations.
 - You could choose to grant key access to the Zoom key broker either at the root or role level. At the root level it would be arn:aws:iam::409910850980:root and at the role level arn:aws:iam::409910850980:role/keybroker-role
- Another way would be to Switch to policy view in order to see and edit the JSON representation.

9 **Configure Zoom Customer Managed Key (CMK) Hybrid Enroll your keys with Zoom:**

- In Zoom web portal, navigate to > Menu > Advanced > Security.
- Under Customer Managed Key > click Add Key > Choose Amazon AWS.
- Enter the key information and click Create. Enter the ARN of the KMS key.
 - A message will appear displaying the ARNs that will be used for different regions. Click Continue when you are done reviewing.
- Click + Add Services and determine which items will be encrypted. Place a check in the box next to any of the data types / services you want encrypted with your key, then click Add.
- Click +Add recipient and add the users who will be notified by email if there is a key status change.

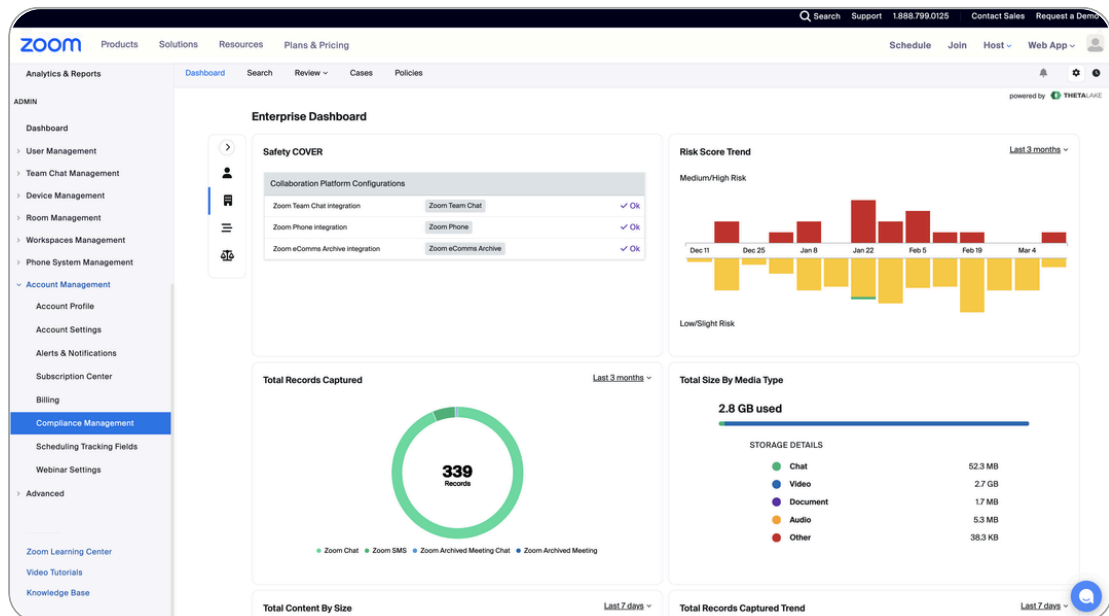
9 **Configure Zoom Customer Managed Key (CMK) Hybrid Assign Customer Managed Key (CMK) licenses to users:**

- In Zoom web portal, navigate to > User Management > Users.
- Check the box to the left of the user's name then click the License drop down.
- Click Zoom Customer Managed Key, then check the box next to the Feature.
- Click Save.

10

Leverage Zoom "compliance manager powered by Theta Lake"

Zoom Compliance Manager Plus helps organizations stay compliant with industry standards and regulations (e.g., GDPR, HIPAA, SOC 2). It provides a centralized dashboard for monitoring compliance requirements and automating audit processes. It is compatible with all Zoom products supported by CMK.

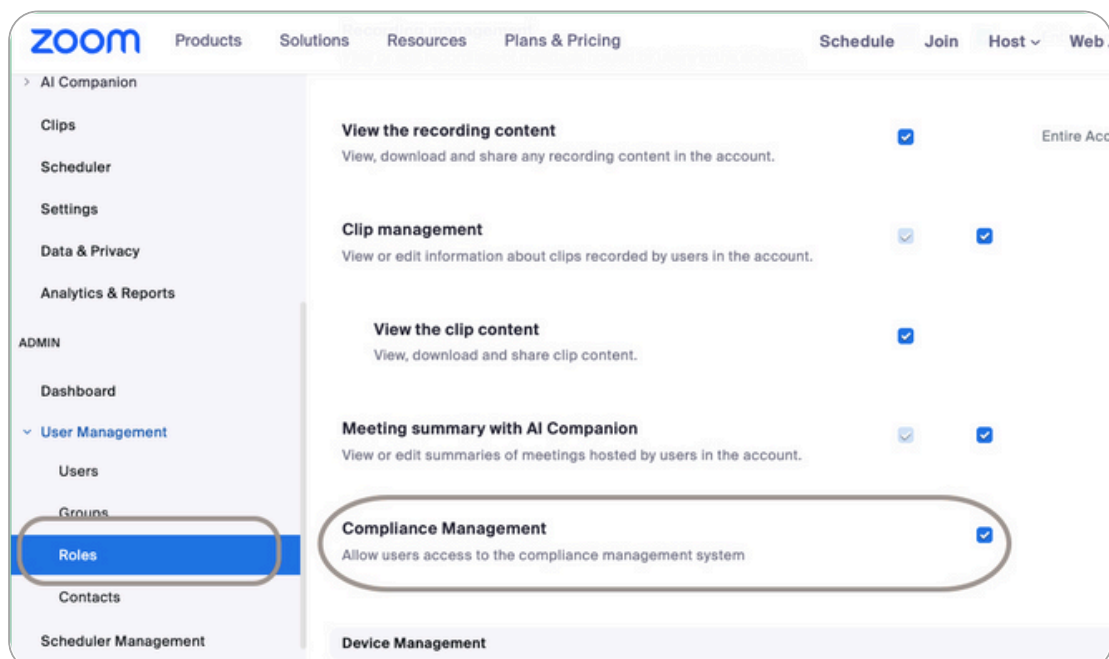


Zoom Compliance Manager connects Zoom's existing archiving functionalities directly with Theta Lake as the archiving service. This product builds upon the archiving solutions Zoom already has, providing a direct connection to Theta Lake's archiving services and consolidating billing for these services.

- In the Zoom admin portal > Account Management > select Compliance Management.

To grant Admins the Compliance Manager role, assign view privileges to access the Compliance Manager tab in Zoom.

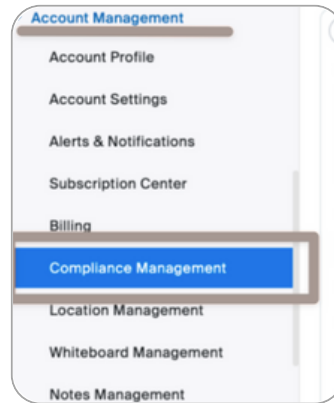
- User Management > Roles > select Compliance Management.



10

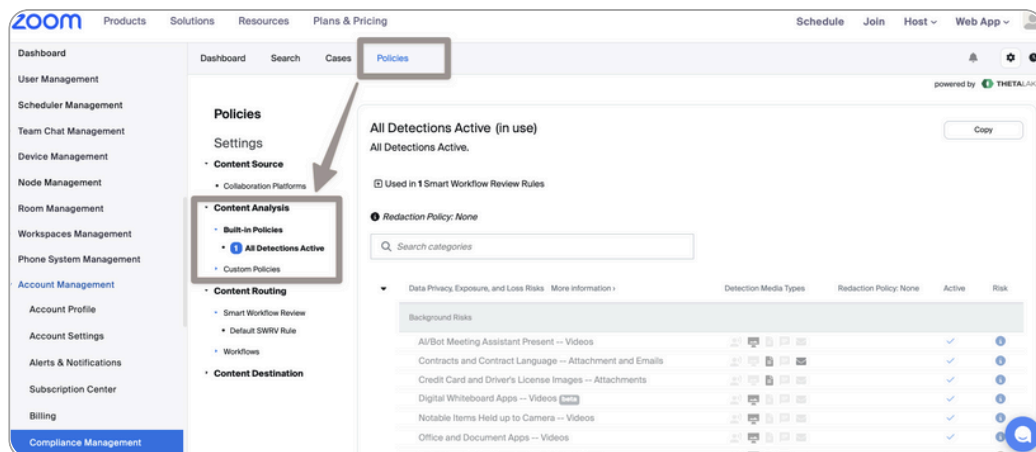
Leverage Zoom "compliance manager powered by Theta Lake"

To understand how Content Routing (SWRV) - Zoom works, how it functions to provide surveillance and compliance oversight for your digital media, and how it's Smart Workflow Review (SWRV) ("swerve") routing policies push data through system visit: [Theta Lake Content Workflow \(SWRV\)](#).



Define data policies in Theta Lake portal, by default, there is a single policy active when you first log in to Theta Lake. This policy was activated by Theta Lake operations to get you up and running quickly. No further action is necessary unless you want to configure one or more specific policies for your organization.

You can view the active policy in zoom as well. To view the active policy navigate to the Policy tab in Compliance Management. You can view the set of rules on the right pane, these set of rules can be updated in the Theta Lake portal.



11

Conduct Regular Security Audits

Security configurations should evolve to address new threats and organizational changes. Schedule quarterly reviews of Zoom security settings.

- Assess compliance with internal policies and external regulations (e.g., GDPR, HIPAA).
- Document all the findings and implement improvements to strengthen your security posture.

12

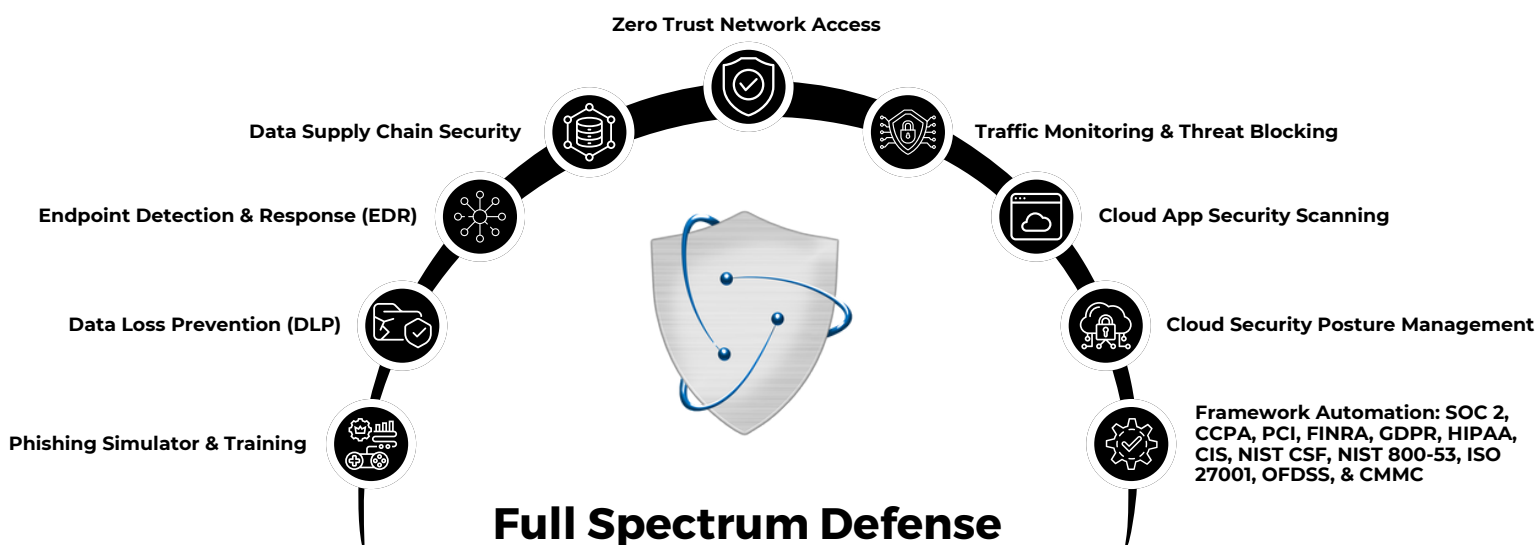
Update Zoom Regularly

Staying updated ensures you benefit from the latest security patches and features. Enable automatic updates for all Zoom clients and periodically check the Zoom Admin Portal for announcements about new security features.



Explore **Cytex Unified Resilience Platform** today

[Schedule demo](#)



<https://cytex.io>



hello@cytex.io



[@cytexsmb](#)



[@cytexsecure](#)