



Advanced Security
Configurations & Tips

The ultimate guide to secure Slack



hello@cytex.io

cytex.io



Slack security best practices

Secure Slack with this step-by-step cheat sheet. Implement these essential settings to eliminate misconfigurations and prevent data breaches and unauthorized access, enabling worry-free collaboration.



1

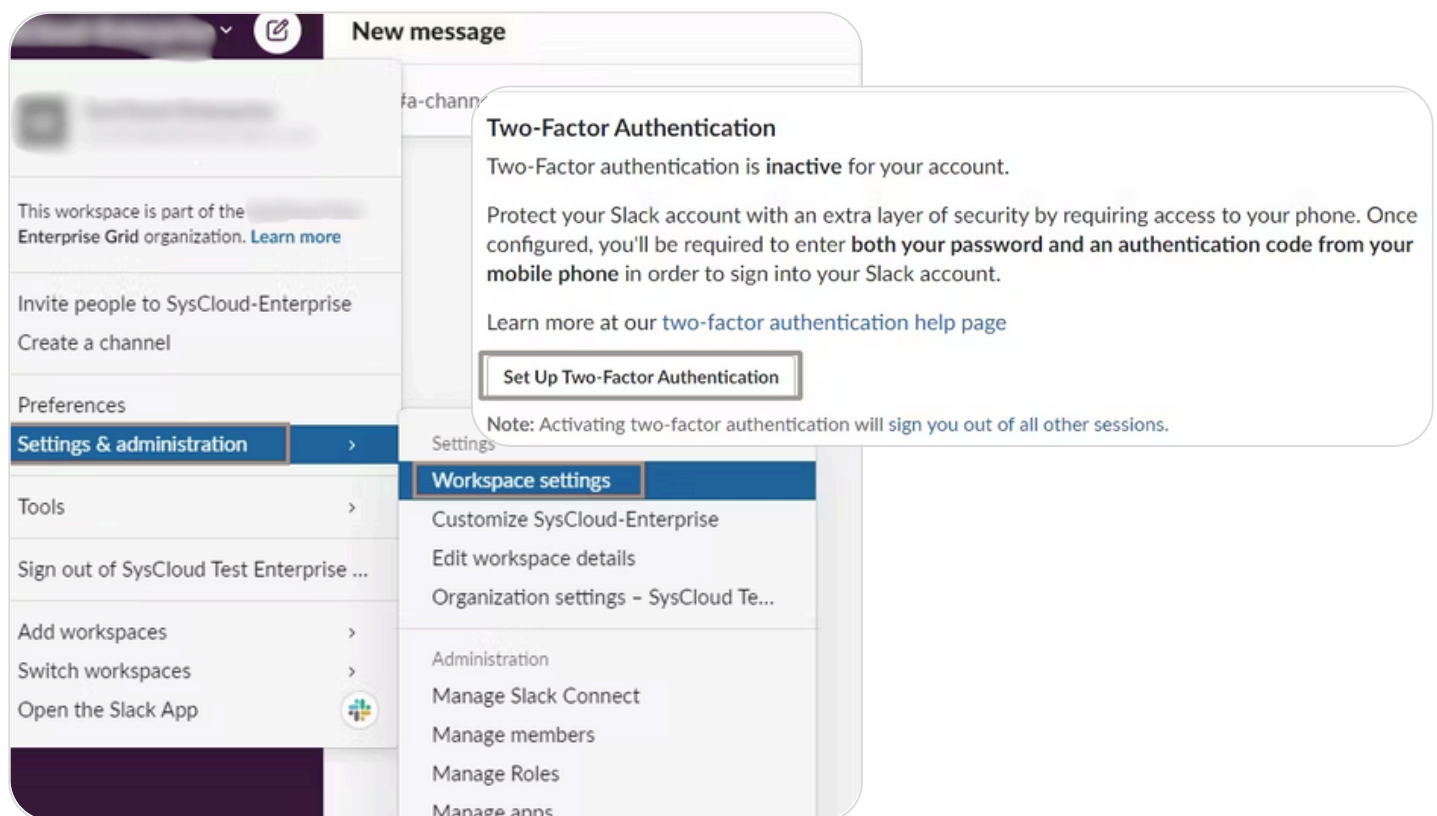
Enable mandatory workspace two-factor authentication (2FA)

For an added layer of security, you should require your members and guests to use two-factor authentication (2FA) when they sign in to Slack.

PS: If you're using single sign-on (SSO), 2FA should be set up through your identity provider.

- Click your workspace name in the sidebar.
- Select Tools & settings > then click Workspace settings/Organization settings.
- Select Security from the left sidebar > click Security settings.
- To the right of Two-factor authentication for email sign-in > click Enable.
- If you'd like, click Require an authenticator app to prevent members from using SMS for 2FA.
- When you're ready, click Enable. Members will get an email and a Slackbot message to help them to get set up.

People who don't set up 2FA within 24 hours will be signed out of Slack and prompted to set up 2FA before they can sign in again. New members will be required to set up 2FA before signing in to Slack.



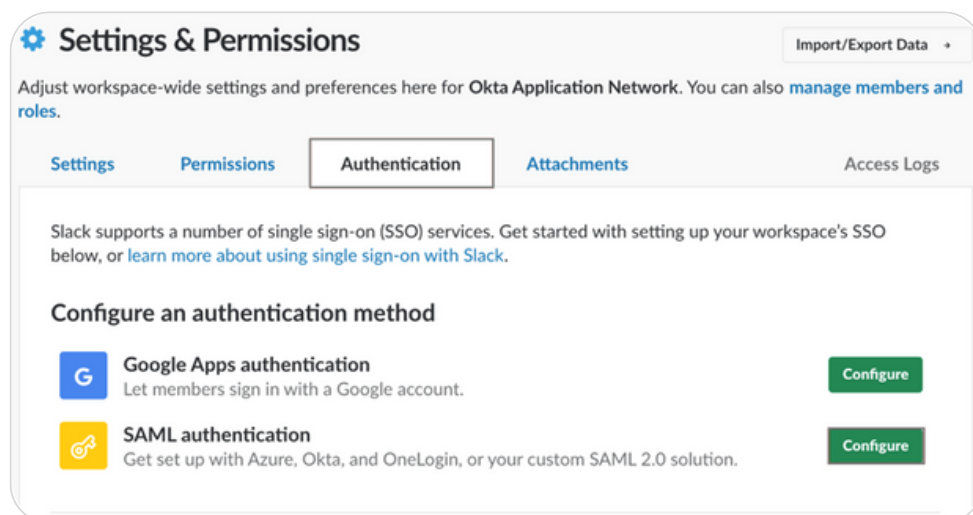
2

Use 2FA with single sign-on ; SSO integration

Single Sign-On (SSO) centralizes user authentication and ensures better control over access to Slack. Workspace Owners and Org Owners can enable single sign-on (SSO) as an extra layer of security for their organization.

When an Org Owner or Workspace Owner enables single sign-on (SSO) or requires members to re-authenticate, each member is notified via email that explains the 'how to connect (or "bind") your Slack account with your identity provider (IDP)'.

- *PS: A team member/employee SSO binding email will expire after 72 hours. You can always request a new email from an Org Owner or Workspace Owner.*
- Click your workspace name in the sidebar.
- Select Tools & settings > click Organization settings.
- From the left sidebar, select Security > click SSO Settings.
- Under For the organization, select the desired configurations.



Slack also provides access through SAML-based SSO, visit this link to find configurations to set up a connection/connector for Slack with the identity provider (IDP) of your choice: [Configuring your identity provider](#)

3

Enable workspace-wide encryption

Slack encrypts data at rest and in transit by default, ensuring security during storage and transmission. For added security, Enterprise Key Management (EKM) is available based on your plan. With Enterprise Grid, you can manage encryption keys via AWS Key Management Service (KMS), offering greater control over data access and encryption.

Slack official setup guide for Slack EKM, AWS KMS, and AWS CloudWatch/CloudTrail Logs setup, visit > [Slack \(detailed\) EKM guide](#)

4 Configure data retention policies

Slack (business/enterprise) will retain all messages, canvases, lists, and files (including audio and video clips) for the lifetime of your workspace. Users can adjust retention settings to automatically delete data after a specified time and allow members to edit retention settings for specific channels and direct messages (DMs).

As an Org Owner, you can establish a message retention policy for all workspaces in your organization. This policy prevents Workspace Owners from modifying retention settings. Additionally, Org Owners can choose to hide messages before permanent deletion. Following options are available for setting message retention for conversations:

1. Keep everything
 - Slack will keep all messages and track message edits and deletions.
 2. Keep all messages, but don't track revisions
 - Slack will keep all messages, but will not track message edits or deletions.
 3. Delete messages after a specific time period
 - Slack will delete messages following the custom time frame you choose.
- For Pro and Business+ subscriptions click on your workspace name
 - Select Settings and Administration > Workspace settings
 - Click on the Expand button next to Message Retention and Deletion.
 - Select your preferred retention settings from the drop-down menu > click save.
 - Check the box next to Yes, apply these new settings > click on Confirm Settings.

Message Retention & Deletion

By default, Slack keeps all your messages for the lifetime of your workspace. If you'd like, you can have them deleted after a set amount of time. You can also [configure this for specific channels](#).

In channels shared with other organizations, your retention settings will only apply to messages from members of your organization. [Learn more about retention in shared channels](#)

Public channels

Keep all messages, but don't track revisions (i.e. edits and deletions)

Private channels

Keep all messages, but don't track revisions (i.e. edits and deletions)

Direct messages

Keep all messages, but don't track revisions (i.e. edits and deletions)

Message Retention Overrides

☐ **Allow admins to override channels**
Admins can override settings on the Manage Channels page

☐ **Allow workspace members to override private channels and direct messages**
Workspace owners can edit settings for public channels

Save

Apply new retention settings?

Warning: Messages deleted by retention settings are truly, permanently deleted. These messages can't be restored or recovered, even by Slack.

Here's what your new settings will be:

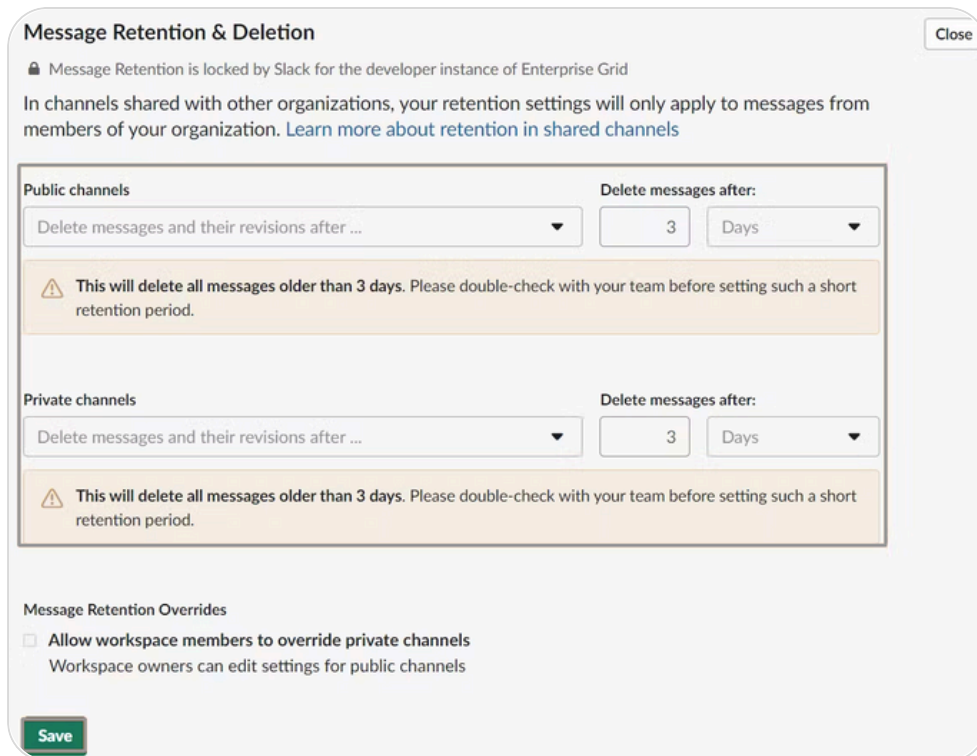
- Public channels – Keep messages, but don't track revisions
- Private channels – Keep messages, but don't track revisions
- Direct messages – Keep messages, but don't track revisions
- Admins cannot override these settings
- Workspace members cannot override these settings

☒ **Yes, apply these new settings**

Cancel **Confirm Settings**

4 Configure data retention policies

- For Enterprise Grid subscription set org-level message retention settings click on your workspace name > select Settings and Administration > Workspace settings
- Select Messages and Files from the Settings bar on the left.
- Review your policies under Message retention policies.
- Click on the Expand button next to Message Retention and Deletion.
- Select your preferred retention settings from the drop-down menu > click save.
- Check the box next to Yes, apply these new settings > click on Confirm Settings.



Message Retention & Deletion Close

Message Retention is locked by Slack for the developer instance of Enterprise Grid

In channels shared with other organizations, your retention settings will only apply to messages from members of your organization. [Learn more about retention in shared channels](#)

Public channels Delete messages after:

Delete messages and their revisions after ... 3 Days

Warning: This will delete all messages older than 3 days. Please double-check with your team before setting such a short retention period.

Private channels Delete messages after:

Delete messages and their revisions after ... 3 Days

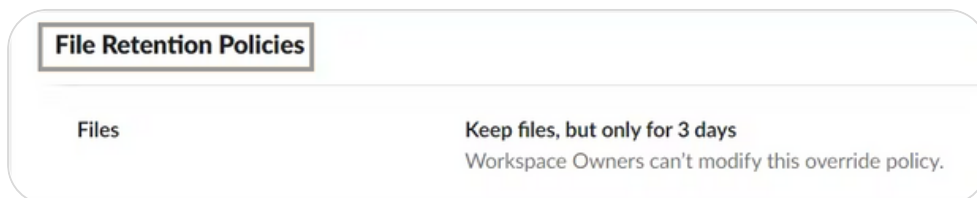
Warning: This will delete all messages older than 3 days. Please double-check with your team before setting such a short retention period.

Message Retention Overrides

☐ Allow workspace members to override private channels
Workspace owners can edit settings for public channels

Save

- Similarly, review and customize the Messages and Files retention policy from the same settings.
- Select Messages and Files from the Settings bar on the left.
- Review your policies below File retention policies.



File Retention Policies

Files Keep files, but only for 3 days

Workspace Owners can't modify this override policy.

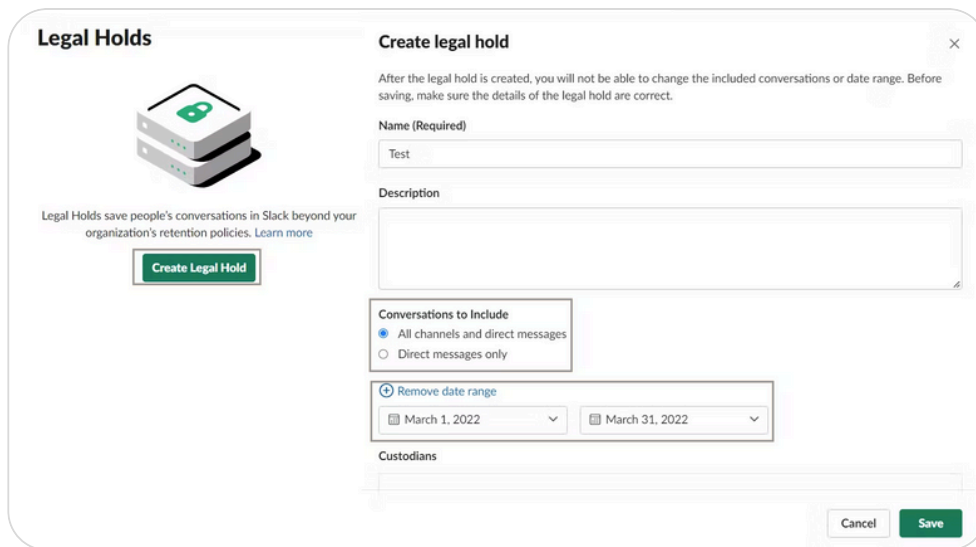
5 Configure and retain Slack data using legal hold

Legal holds preserve information for litigation by saving all messages and files in a conversation, regardless of retention settings. Data under legal hold can be accessed via export or Discovery API. In Enterprise Grid subscriptions, compliance system admins can place holds on specific members to secure their messages and files in Slack.

5

Configure and retain Slack data using legal hold

- Login to Slack using your compliance admin credentials
- Click on your workspace name on the top left > select Settings and Administration.
- Click on organizational settings > select security from the left sidebar.
- Select legal holds > click on create hold.
- Create a hold by adding name, description, selecting which conversations to include and an optional date range.
- To select the members to include in the hold, click on add custodians.
- Click Save.



6

Slack Connect configurations for secure collaboration with external organizations

Fine-tune Slack Connect settings to prevent unauthorized access and to control external access to your workspace: manage who can send invites and what permissions external guests have in your channels.

- Click on your workspace name on the top left > select Tools & settings > click Organization settings.
- Click Slack Connect in the left sidebar > select Settings.
- Select the Channels tab > next to Sending channel invitations > click Edit.
- Toggle off/on for the invitation type. If on, decide who from your organization can send each invitation type > click Save.

Slack Connect member profiles

Choose what information about your members should be visible when working with other organisations.

What information should be visible to people outside ClearFeed?

- ☒ **Basic details (default)**
Name and photo only
- ☐ **Standard work details**
Information that helps everyone know who they're working with, including title, status, local time, pronouns, pronunciation and do not disturb settings

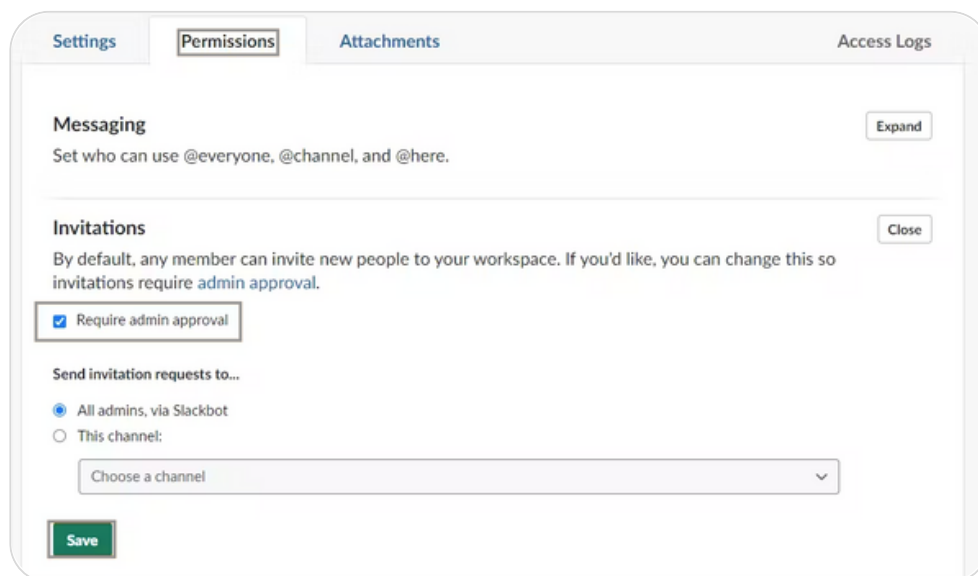
 To manage email address visibility, go to [Email address display](#).

7

Limit access to workspace

To protect sensitive information in Slack, admins must control workspace access by managing invitations, verifying email domains, deactivating inactive accounts, and limiting guest access to specific channels.

- Click on your workspace name on the top left > select Settings and Administration > click Workspace Settings.
- Click the Permissions tab.
- Click Expand in the Invitations section.
- Check the box next to Require admin approval > click Save.



8

Account deactivation configurations - Employee off-boarding

Deactivating former employees' accounts is crucial to prevent security breaches and compliance lapses. This immediately signs the user out of all devices, preventing further access.

Remove someone from a workspace

- Click on your workspace name on the top left > select Tools & settings > click Manage Members.
- Click the three dots icon to the right of the member you'd like to remove.
- Select Remove from workspace.

Deactivate an account

- Click on your workspace name on the top left > select Tools & settings > select Organization settings.
- Click People in the left sidebar > select Members.
- Check the box next to any members you'd like to deactivate.
- Click Deactivate above the list of members.

9

Install and enable Enterprise Mobility Management (EMM) for your organization

Enterprise Mobility Management (EMM), or Mobile Device Management, allows organizations to control the use and access of company data on mobile devices. EMM allows a company to control how employees access apps and networks on mobile devices. With EMM for Slack installed, only approved mobile devices can access workspaces on your Slack Enterprise Grid.

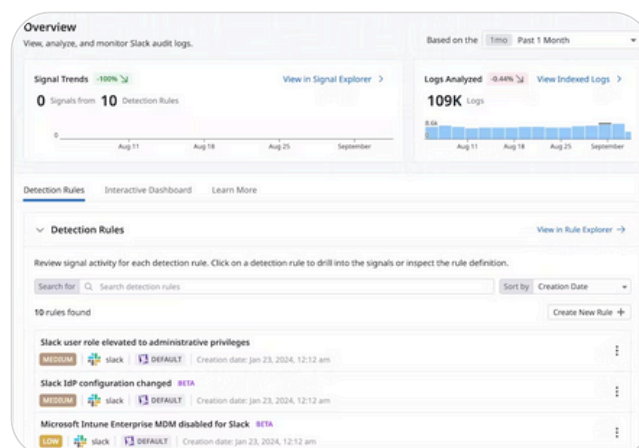
- Step 1: Choose an EMM provider
 - Connect with a Slack for EMM provider to learn more and set up your account. Slack supports several EMM providers like: VMWare Workspace ONE UEM, MobileIron, and BlackBerry.
- Step 2: Turn on EMM
 - Contact Slack to activate or modify mobile security settings for your organization. Only members using an approved device can access your organization's workspaces. You can select one of the options below:
 - All members (excluding guests) will be required to update to the Slack for EMM app. Guests can sign in from any device.
 - All members (including guests) will be required to update to the Slack for EMM app and must use an approved device to access Slack.
 - All members and guests can use either the regular Slack app or the Slack for EMM app and sign in from any device.

10

Leverage Slack's audit logs for compliance

Audit logs support regulatory compliance by granting access to message and file data for audits. Slack's audit reports on Enterprise Grid allow organizations to send data to SIEM tools and monitor for potential security issues or unauthorized access attempts.

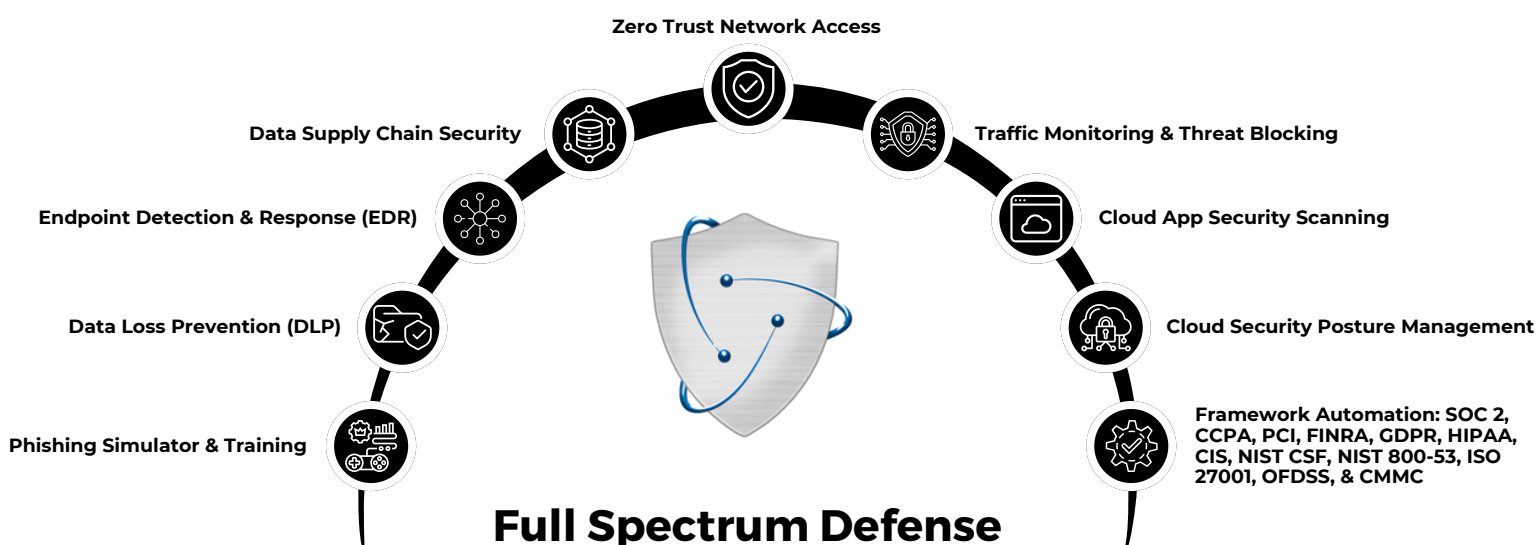
- Click on your organization name on the top left > select Tools & settings > click Organization Settings.
- From the left sidebar select Security > click Audit Logs.
- Use the drop-down menus to filter the log entries by Acting user, Event, Affects, or Date range and review the log entries below. If you'd like, click Export Logs in the top-right corner, then select a formatting option from the drop-down menu to download them.





Explore **Cytex Unified Resilience Platform** today

[Schedule demo](#)



<https://cytex.io>



hello@cytex.io



[@cytexsmb](#)



[@cytexsecure](#)