

Best Practices for Auditor setup

For Auditor to begin scanning and flagging emails effectively, it is necessary that all the primary setups required for its working are in place. To avoid encountering any problems using Auditor, please refer to the setup best practices provided here.

1. When registering for Auditor, always use the domain that student email addresses belong to. For example, if your school has two domains 'domain.com' and 'domain.org' and the student email IDs are 'student@domain.com' then you should use 'domain.com' to register. This ensures that all student emails are scanned by Auditor.
Note: All types of domain names such as '.com', '.org', '.edu', '.net' etc. can be used when registering for Auditor without impacting its efficiency.
2. Ensure that the domain you use for sign-up has not been used previously. If you use the same domain name you will encounter an error in sign up.
3. The subdomain you enter should also be a valid subdomain of the primary domain you enter. If not, you will encounter an error in sign up.
4. Remember to remove any special characters such as '@' when providing the domain name during Auditor sign up. *Note: If your school district uses multiple domains, you would need to register for Auditor using each of the domains separately to scan emails on all domains.*
5. Ensure that the credentials you use belong to the Super Admin account. Any other credentials will lead to an error in sign up.
6. Configure Auditor routing for the OU for which Auditor is set up. (The routing setup process is explained in the Auditor Setup Guide.)
Note: OU settings associated with a parent OU are inherited by the child OU.
7. Always uncheck the 'Bypass spam filter for this message' under the OU's Routing settings to ensure that even spam messages are filtered by Auditor. Unchecking this option would not flood student or staff inboxes with spam as the setting only ensures that a copy of the spam message is sent to the Auditor server. Student spam settings remain unchanged.

Add setting

Prepend custom subject

Route

Change route

Envelope recipient

Change envelope recipient

Spam

Bypass spam filter for this message

Attachments

Remove attachments from message

Also deliver to

Add more recipients

Recipients ADD

Use route: Auditor

CANCEL ADD SETTING

8. Always check the 'Add X-Gm-Spam and X-Gm-Phishy headers' checkbox to help the Auditor engines handle spam messages better.
9. Make sure not to check the 'Remove attachments from message' checkbox under 'Attachments' if you have also signed up for Auditor. (Learn why.) If you are only an Auditor customer, check the checkbox for this field.

Add setting ✕

Change envelope recipient

Spam and delivery options

Do not deliver spam to this recipient

Suppress bounces from this recipient

Headers

Add X-Gm-Original-To header

Add X-Gm-Spam and X-Gm-Phishy headers

Add custom headers

Subject

Prepend custom subject

Attachments

Remove attachments from message

Append this text to notify recipients that attachments have been removed:

CANCEL **ADD SETTING**

10. Ensure that you have whitelisted securly.com in your G Suite and can receive emails from Securly in your inbox. Without this, your Auditor setup will fail. To learn more about this setting, [click here](#).

By following these best practices, you can ensure that your Auditor is set up correctly and monitors student emails for cyberbullying and self-harm effectively.