# Audit Bot

Audit Bot is for compliance with the law or your organization's guidelines. This service account allows you to read every conversation on your server, including encrypted conversations.

**Audit Bot is only available on homeservers with the Element Enterprise Cloud plan.**

## Use case examples

- A law or organisational guideline requires you to store all written correspondence.
- A legal investigation requires you to verify or deny if a certain message has been sent.

## Good to know

- Audit Bot joins all rooms and spaces created by your users.
- Audit Bot also joins Direct Message rooms created by your users.
- The use of Audit Bot is visible to your users. The service account cannot be hidden. In Direct Message rooms it will not appear in the room title but is visible in the room member list.
- Audit Bot does not join rooms created by users on others servers. You can still manually invite Audit Bot.
- The user account `auditbot` will be used. The full Matrix ID will be something like `@auditbot:element.io` .
- Audit Bot is able to read encrypted messages to allow you to read or store all messages.

## See also

AuditBot for regulation and compliance.

# Setup

1. Go to the Integrations tab on the EMS homeserver page.
2. If you have more than one homesever, select the homeserver to add Audit Bot to.
3. In the section Extensions, click on `Audit Bot`. If this is not visible, check that the homeserver is using the Element Enterprise Cloud plan.
4. Click on `Set Up Integration` and confirm the pricing in a modal.

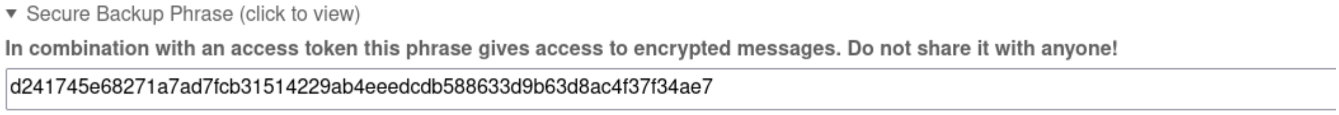
# Optional export

Audit Bot can be configured to write all decrypted events in all rooms to an S3-compatible storage of your choice. This is a continous export which will start with the configuration of a bucket and stop if you clear the configuration. Messages from the past are not exported retrospectively.

# Usage

You can use Element Web to log into the `auditbot` account:

1. Go to the Integrations tab on the EMS homeserver page.
2. If you have more than one homeserver, select the one you want to administrate.
3. In the section Extensions, click on `Audit Bot`. If this is not visible, check that the homeserver is using the Element Enterprise Cloud plan.
4. If this is the first time you log in using this browser, click `Secure Backup Phrase (click to view)` and copy the phrase to your clipboard.

   ▼ Secure Backup Phrase (click to view)

   **In combination with an access token this phrase gives access to encrypted messages. Do not share it with anyone!**

   d241745e68271a7ad7fcb31514229ab4eeedcdb588633d9b63d8ac4f37f34ae7

5. Click on `Log in as Audit bot`. You will need to enter the Secure Backup Phrase on first login with a new browser in order to access Secure Storage and encrypted messages.

# Removal

Removing the integration will not cause the user `auditbot` to leave rooms. This is a separate step to make mistakes easier to recover from. If the integration was accidentally deactivated and Audit Bot left rooms as the last local Administrator in that room, such rooms can no longer be moderated by anyone and need to be abandoned. Those room also couldn't be rejoined by Audit Bot.

You can deactivate the `auditbot` account using the EMS Admin GUI or Synapse Admin API, if you want it to leave all rooms.

Revision #5
Created 18 April 2022 14:20:05 by Karl Abbott
Updated 6 November 2024 12:28:58 by Kieran Mitchell Lane