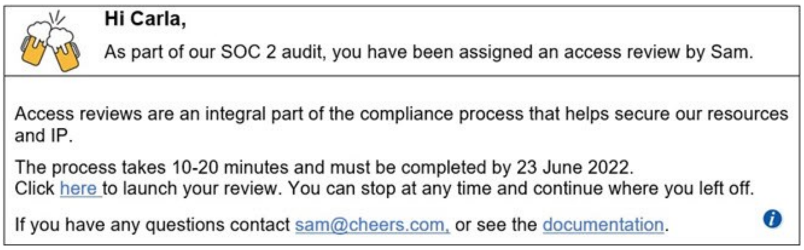
Reviewing access privileges (Reviewer’s experience)

Access to digital assets must be reviewed to ensure that only people who actually need access, get access. This greatly decreases the asset’s vulnerability to attacks and abuse. Industrial and government standards and regulations require periodic reviews of privileged or sensitive access to help you stay secure.

Note: Access privileges are the specific actions you can perform on the asset (such as edit, copy, delete). Assets can be files, folders, databases, drives or applications.

You've got mail!

If you got an email (or Slack message) like the one below, you are required to complete an access review.



Hi Carla,

As part of our SOC 2 audit, you have been assigned an access review by Sam.

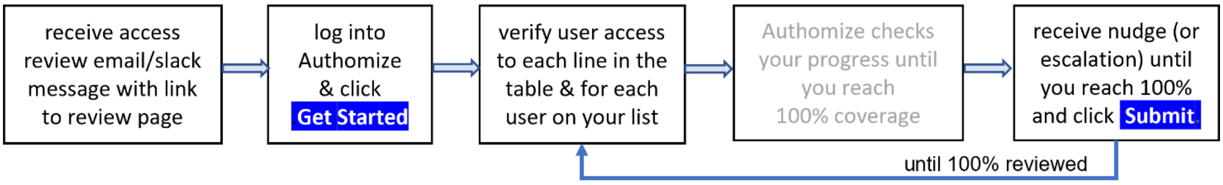
Access reviews are an integral part of the compliance process that helps secure our resources and IP.

The process takes 10-20 minutes and must be completed by 23 June 2022.
Click here to launch your review. You can stop at any time and continue where you left off.

If you have any questions contact sam@cheers.com, or see the documentation.

Access review workflow

The reviewer’s access review process looks like this:

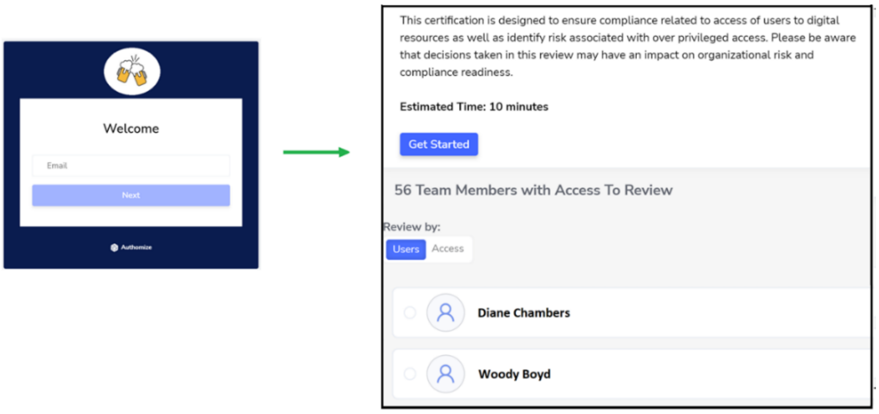

receive access review email/slack message with link to review page
log into Authomize & click Get Started
verify user access to each line in the table & for each user on your list
Authomize checks your progress until you reach 100% coverage
receive nudge (or escalation) until you reach 100% and click Submit
until 100% reviewed

Click the **here** button in the message to launch the review.

Logging into Authomize

In some organizations the summary page will open automatically and ask you to log in. In others, you will need to register first before you can log in (for more information see the SSO section below).

Once you’ve logged in, an access review summary page opens. To start the review process, click Get Started .



This certification is designed to ensure compliance related to access of users to digital resources as well as identify risk associated with over privileged access. Please be aware that decisions taken in this review may have an impact on organizational risk and compliance readiness.

Estimated Time: 10 minutes

56 Team Members with Access To Review

Review by:

○ **Diane Chambers**

○ **Woody Boyd**

Based on the link that you received you might be directed into the campaign directly or into the personal reviewer dashboard.

Review dashboard

At the top of the page you will find a message directing you to the campaign that you should review first, since it's review date is about to pass (or may have already passed).

Below you will find a list of all the campaigns that are pending you decisions

It's possible to use the toggle at the top of the table to switch the view and see a list of all completed campaigns that were assigned to you, those include reviews that you have submitted or non completed reviews if the campaign itself was marked as completed by the admin

Verify access privileges

When starting an access review, a review dialog opens to show you:

○ an **Access** list (of assets, roles and groups) whose users you need to confirm
or a list of **Team members** whose access privileges you need to confirm

Note: These are different views of the same list. You can toggle between Users and Access (Users Access).

② you can pick an entry from the list or review them sequentially
the entry under review is listed up top, along with the type of entity it is

③ in the case of an Access list, pane ③ lists the people who currently have access
in the case of a Team members list, pane ③ lists what each member can access

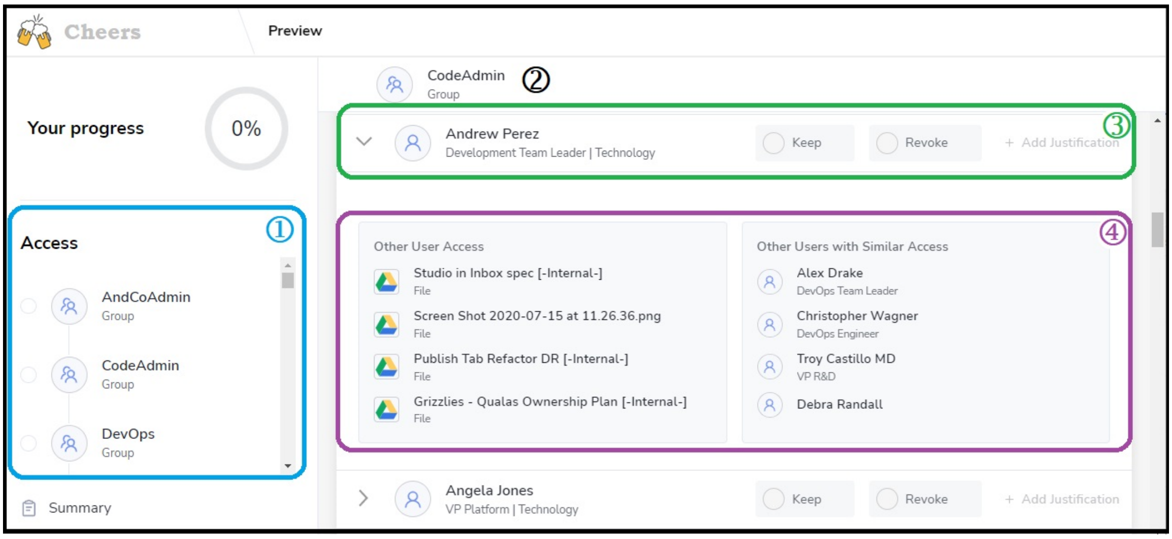
④ an additional context pane opens when **>** or **+ Add Justification** is clicked

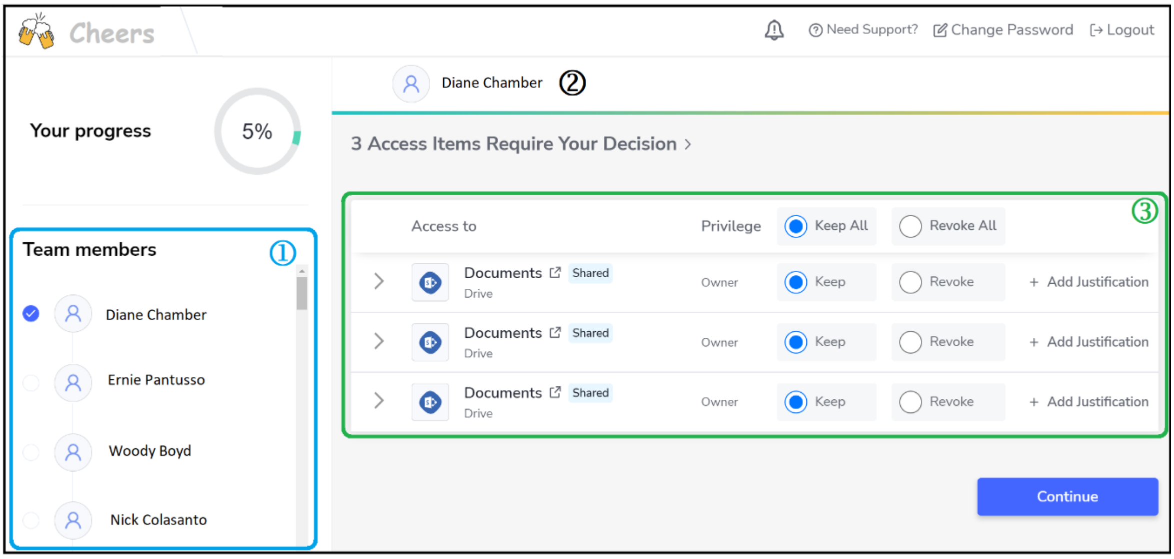
Go through the entire list (be it Access or Team members) until you have reviewed all the entries on the right (in pane ③). Note that the type of privilege the team member has on each asset is listed in the privilege column.

The account column provides information about the exact user account that grants this identity access to the asset or group membership

Click **Keep** or **Revoke** for each entry. You can explain your decision by clicking **+ Add Justification**.

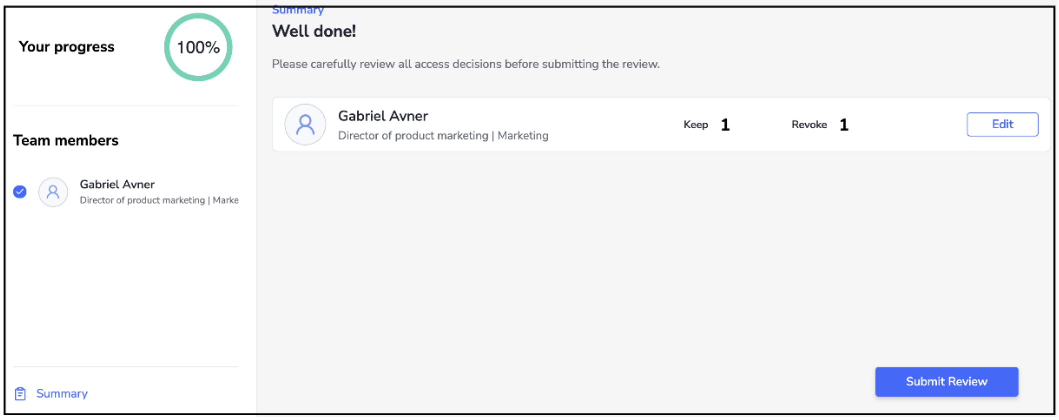
Note 1: You can go back and change your Keep/Revoke decision, until submitting your review.





Access to	Privilege	● Keep All	○ Revoke All	
Documents Shared Drive	Owner	● Keep	○ Revoke	+ Add Justification
Documents Shared Drive	Owner	● Keep	○ Revoke	+ Add Justification
Documents Shared Drive	Owner	● Keep	○ Revoke	+ Add Justification

Click **Continue** to jump to the next review. If you leave in the middle, the review restarts where you left off (and nothing is lost). When you have completed the review ("Your progress" is 100%), Once completed, go to the summary screen to submit the review by clicking `Submit Review`.

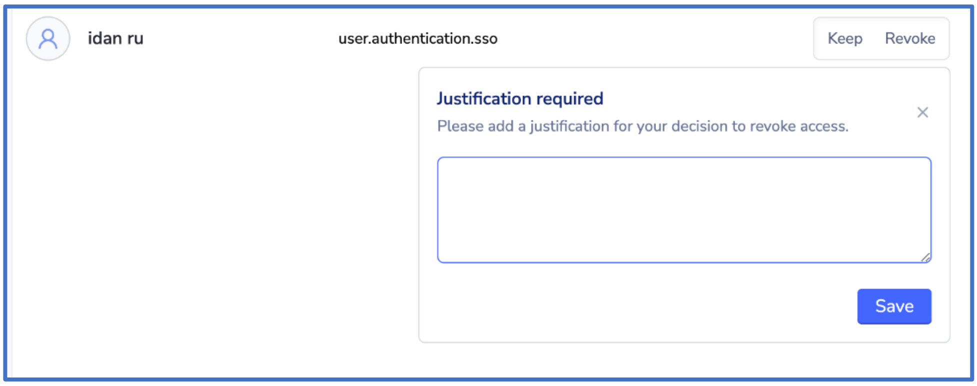


Please carefully review all access decisions before submitting the review.

Gabriel Avner Director of product marketing | Marketing	Keep 1	Revoke 1	Edit

When all Revoke decisions must be justified

In some campaigns, "Revoke" decisions cannot be submitted without written justification.



Justification required

Please add a justification for your decision to revoke access.

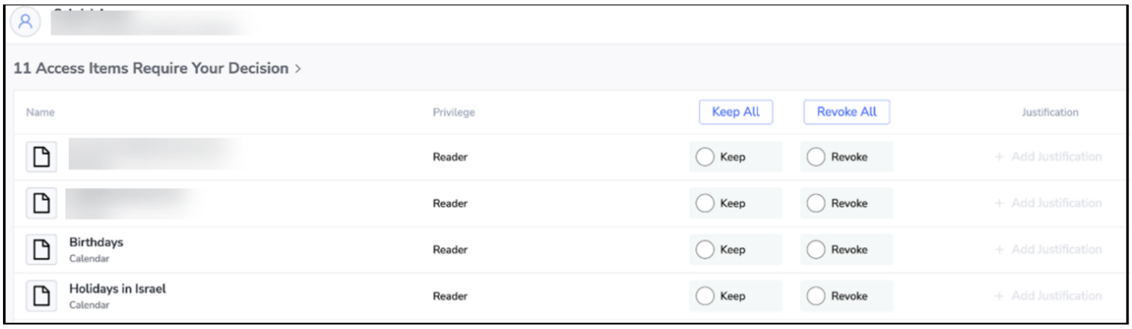
If you missed a "Revoke" justification, in such a campaign, the campaign will be incomplete.

Multiple justification

The access review process can potentially be tedious and repetitive, costing the company resources and fatiguing the reviewers. This is where automation and intuitive user experience come in.

Reviewers can provide multiple-entitlements with the same justification, which can be useful if entitlements can be grouped in some way and all deserve the same explanation.

To do this, hit Keep All or Revoke All:

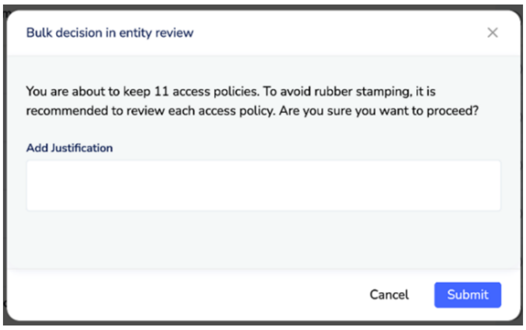


[redacted]

11 Access Items Require Your Decision >

Name	Privilege	Keep All	Revoke All	Justification
[redacted]	Reader	○ Keep	○ Revoke	+ Add Justification
[redacted]	Reader	○ Keep	○ Revoke	+ Add Justification
Birthdays Calendar	Reader	○ Keep	○ Revoke	+ Add Justification
Holidays in Israel Calendar	Reader	○ Keep	○ Revoke	+ Add Justification

When you do this, a new pop-up appears, asking if you are sure and asking you to provide a justification:



Bulk decision in entity review

You are about to keep 11 access policies. To avoid rubber stamping, it is recommended to review each access policy. Are you sure you want to proceed?

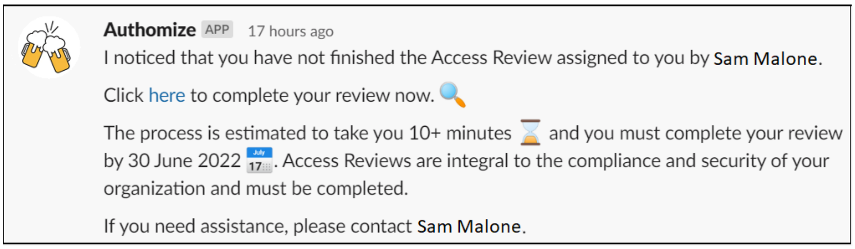
Add Justification

Type anything and click **Submit**. You'll see all of the entitlements got updated with the decision and with the justification. You can now edit any justification by clicking **View Justification** next to the entitlement.

This option is only available if the campaign owner enabled this in your organization. If you are not seeing those buttons, it means that the option is disabled.

Nudges and Escalation

The review request email has a completion date. If you do not make timely progress, Authomize will automatically send you a "nudge":



Authomize APP 17 hours ago

I noticed that you have not finished the Access Review assigned to you by Sam Malone.

Click here to complete your review now. 🔍

The process is estimated to take you 10+ minutes ⌛ and you must complete your review by 30 June 2022 📅. Access Reviews are integral to the compliance and security of your organization and must be completed.

If you need assistance, please contact Sam Malone.

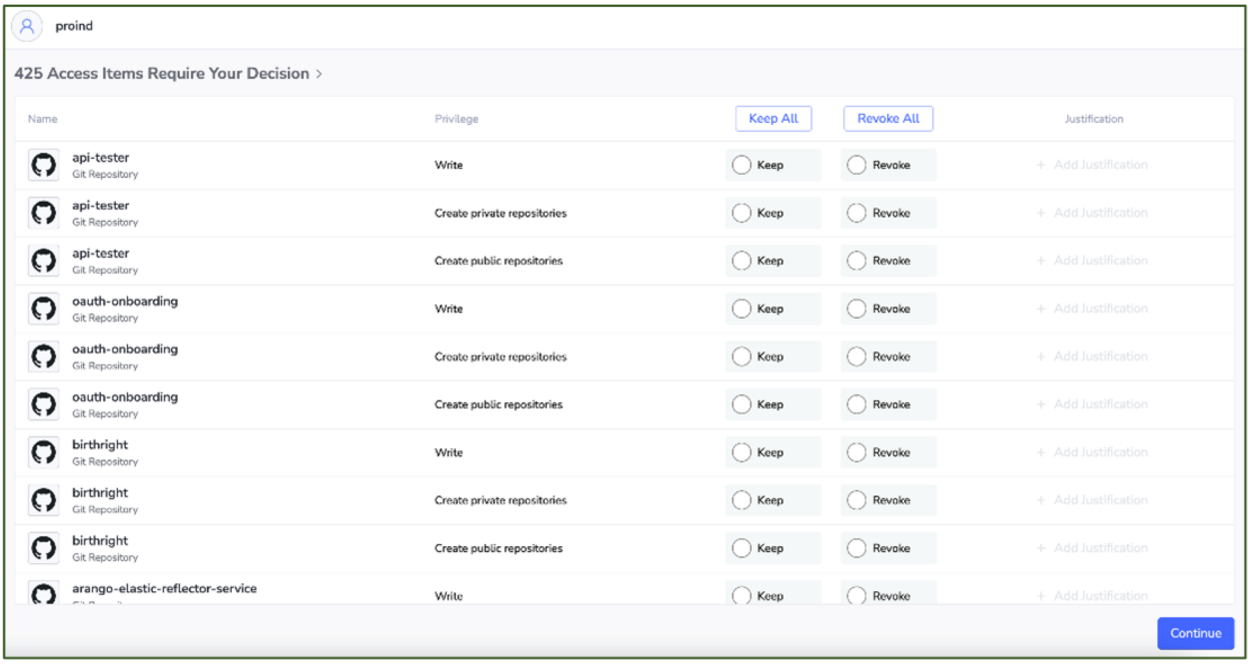
If you do not complete it on time, Authomize may be used to escalate or assign the review to someone else.

Reviewer Context

Reviewers need to be able to make educated decisions during an access review. This is important to ensure least privilege: stale, redundant accesses are removed while accesses needed for work is kept. It is also important to ensure no rubber stamping is taking place (rubber stamping is the practice of approving access automatically without proper consideration).

To this end, Authomize is provides a Context Panel feature with much more information about reviewed entitlements.

During the review experience, click on any entitlement on the left side of the table:



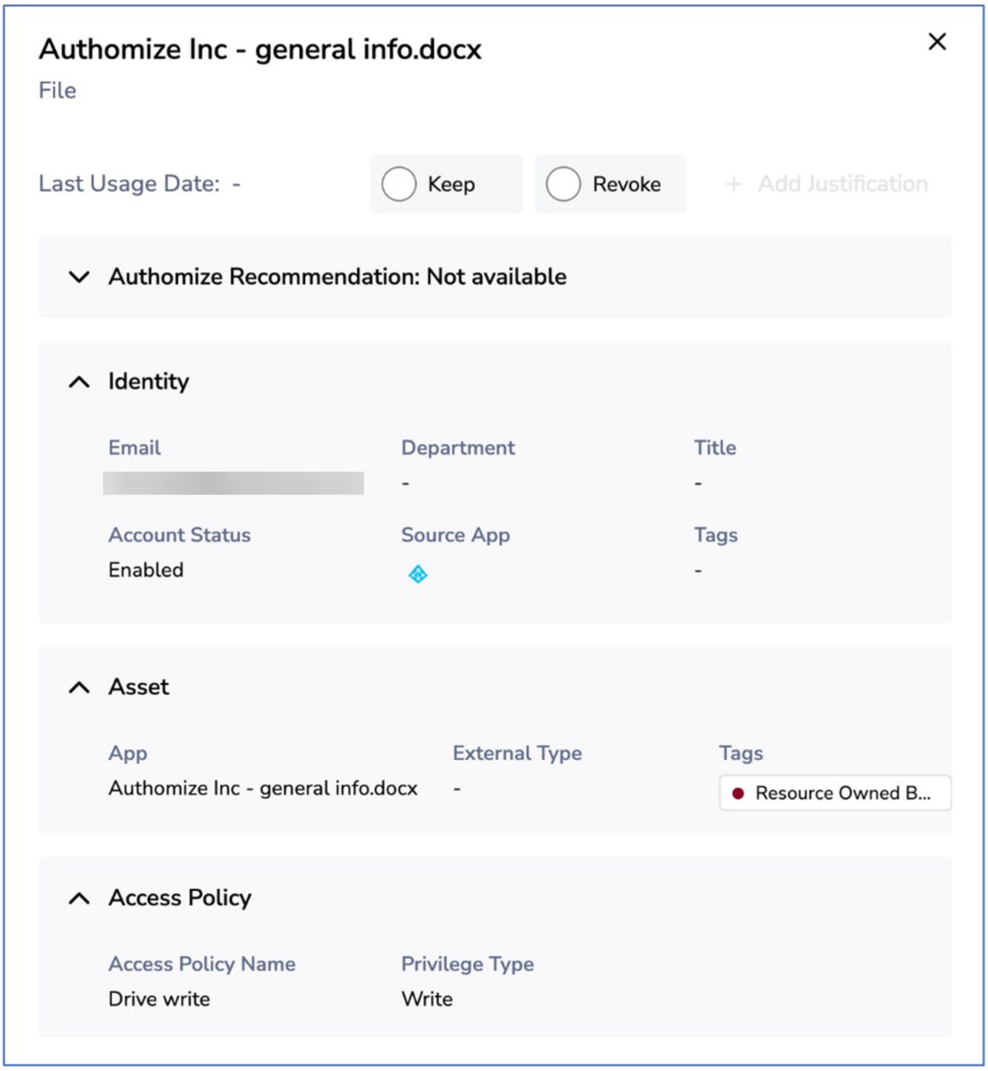
proind

425 Access Items Require Your Decision >

Name	Privilege	Keep All	Revoke All	Justification
api-tester Git Repository	Write	○ Keep	○ Revoke	+ Add Justification
api-tester Git Repository	Create private repositories	○ Keep	○ Revoke	+ Add Justification
api-tester Git Repository	Create public repositories	○ Keep	○ Revoke	+ Add Justification
oauth-onboarding Git Repository	Write	○ Keep	○ Revoke	+ Add Justification
oauth-onboarding Git Repository	Create private repositories	○ Keep	○ Revoke	+ Add Justification
oauth-onboarding Git Repository	Create public repositories	○ Keep	○ Revoke	+ Add Justification
birthright Git Repository	Write	○ Keep	○ Revoke	+ Add Justification
birthright Git Repository	Create private repositories	○ Keep	○ Revoke	+ Add Justification
birthright Git Repository	Create public repositories	○ Keep	○ Revoke	+ Add Justification
arango-elastic-reflector-service	Write	○ Keep	○ Revoke	+ Add Justification

The context Quick View panel opens on the right, with all the information Authomize has on the entitlement:

1. Authomize's **recommendation** and reasoning.
2. The **identity** that accesses the asset, is a member of the group or can assume the role.
3. The **asset** or **group** they have access to.
4. The **role** and **privileges** they have over them.



Authomize Inc - general info.docx

File

Last Usage Date: - ○ Keep ○ Revoke + Add Justification

Authomize Recommendation: Not available

Identity

Email	Department	Title
[redacted]	-	-
Account Status	**Source App**	**Tags**
Enabled	◈	-

Asset

App	External Type	Tags
Authomize Inc - general info.docx	-	● Resource Owned B...

Access Policy

Access Policy Name	Privilege Type
Drive write	Write

You can make decisions right on the panel, or close it by clicking the x icon on the top right corner.

Note: In the near future, the last usage date will be displayed on the top left corner.

Background information

Access to apps, assets, groups and roles is granted to people in the organization so they can do their jobs. Most organizations use hundreds of apps across different business units and entities. With so many apps it is very easy to lose track of who has access to what, causing massive security risks. That is Authomize's job: helping organizations stay *least privileged* in a complex landscape.

Authomize is used to set up Access review campaigns. Authomize finds the relationships between assets, identities and groups and sends access lists to reviewers for approval. Reviewers can be managers, asset owners or group owners. Access privileges that were revoked by reviewers are aggregated by the campaign owner and sent to the IT department for further action.

SSO (Single Sign-On)

If your organization has an SSO system in which Authomize is configured, you will automatically be transferred to your review.

If SSO is not configured, you'll get Authomize login credentials in an email or Slack message. The first time you log into Authomize, change your password after entering the email and password provided.

Terms used in the Entitlements dialog & elsewhere

Access privilege	The specific action you can perform on the asset (such as edit, copy, delete) Authorize displays the privilege in the same way that it appears in the downstream application.
Access to	The name and type of entity. If it is an asset, there is a link to the asset itself.
Asset	Any object that has permissions (file, folder, database, drive, application ...)
Entitlement	Entitlements or access privileges provide users with the ability to perform actions on different assets (such as edit, copy and delete).
Group	A collection of users.
Keep	Button that marks the entitlement to remain as-is.
Least privileged	Provide no more authorizations than necessary to perform required functions
Revoke	Button that marks an entitlement to be revoked.
Role	A function in an organization that has access privileges. Users may gain access privileges from their roles.
SSO	An authentication scheme that allows a user to log in with a single ID to any of several independent software systems.
Usage	How often the entitlement is used. Possible options - **unused** (not any usage or unknown), **frequently** (more than 100 times), **rarely** (less than 100 times).
+ Add Justification	Button to add justification note for the entitlement (will be seen by the campaign owner and auditor).