bitwarden | Help Center Article

Access Intelligence

View in the help center

https://bitwarden.com/help/access-intelligence/

Access Intelligence

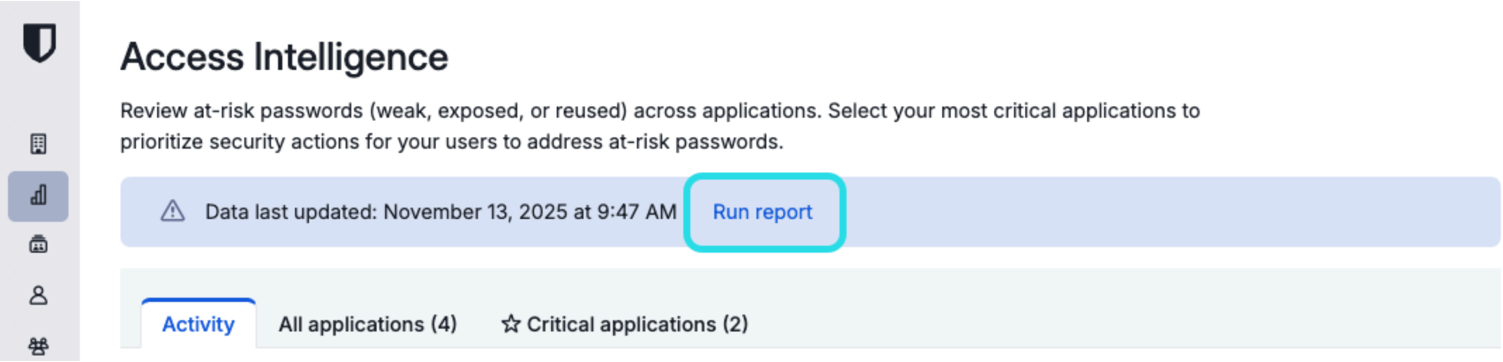
Enterprise organizations can use **Access Intelligence** to identify and prioritize applications with at-risk credentials that are stored within your Bitwarden organization by its members. Using this report, select critical applications and notify organization members that they need to take action on at-risk passwords.

Access Intelligence provides easy co-located visibility for admins into which credentials are at-risk, it does not grant administrators direct access to passwords they don't otherwise have access to.

> **Note**
>
> Access Intelligence does not allow admin visibility into items for which the organization is not the owner. To ensure full visibility into all potential at-risk credentials, Bitwarden recommends activating the Enforce organization data ownership policy so that all data is owned by the organization.

Run the report

As the application landscape evolves and changes within your organization, the contents of this report will change. It is critically important that Access Intelligence be treated as a continuous exercise. To update the report, take note of the **Data last updated** timestamp and select the **Run report** button.



Access Intelligence

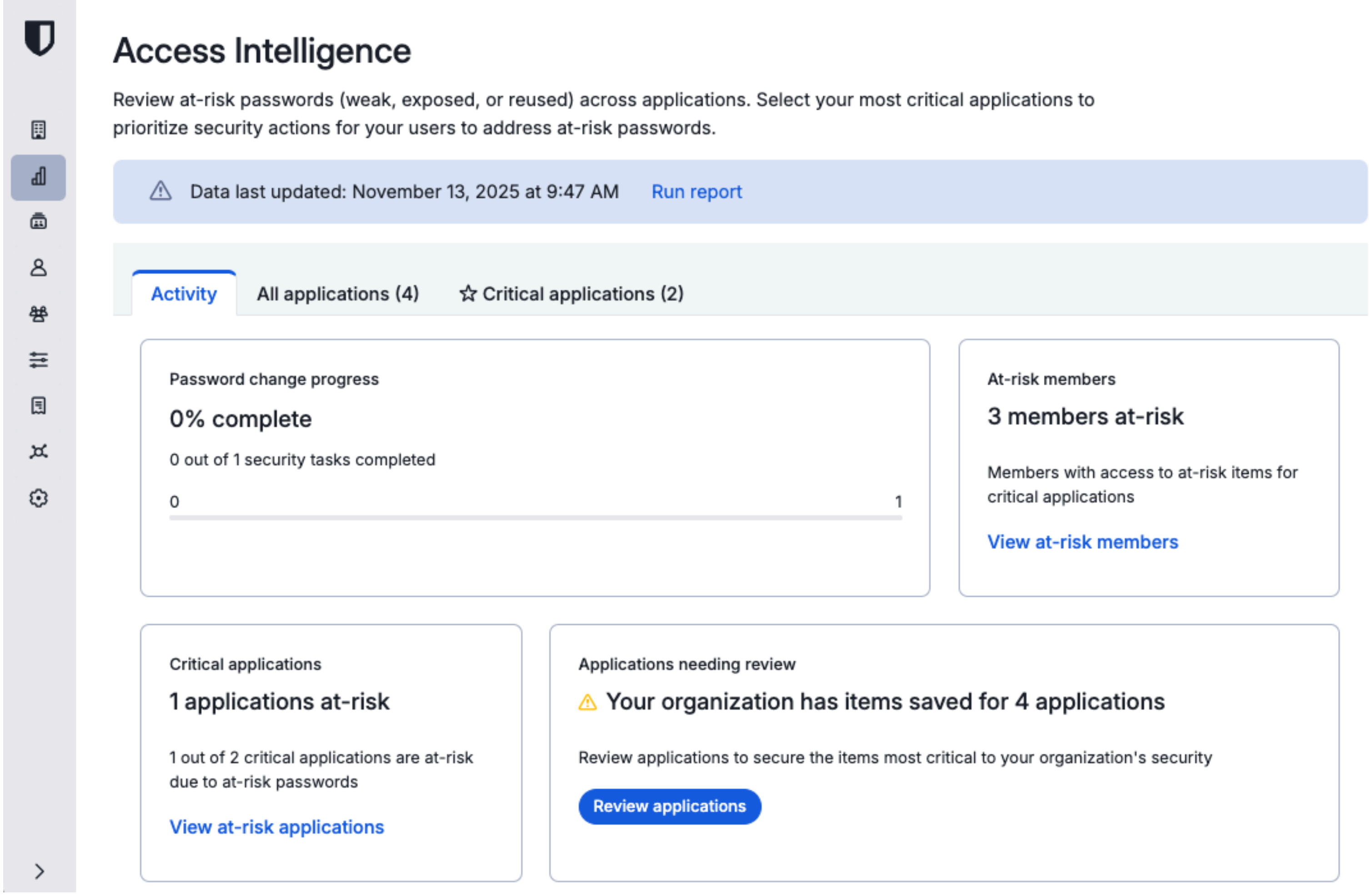
Review at-risk passwords (weak, exposed, or reused) across applications. Select your most critical applications to prioritize security actions for your users to address at-risk passwords.

Data last updated: November 13, 2025 at 9:47 AM

Run the Access Intelligence report

Activity

The **Activity** tab of the Access Intelligence report provides a summary of crucial datapoints and tasks. While the Activity tab provides this information at-a-glance, you should familiarize yourself with the **All applications** and **Critical applications** tab to best understand what's surfaced here:



Access Intelligence

Review at-risk passwords (weak, exposed, or reused) across applications. Select your most critical applications to prioritize security actions for your users to address at-risk passwords.

⚠ Data last updated: November 13, 2025 at 9:47 AM Run report

Activity | All applications (4) | ☆ Critical applications (2)

Password change progress

0% complete

0 out of 1 security tasks completed

0 1

At-risk members

3 members at-risk

Members with access to at-risk items for critical applications

View at-risk members

Critical applications

1 applications at-risk

1 out of 2 critical applications are at-risk due to at-risk passwords

View at-risk applications

Applications needing review

⚠ Your organization has items saved for 4 applications

Review applications to secure the items most critical to your organization's security

Review applications

Access Intelligence, Activity tab

- **Password change progress**: Percentage completion of dispatched password change requests.
- **At-risk members**: Number of members with access to at-risk items for critical applications.
- **Critical applications**: Proportion of critical applications that are currently at-risk.
- **Applications needing review**: Number of new applications added by members since the report was last run.

Determining risk

A password is determined to be **at-risk** if it is weak, exposed, or re-used within the organization. This analysis is done with the same tools used in the Weak passwords report, Exposed passwords report, and Reused passwords report. As is the case for running reports manually, the analysis done by Access Intelligence is done locally to preserve zero-knowledge and protect your data integrity and anonymity.

All applications

The Access Intelligence report lists all applications saved as items within your Bitwarden organization. Each application represents the set of all items with a URI that matches a given web service (for example, the "Atlassian" application may contain 26 "Total passwords", indicating there are 26 items that contain credentials for logging into Atlassian) and contains:

Column	Description
Application	The name of the application that is at-risk.
At-risk passwords	The number of passwords associated with the application that are at-risk.
Total passwords	The total number of passwords associated with the application.
At-risk members	The number of members who have access to the at-risk passwords associated with the application.
Total members	The total number of members who have access to the application.

Tip

By surfacing a list of all applications for which organization members have credentials, Access Intelligence can also help administrators detect the use of unsanctioned applications as well as those which could be migrated to single sign-on (SSO) authentication through an IdP.

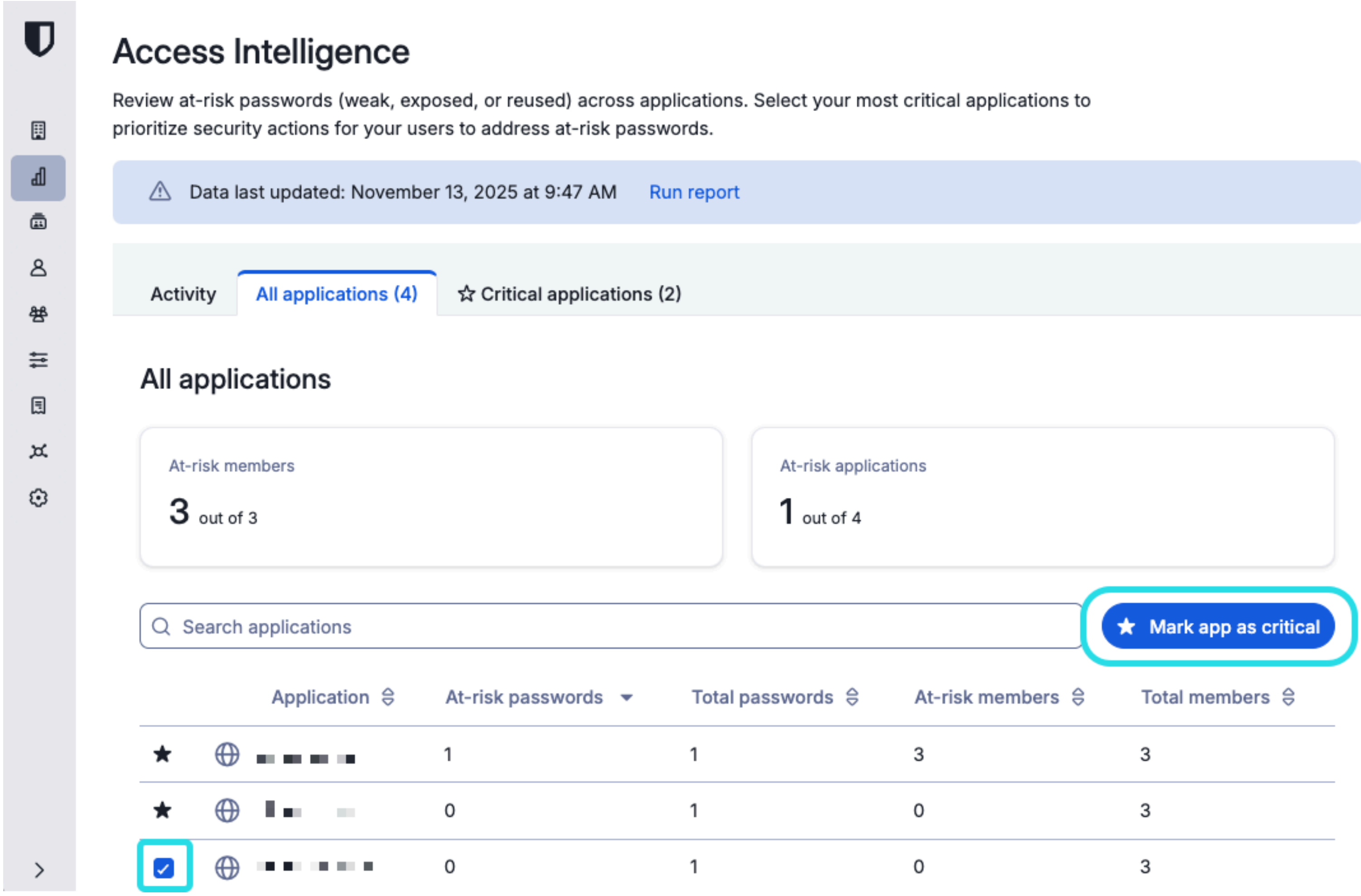
Marking critical applications

Tip

Marking a distinction between **Critical applications** and **All applications** is an important tool for ensuring organization members are encouraged to take quick action on the applications that matter most.

One important function of Access Intelligence is the ability to dispatch notifications to members informing them they need to take action on a critical at-risk password. Dispatching these notifications in targeted waves will help prevent member alert fatigue and resultant delays in remediation.

Applications marked **critical** are those which will have notifications dispatched to organization members informing them that they need to take action on at-risk passwords. To mark applications critical, toggle one or more checkboxes and select select the **Mark app as critical** button:



Access Intelligence

Review at-risk passwords (weak, exposed, or reused) across applications. Select your most critical applications to prioritize security actions for your users to address at-risk passwords.

⚠ Data last updated: November 13, 2025 at 9:47 AM Run report

All applications

At-risk members: 3 out of 3

At-risk applications: 1 out of 4

	Application	At-risk passwords	Total passwords	At-risk members	Total members
★	[redacted]	1	1	3	3
★	[redacted]	0	1	0	3
☑	[redacted]	0	1	0	3

Mark a critical application

Critical applications

Using Access Intelligence, administrators can preemptively assess which applications they want prioritized for members to take action on. The report can be narrowed down from **All applications** for which there are credentials stored within your organization to only those you select as the current **Critical applications** to take action on.

Requesting password changes

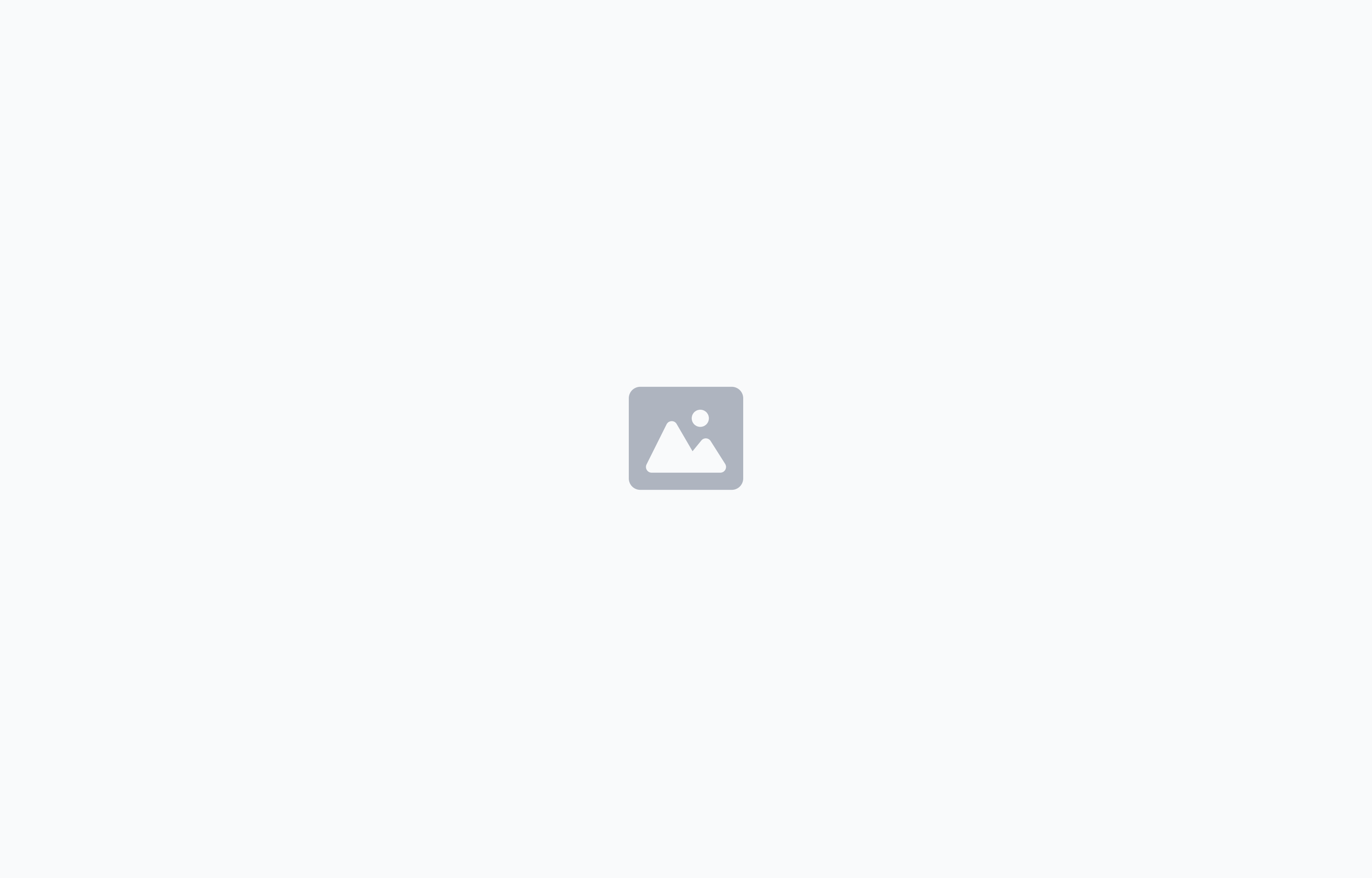
Requesting password changes will dispatch notifications to organization members with access to critical applications informing them that they need to take action on at-risk passwords. Members will receive notifications both in their email inbox and as a banner in a Bitwarden browser extensions they're logged in to.

Tip

Before dispatching your first password change requests, or as part of employee Bitwarden training, we recommend:

- Informing members that these emails are legitimate and should not be ignored.
- Providing members with instructions for how to take action on password change requests.

To request password changes on all applications currently marked critical, navigate to the **Critical applications** view and select **Request password changes**:



Request a password change