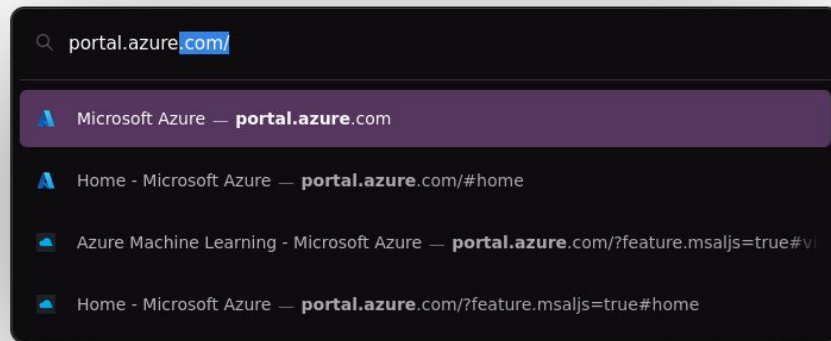
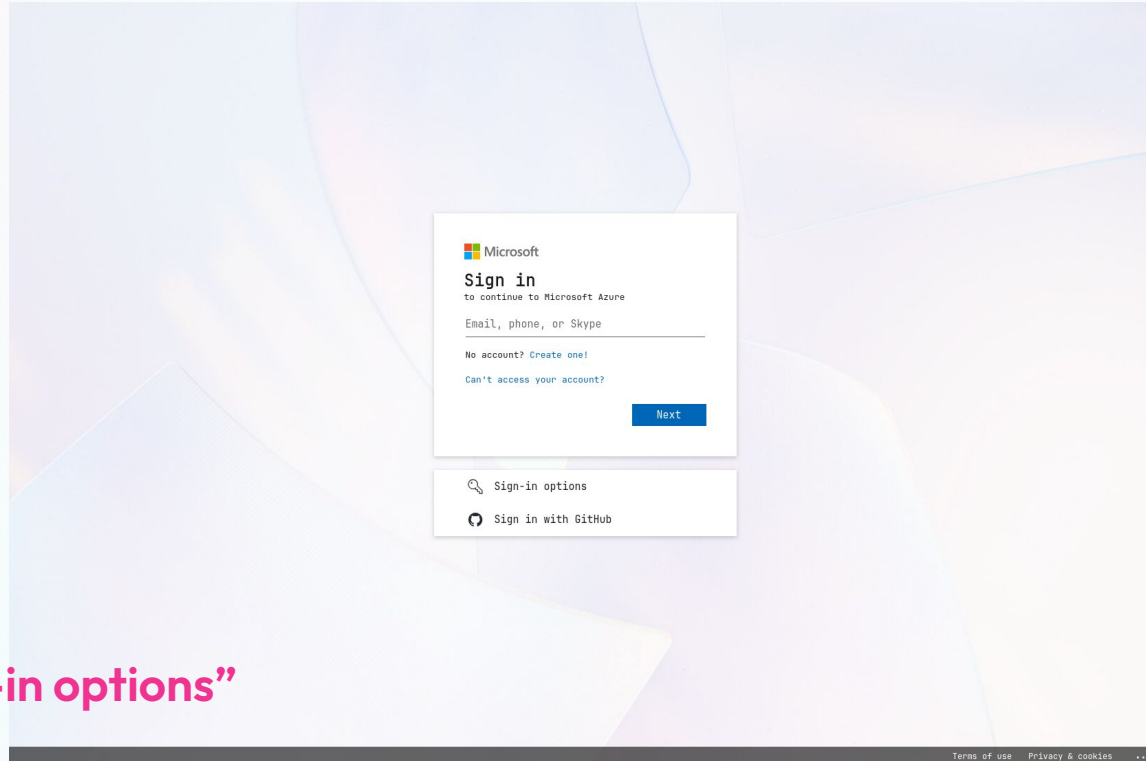


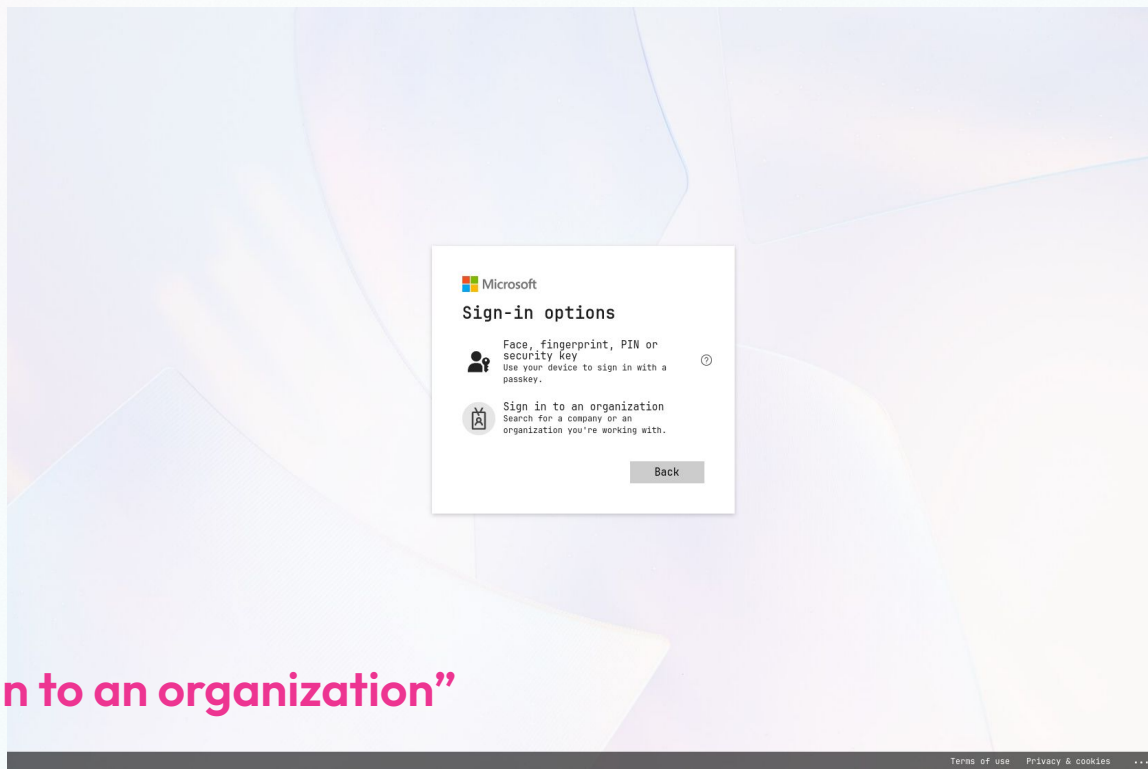
How to setup Azure Platform




Access website



Go to “Sign-in options”



Go to “Sign in to an organization”



The image shows a Microsoft login interface for organizations. It features a white central box on a background of soft, overlapping pastel shapes in shades of blue, purple, and yellow. The box contains the Microsoft logo, the heading 'Find your organization', and instructions to enter a domain name. Below the instructions is a text input field labeled 'Domain name' and two buttons: 'Back' and 'Next'. At the bottom of the screen, there is a dark grey footer bar with links for 'Terms of use', 'Privacy & cookies', and a three-dot menu icon.

Microsoft

Find your organization

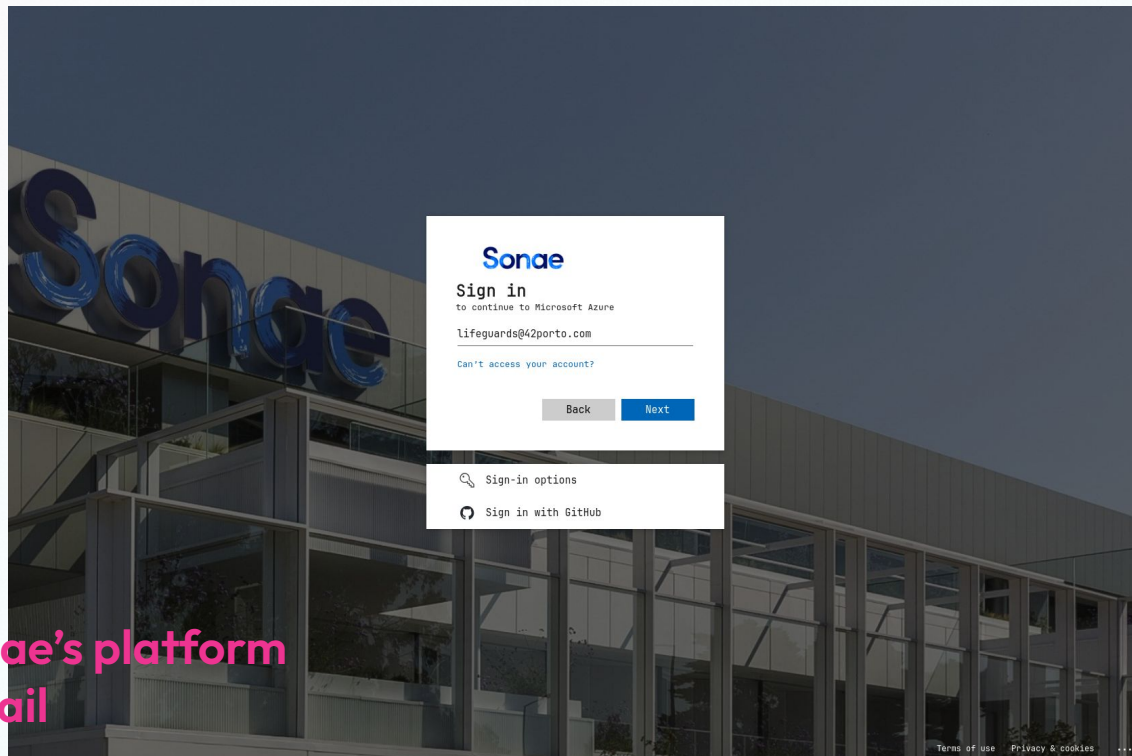
Enter the domain name of the organization you'd like to sign in to.

Domain name

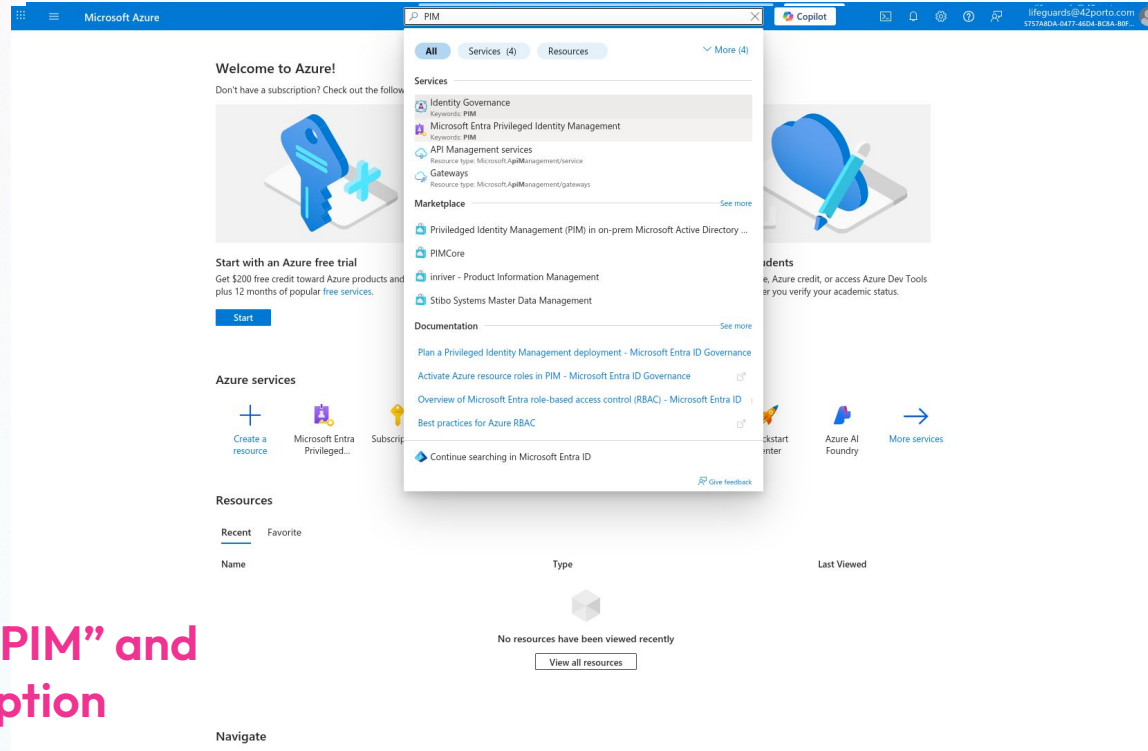
Back Next

Terms of use Privacy & cookies ...

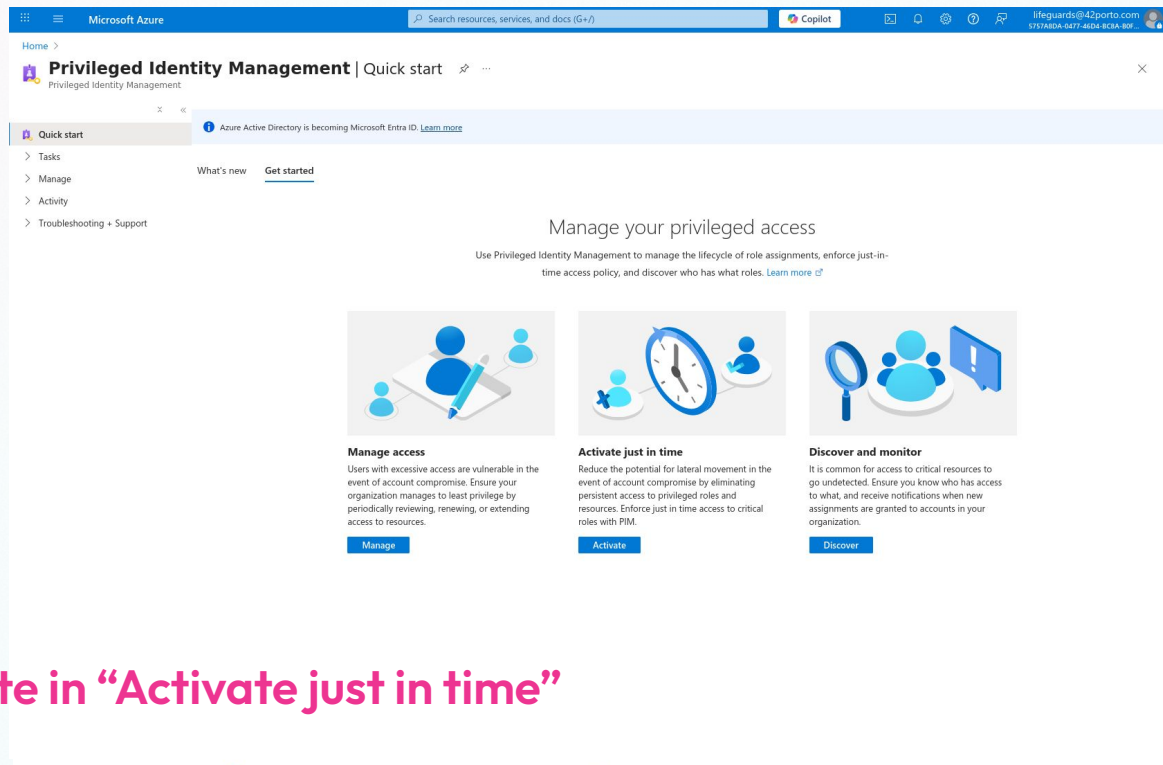
Input “SonaSystems.onmicrosoft.com”



**Sign in in Sonae's platform
with your email**



**Search for “PIM” and
select 2nd option**



Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Home >

Privileged Identity Management | Quick start

Privileged Identity Management

Quick start


Azure Active Directory is becoming Microsoft Entra ID. [Learn more](#)

- Tasks
- Manage
- Activity
- Troubleshooting + Support

What's new Get started

Manage your privileged access


Use Privileged Identity Management to manage the lifecycle of role assignments, enforce just-in-time access policy, and discover who has what roles. [Learn more](#)



Manage access

Users with excessive access are vulnerable in the event of account compromise. Ensure your organization manages to least privilege by periodically reviewing, renewing, or extending access to resources.


[Manage](#)



Activate just in time

Reduce the potential for lateral movement in the event of account compromise by eliminating persistent access to privileged roles and resources. Enforce just in time access to critical roles with PIM.

[Activate](#)

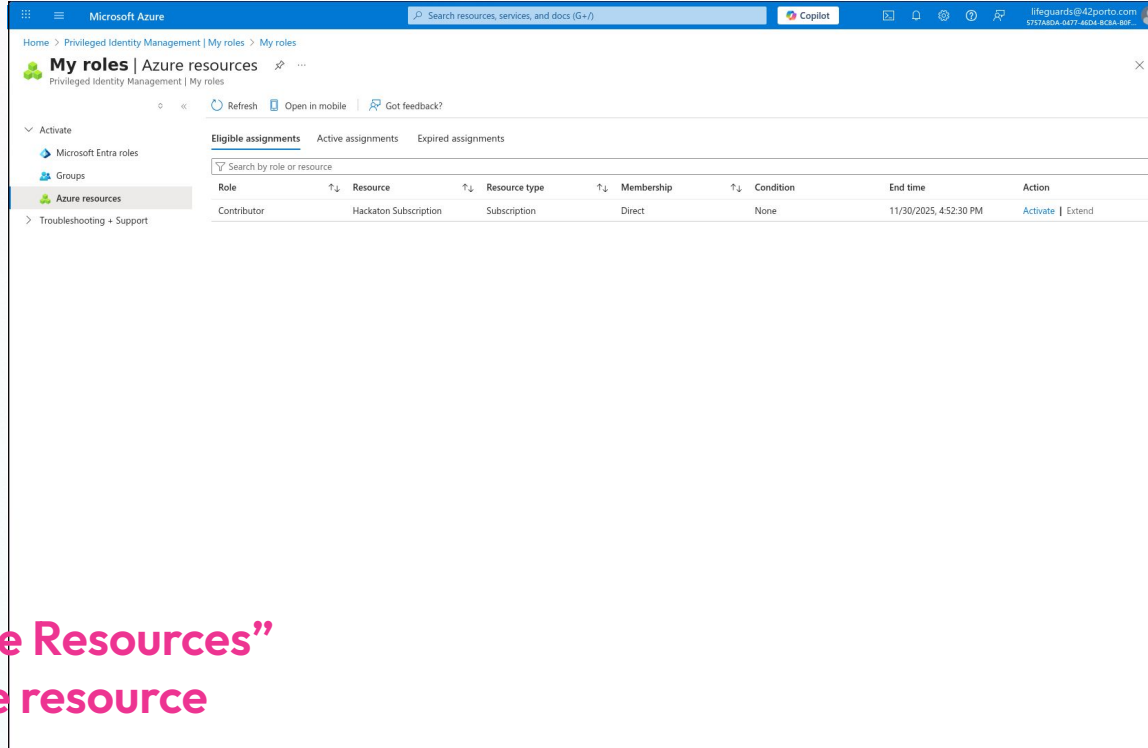


Discover and monitor

It is common for access to critical resources to go undetected. Ensure you know who has access to what, and receive notifications when new assignments are granted to accounts in your organization.

[Discover](#)

Click Activate in “Activate just in time”



Home > Privileged Identity Management | My roles > My roles

My roles | Azure resources

Privileged Identity Management | My roles

Refresh Open in mobile Got feedback?

Activate

- Microsoft Entra roles
- Groups
- Azure resources**

Troubleshooting + Support

Eligible assignments Active assignments Expired assignments

Search by role or resource

Role	Resource	Resource type	Membership	Condition	End time	Action
Contributor	Hackaton Subscription	Subscription	Direct	None	11/30/2025, 4:52:30 PM	Activate Extend

Select “Azure Resources”
and Activate resource

The screenshot shows the Microsoft Azure portal interface. On the left, the 'My roles' page is visible, showing a table of roles. The 'Activate' button is highlighted in the left sidebar. The main content area shows the 'Activate - Contributor' dialog box. The dialog box has tabs for 'Roles', 'Activate', 'Scope', and 'Status'. The 'Activate' tab is selected. It contains a checkbox for 'Custom activation start time', a 'Duration (hours)' slider set to 8, and a 'Reason (max 500 characters)' text area filled with 'Hackathon 42-Sonae'. At the bottom of the dialog box are 'Activate' and 'Cancel' buttons.

Role	Resource	Resource type	Membership
Contributor	Hackathon Subscription	Subscription	Direct

Fill Reason and Activate

Done and Good Luck!