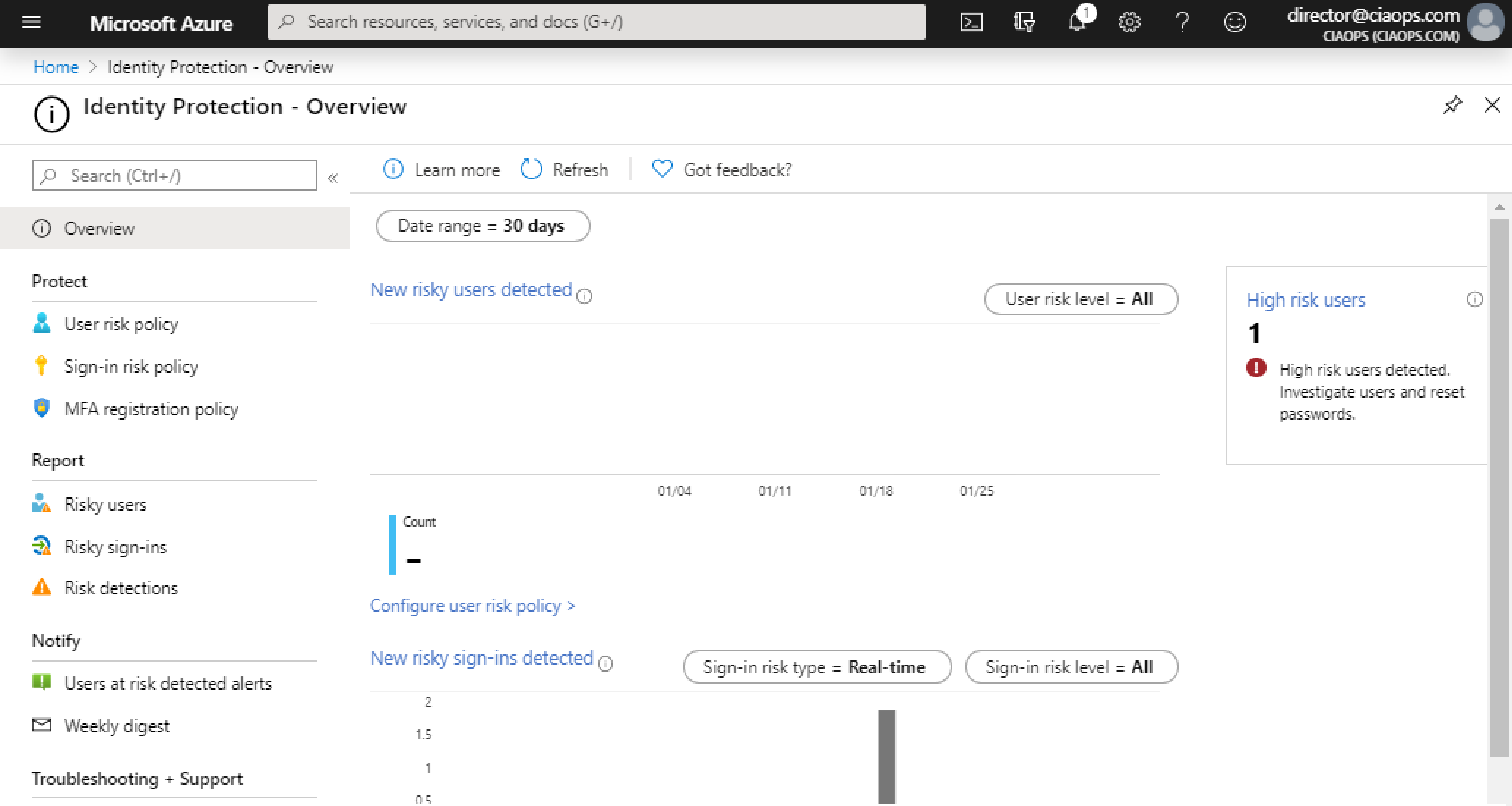


Microsoft Azure
Search resources, services, and docs (G+/)
1
director@ciaops.com
CIAOPS (CIAOPS.COM)
Home > Identity Protection - Overview

Identity Protection - Overview

Overview

Protect

- User risk policy
- Sign-in risk policy
- MFA registration policy

Report

- Risky users
- Risky sign-ins
- Risk detections

Notify

- Users at risk detected alerts
- Weekly digest

Troubleshooting + Support

Date range = **30 days**

New risky users detected

User risk level = **All**

Configure user risk policy >

New risky sign-ins detected

Sign-in risk type = **Real-time**

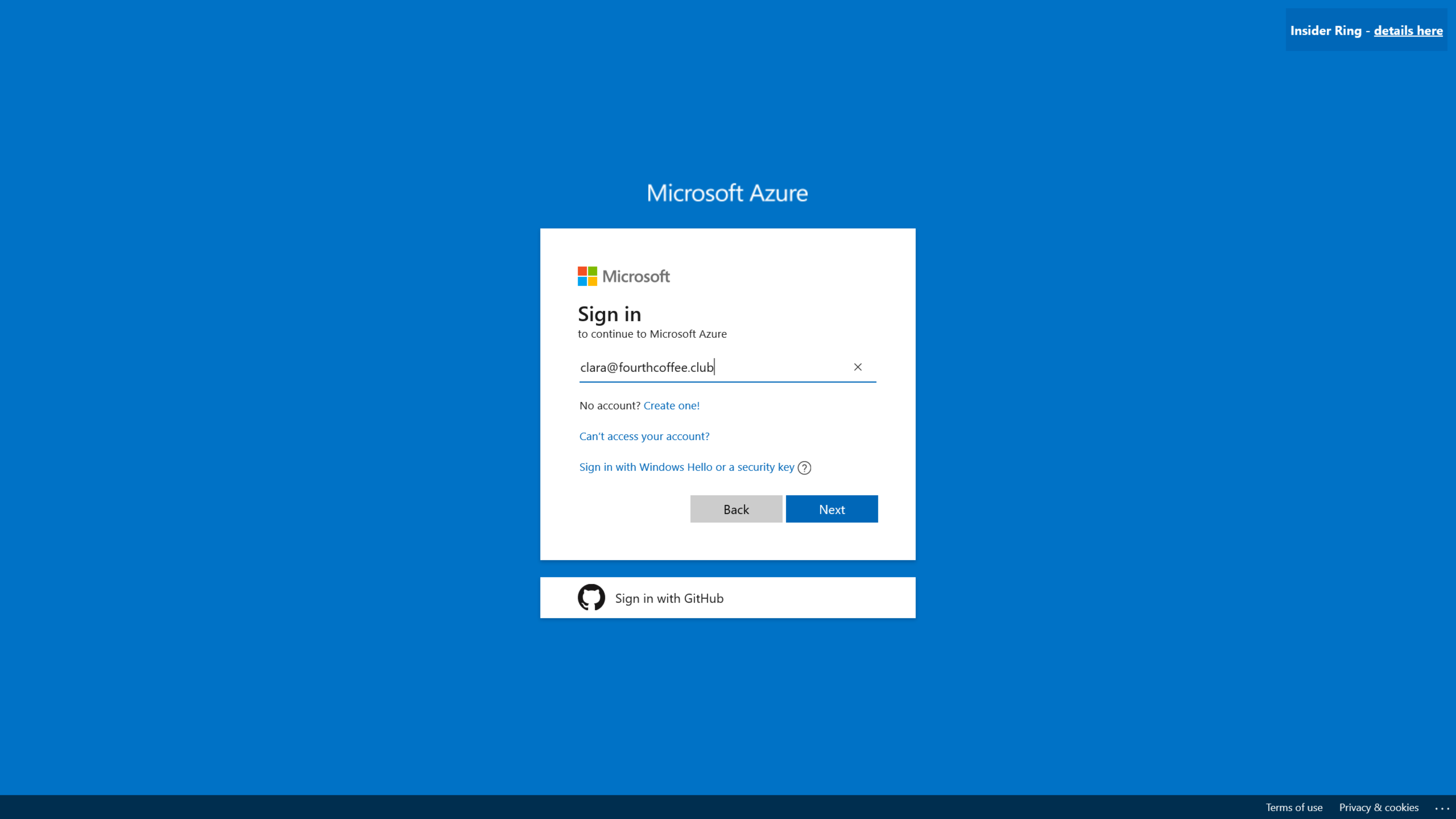
Sign-in risk level = **All**

High risk users

1

High risk users detected. Investigate users and reset passwords.

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection



Insider Ring - details here

Microsoft Azure

Microsoft

Sign in

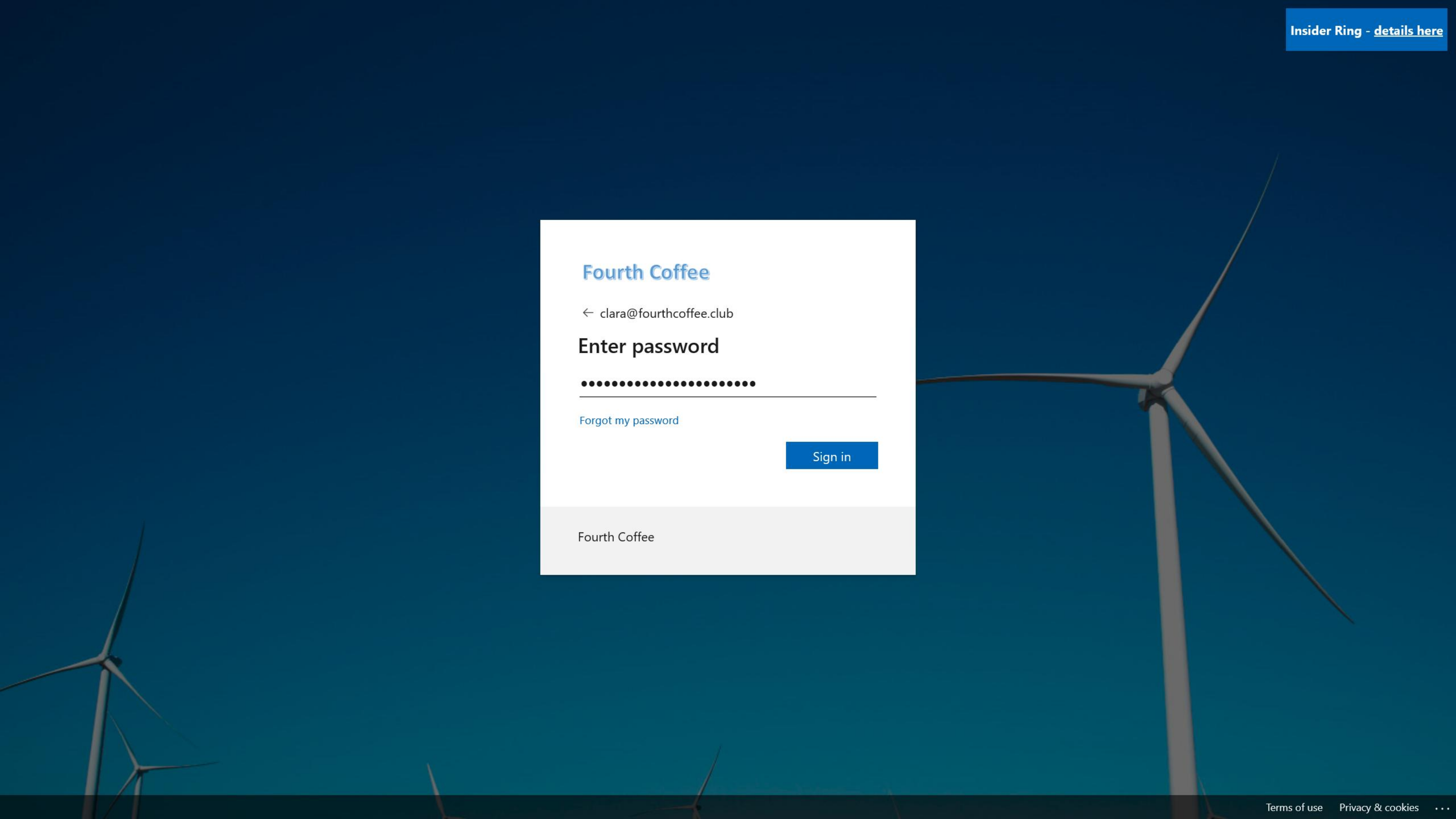
to continue to Microsoft Azure

clara@fourthcoffee.club

No account? Create one!

Can’t access your account?

Sign in with Windows Hello or a security key



Insider Ring - details here

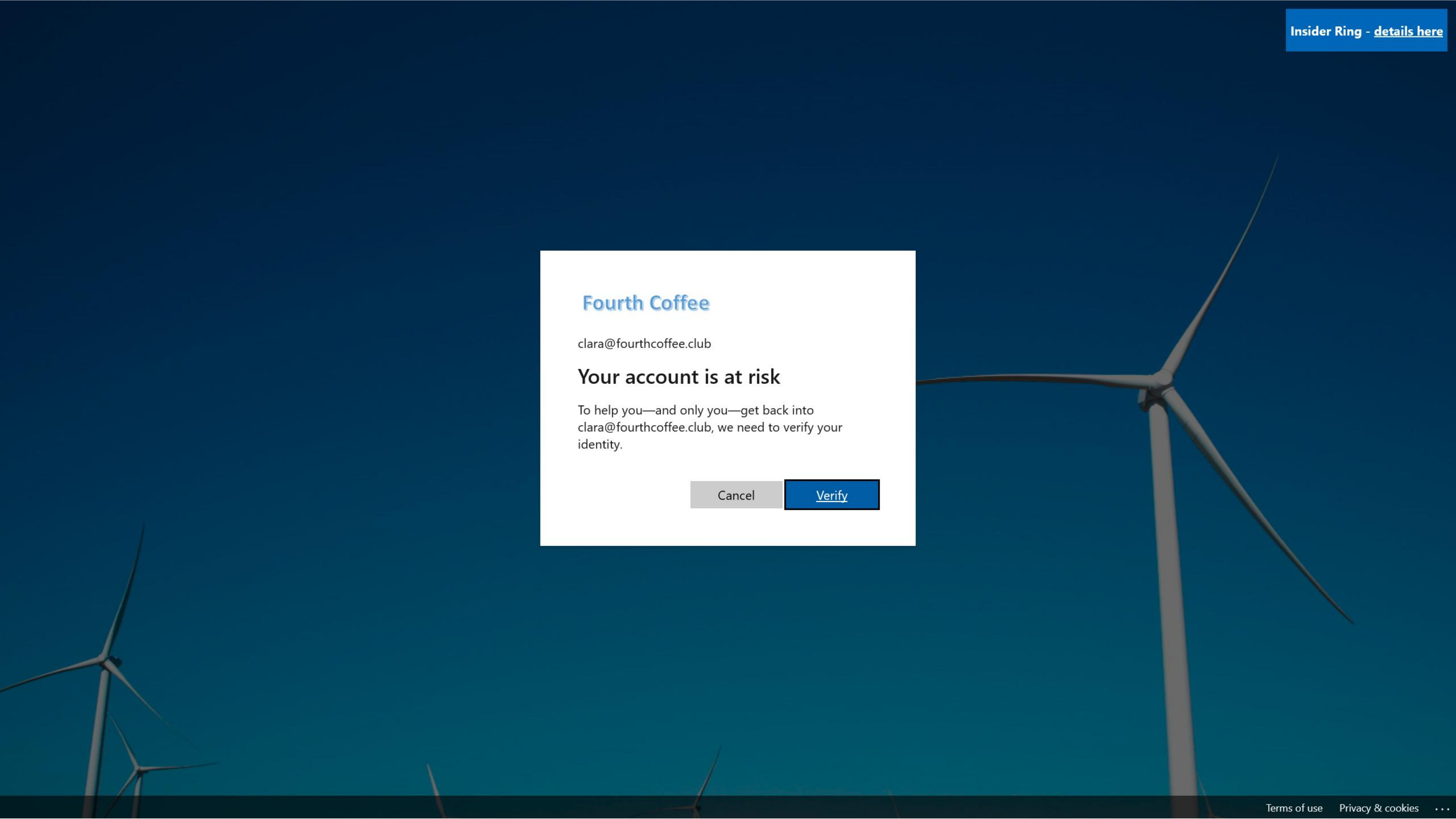
Fourth Coffee

← clara@fourthcoffee.club

Enter password

••••••••••••••••••••••

Fourth Coffee

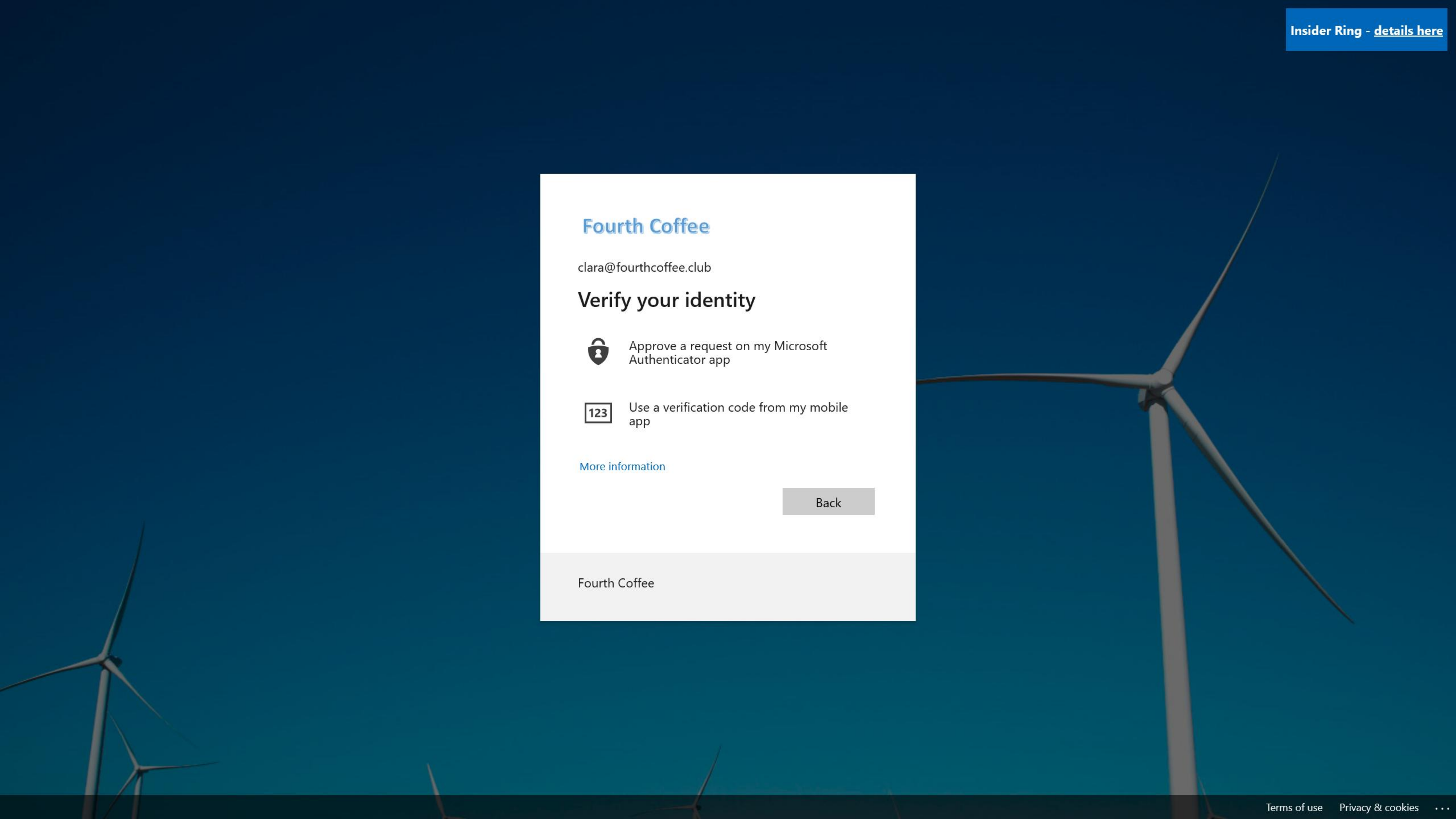


Fourth Coffee

clara@fourthcoffee.club

Your account is at risk

To help you—and only you—get back into clara@fourthcoffee.club, we need to verify your identity.



Insider Ring - details here

Fourth Coffee

clara@fourthcoffee.club

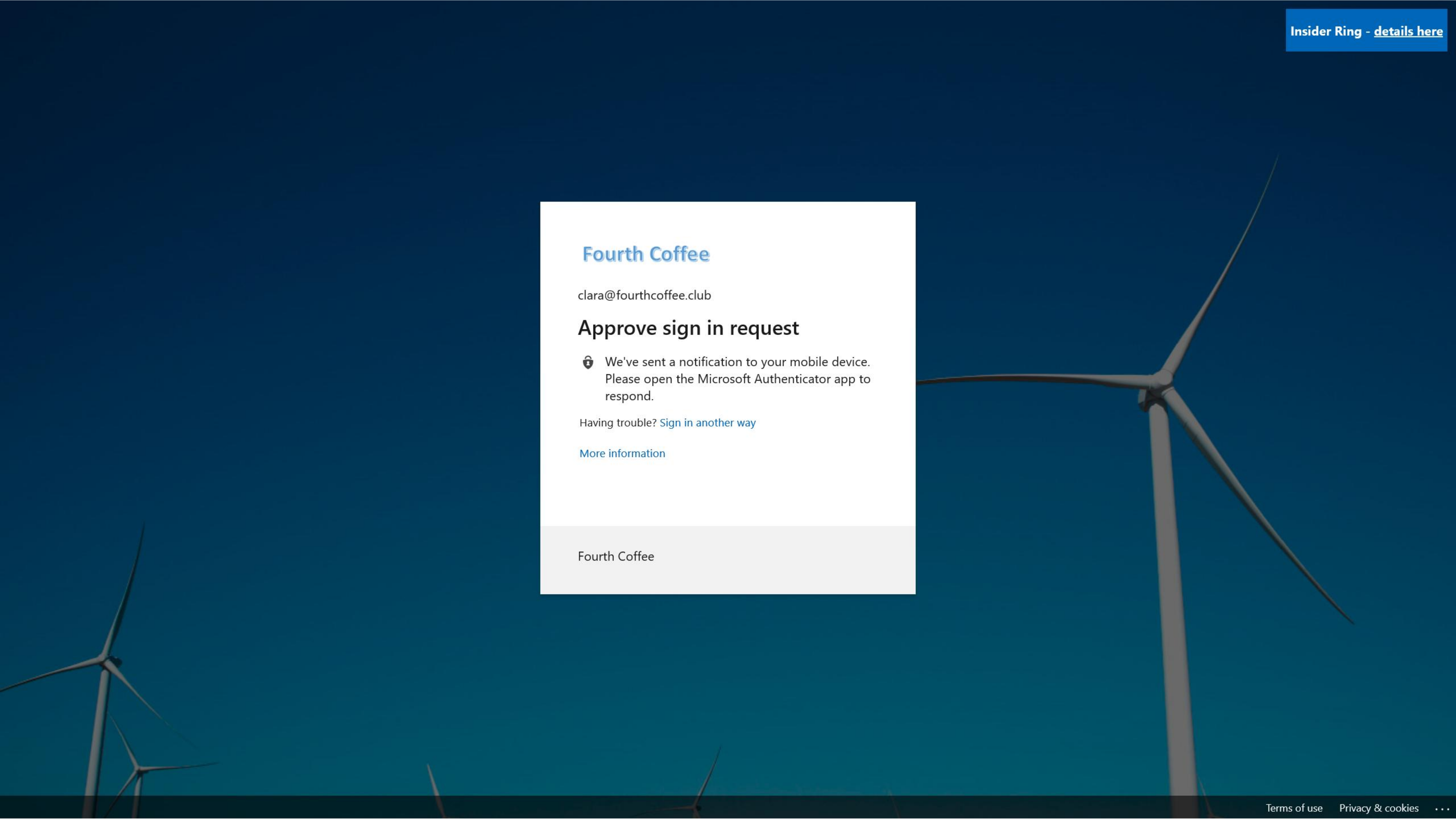
Verify your identity

Approve a request on my Microsoft Authenticator app

Use a verification code from my mobile app

More information

Fourth Coffee



Fourth Coffee

clara@fourthcoffee.club

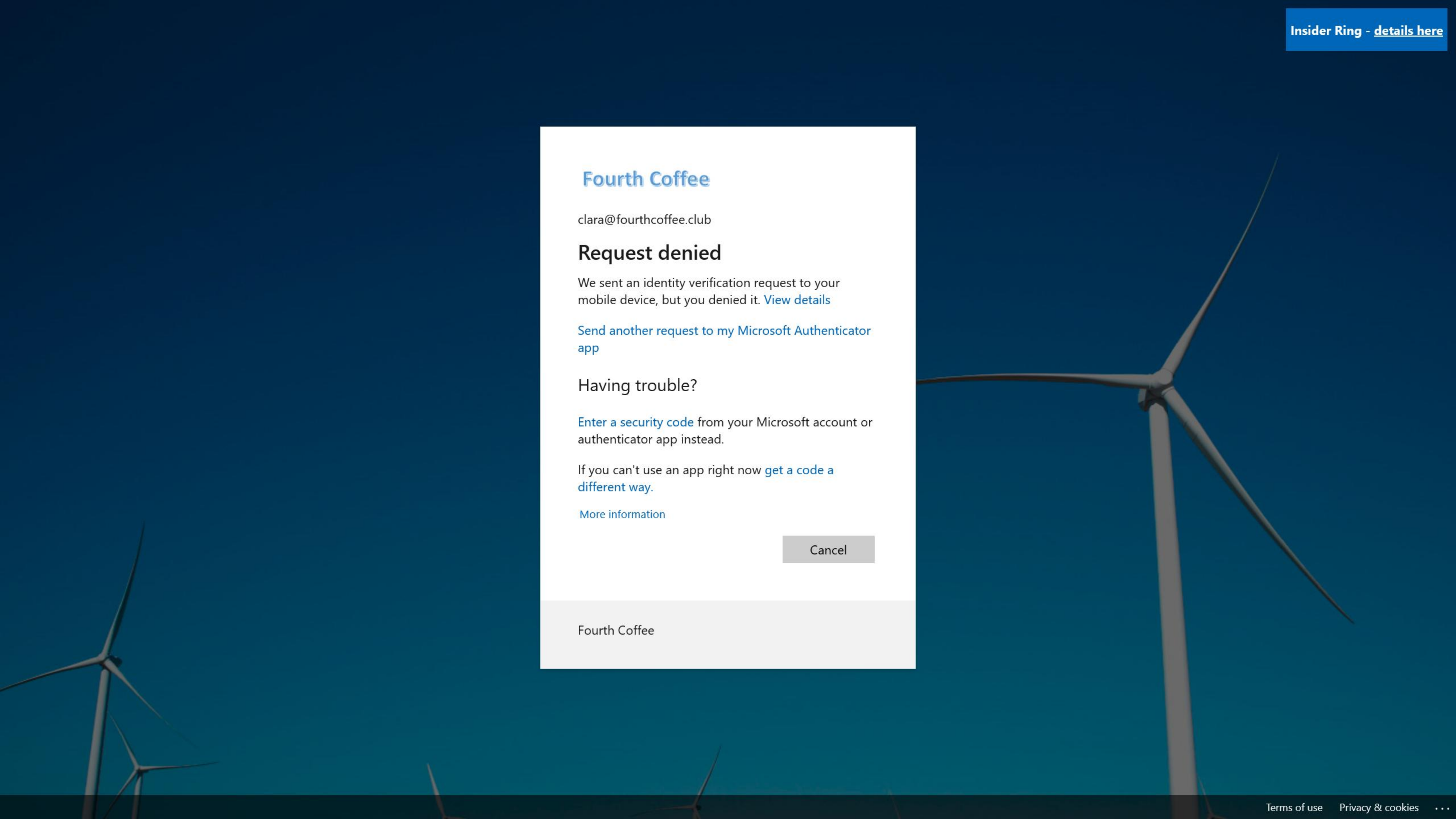
Approve sign in request

We've sent a notification to your mobile device. Please open the Microsoft Authenticator app to respond.

Having trouble? Sign in another way

More information

Fourth Coffee



Insider Ring - details here

Fourth Coffee

clara@fourthcoffee.club

Request denied

We sent an identity verification request to your mobile device, but you denied it. View details

Send another request to my Microsoft Authenticator app

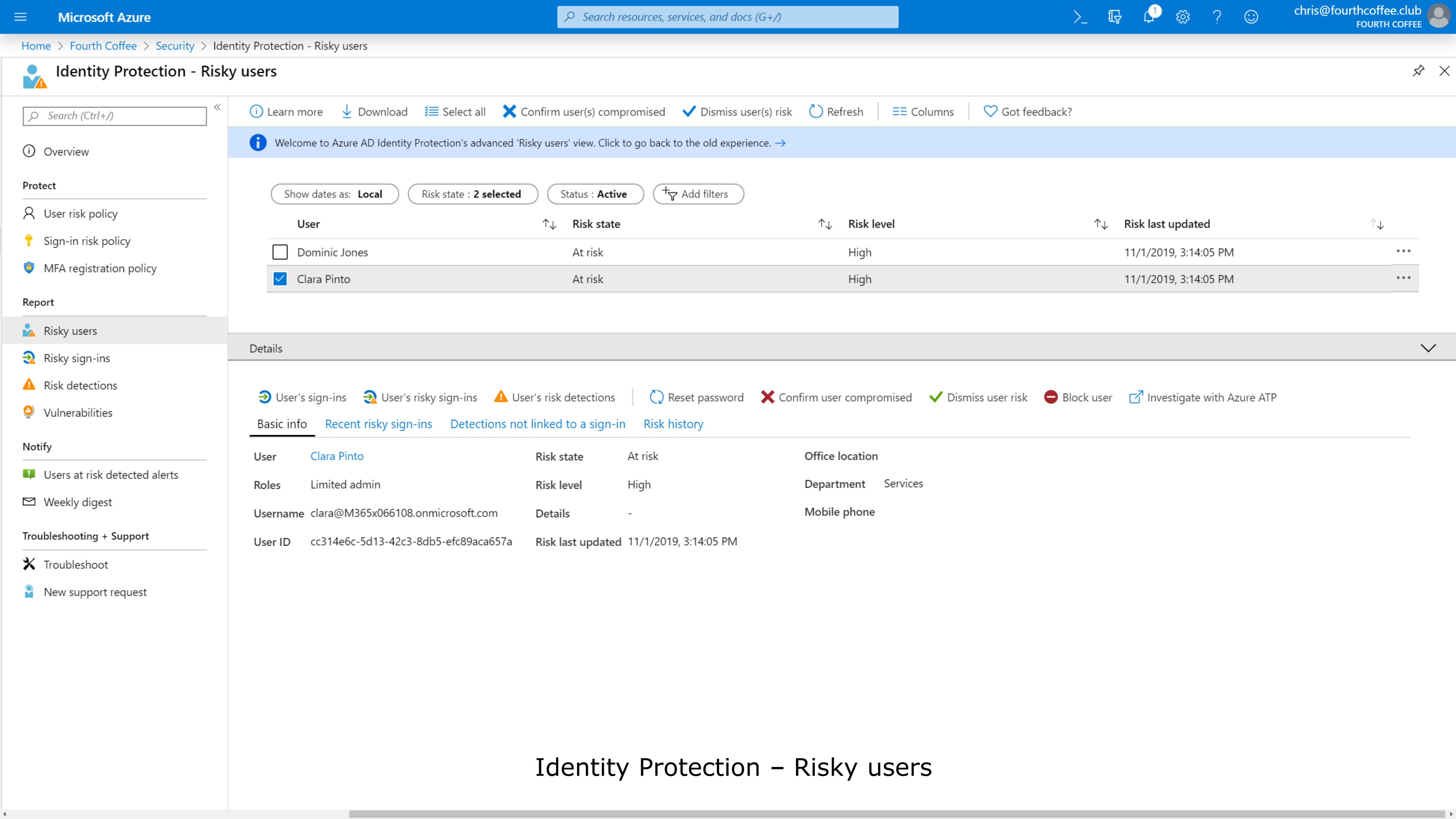
Having trouble?

Enter a security code from your Microsoft account or authenticator app instead.

If you can't use an app right now get a code a different way.

More information

Fourth Coffee



Microsoft Azure
Search resources, services, and docs (G+/)
chris@fourthcoffee.club
FOURTH COFFEE
Home > Fourth Coffee > Security > Identity Protection - Risky users

Identity Protection - Risky users

Welcome to Azure AD Identity Protection's advanced 'Risky users' view. Click to go back to the old experience. →

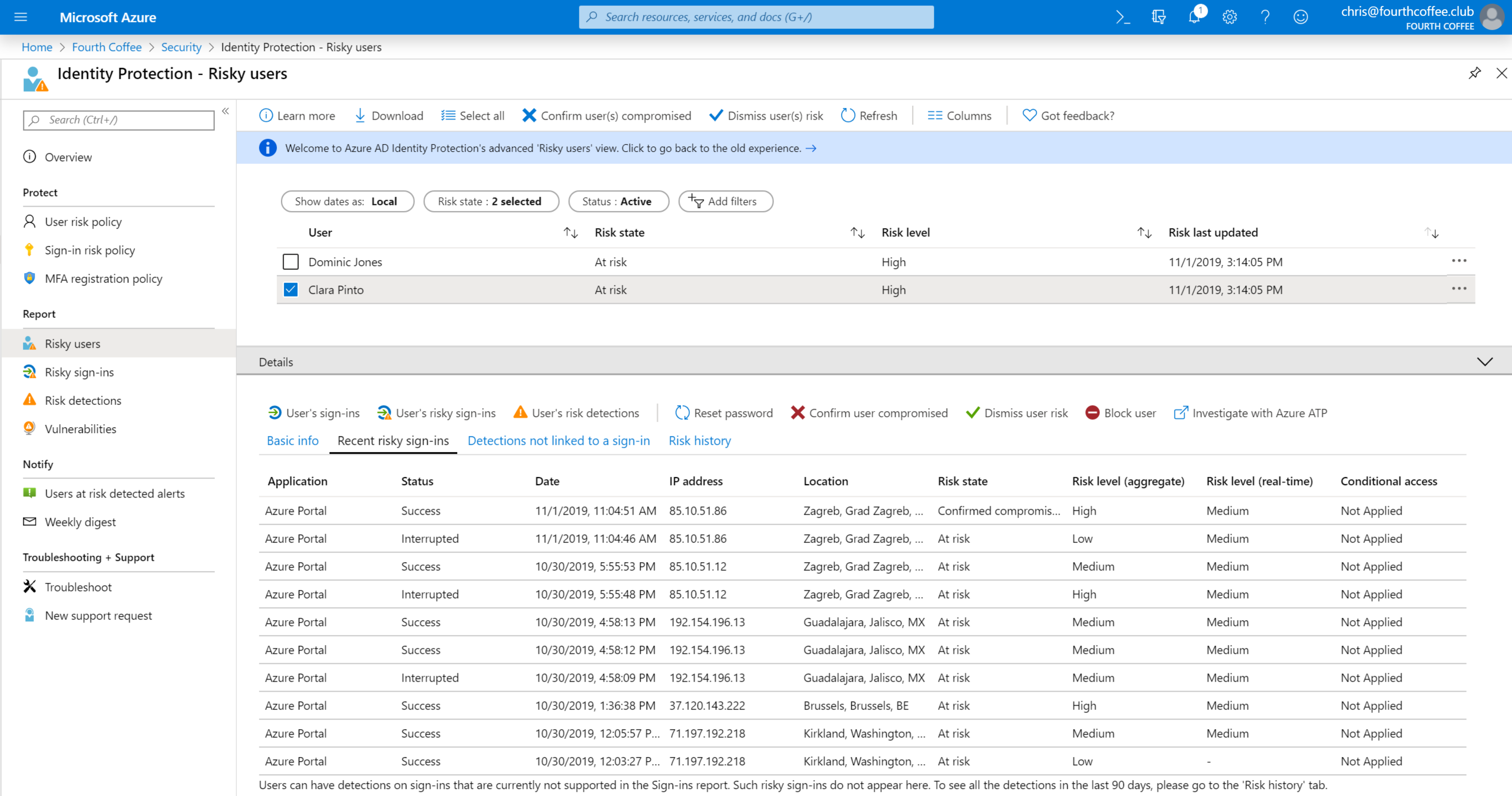
Show dates as: **Local** | Risk state : **2 selected** | Status : **Active** | Add filters

	User	Risk state	Risk level	Risk last updated
☐	Dominic Jones	At risk	High	11/1/2019, 3:14:05 PM
☑	Clara Pinto	At risk	High	11/1/2019, 3:14:05 PM

Details

User	Clara Pinto	Risk state	At risk	Office location	
Roles	Limited admin	Risk level	High	Department	Services
Username	clara@M365x066108.onmicrosoft.com	Details	-	Mobile phone	
User ID	cc314e6c-5d13-42c3-8db5-efc89aca657a	Risk last updated	11/1/2019, 3:14:05 PM		

Identity Protection – Risky users



Home > Fourth Coffee > Security > Identity Protection - Risky users

Identity Protection - Risky users

Welcome to Azure AD Identity Protection's advanced 'Risky users' view. Click to go back to the old experience. →

Show dates as: **Local** | Risk state : **2 selected** | Status : **Active** | Add filters

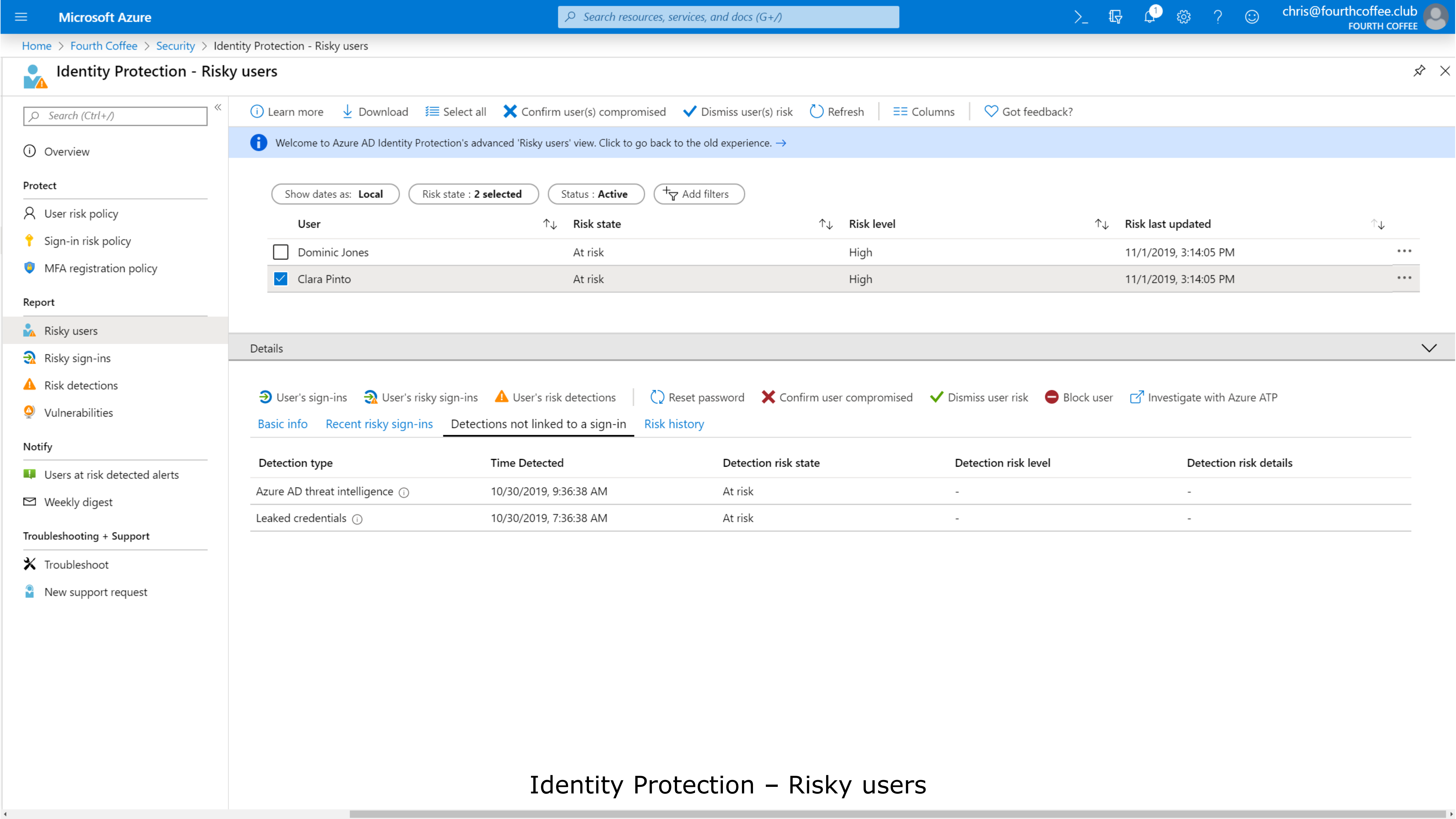
	User	Risk state	Risk level	Risk last updated
□	Dominic Jones	At risk	High	11/1/2019, 3:14:05 PM
☑	Clara Pinto	At risk	High	11/1/2019, 3:14:05 PM

Details

Application	Status	Date	IP address	Location	Risk state	Risk level (aggregate)	Risk level (real-time)	Conditional access
Azure Portal	Success	11/1/2019, 11:04:51 AM	85.10.51.86	Zagreb, Grad Zagreb, ...	Confirmed compromis...	High	Medium	Not Applied
Azure Portal	Interrupted	11/1/2019, 11:04:46 AM	85.10.51.86	Zagreb, Grad Zagreb, ...	At risk	Low	Medium	Not Applied
Azure Portal	Success	10/30/2019, 5:55:53 PM	85.10.51.12	Zagreb, Grad Zagreb, ...	At risk	Medium	Medium	Not Applied
Azure Portal	Interrupted	10/30/2019, 5:55:48 PM	85.10.51.12	Zagreb, Grad Zagreb, ...	At risk	High	Medium	Not Applied
Azure Portal	Success	10/30/2019, 4:58:13 PM	192.154.196.13	Guadalajara, Jalisco, MX	At risk	Medium	Medium	Not Applied
Azure Portal	Success	10/30/2019, 4:58:12 PM	192.154.196.13	Guadalajara, Jalisco, MX	At risk	Medium	Medium	Not Applied
Azure Portal	Interrupted	10/30/2019, 4:58:09 PM	192.154.196.13	Guadalajara, Jalisco, MX	At risk	Medium	Medium	Not Applied
Azure Portal	Success	10/30/2019, 1:36:38 PM	37.120.143.222	Brussels, Brussels, BE	At risk	High	Medium	Not Applied
Azure Portal	Success	10/30/2019, 12:05:57 P...	71.197.192.218	Kirkland, Washington, ...	At risk	Medium	Medium	Not Applied
Azure Portal	Success	10/30/2019, 12:03:27 P...	71.197.192.218	Kirkland, Washington, ...	At risk	Low	-	Not Applied

Users can have detections on sign-ins that are currently not supported in the Sign-ins report. Such risky sign-ins do not appear here. To see all the detections in the last 90 days, please go to the 'Risk history' tab.

Identity Protection – Risky users



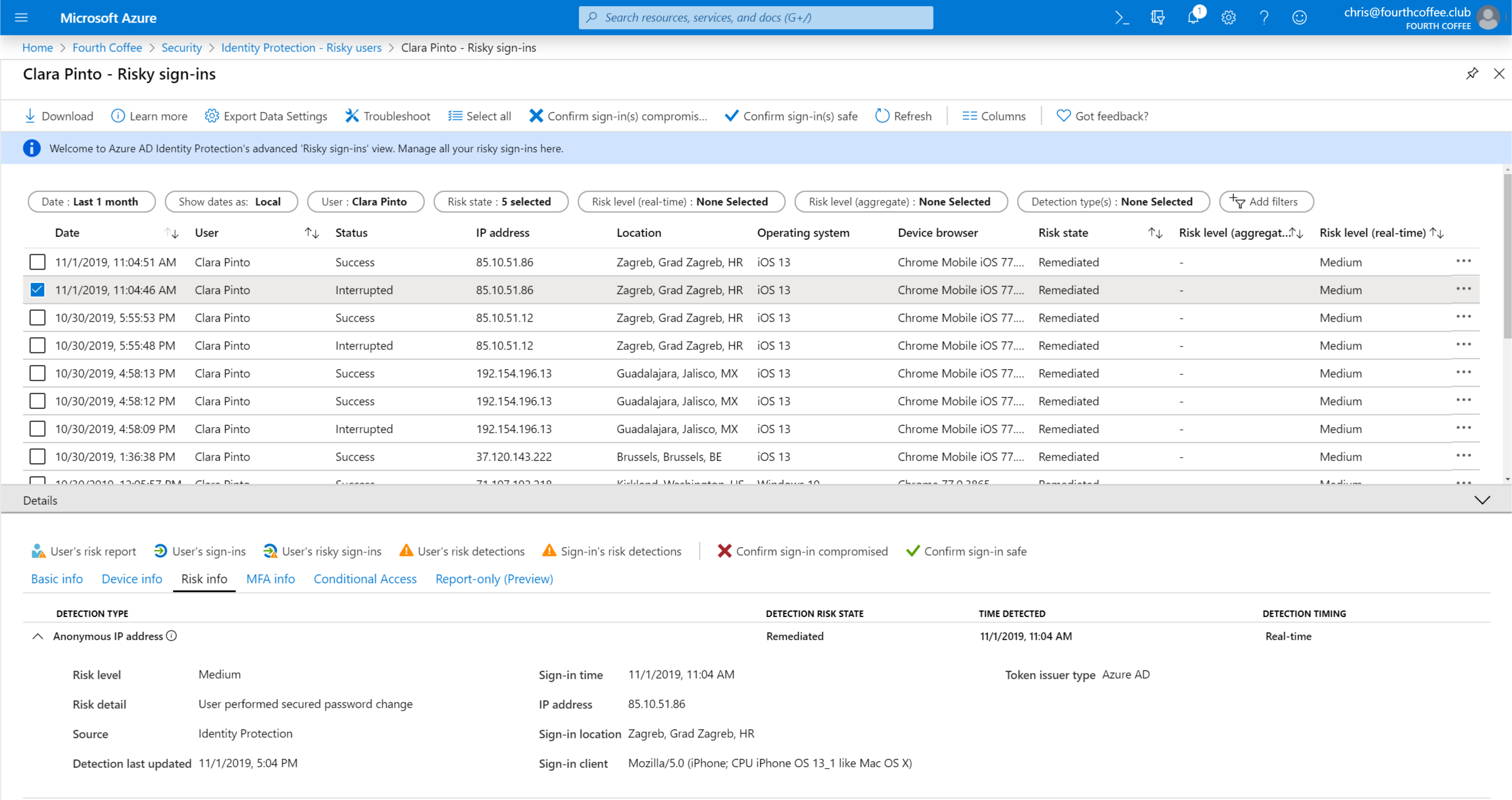
Welcome to Azure AD Identity Protection's advanced 'Risky users' view. Click to go back to the old experience. →

Show dates as: **Local** Risk state : **2 selected** Status : **Active**

	User	Risk state	Risk level	Risk last updated
□	Dominic Jones	At risk	High	11/1/2019, 3:14:05 PM
☑	Clara Pinto	At risk	High	11/1/2019, 3:14:05 PM

Detection type	Time Detected	Detection risk state	Detection risk level	Detection risk details
Azure AD threat intelligence ⓘ	10/30/2019, 9:36:38 AM	At risk	-	-
Leaked credentials ⓘ	10/30/2019, 7:36:38 AM	At risk	-	-

Identity Protection – Risky users


Microsoft Azure
Search resources, services, and docs (G+/)
chris@fourthcoffee.club
FOURTH COFFEE
Home > Fourth Coffee > Security > Identity Protection - Risky users > Clara Pinto - Risky sign-ins

Clara Pinto - Risky sign-ins

Download
Learn more
Export Data Settings
Troubleshoot
Select all
Confirm sign-in(s) compromis...
Confirm sign-in(s) safe
Refresh
Columns
Got feedback?

Welcome to Azure AD Identity Protection's advanced 'Risky sign-ins' view. Manage all your risky sign-ins here.

Date : **Last 1 month** | Show dates as: **Local** | User : **Clara Pinto** | Risk state : **5 selected** | Risk level (real-time) : **None Selected** | Risk level (aggregate) : **None Selected** | Detection type(s) : **None Selected** | Add filters

	Date	User	Status	IP address	Location	Operating system	Device browser	Risk state	Risk level (aggregat...	Risk level (real-time)
□	11/1/2019, 11:04:51 AM	Clara Pinto	Success	85.10.51.86	Zagreb, Grad Zagreb, HR	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
☑	11/1/2019, 11:04:46 AM	Clara Pinto	Interrupted	85.10.51.86	Zagreb, Grad Zagreb, HR	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
□	10/30/2019, 5:55:53 PM	Clara Pinto	Success	85.10.51.12	Zagreb, Grad Zagreb, HR	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
□	10/30/2019, 5:55:48 PM	Clara Pinto	Interrupted	85.10.51.12	Zagreb, Grad Zagreb, HR	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
□	10/30/2019, 4:58:13 PM	Clara Pinto	Success	192.154.196.13	Guadalajara, Jalisco, MX	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
□	10/30/2019, 4:58:12 PM	Clara Pinto	Success	192.154.196.13	Guadalajara, Jalisco, MX	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
□	10/30/2019, 4:58:09 PM	Clara Pinto	Interrupted	192.154.196.13	Guadalajara, Jalisco, MX	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
□	10/30/2019, 1:36:38 PM	Clara Pinto	Success	37.120.143.222	Brussels, Brussels, BE	iOS 13	Chrome Mobile iOS 77....	Remediated	-	Medium
□	10/30/2019, 12:05:57 PM	Clara Pinto	Success	71.197.193.218	Kirkland, Washington, US	Windows 10	Chrome 77.0.3865	Remediated		Medium

Details

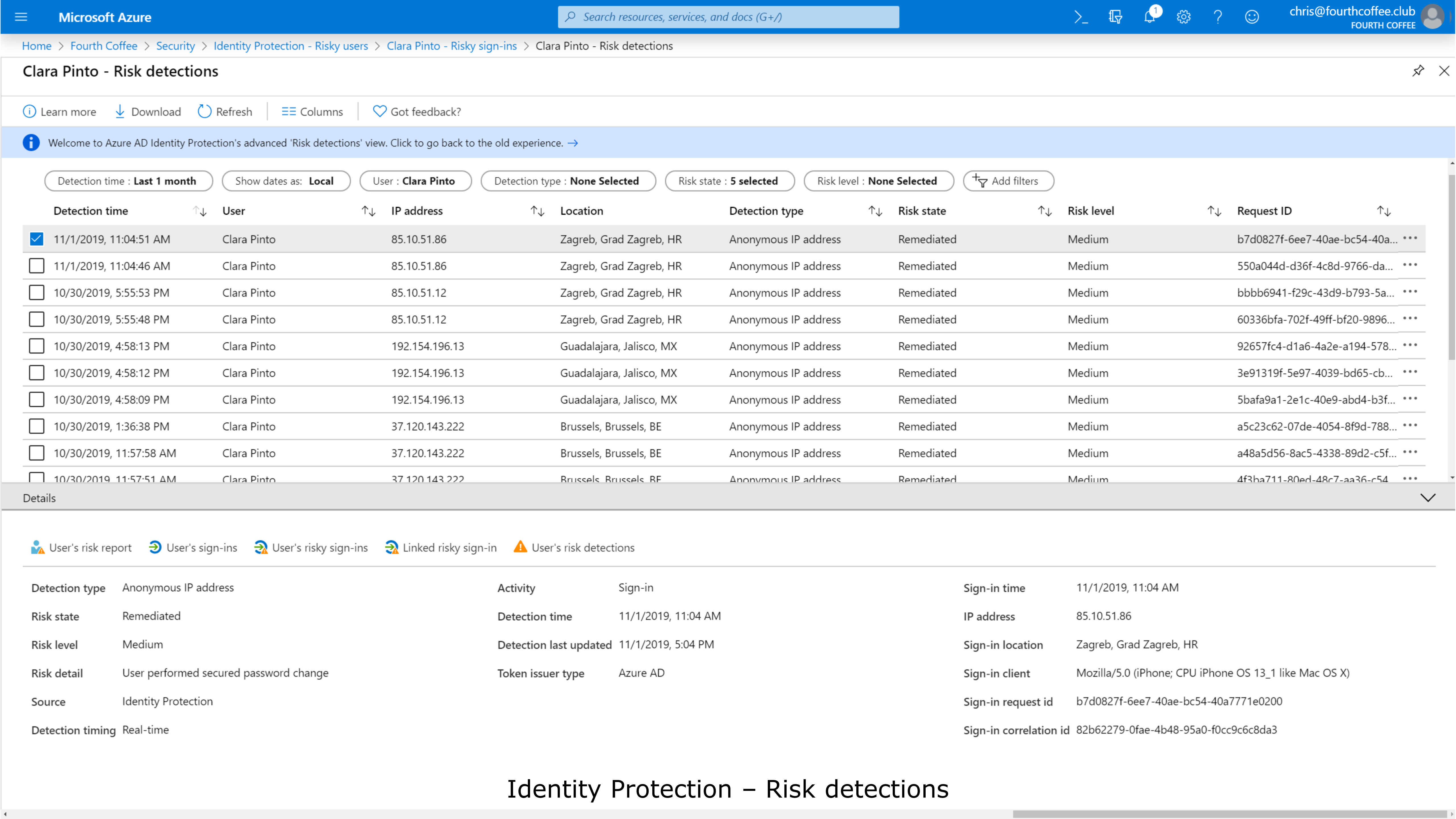
DETECTION TYPE	DETECTION RISK STATE	TIME DETECTED	DETECTION TIMING
Anonymous IP address	Remediated	11/1/2019, 11:04 AM	Real-time

Risk level: Medium
Risk detail: User performed secured password change
Source: Identity Protection
Detection last updated: 11/1/2019, 5:04 PM

Sign-in time: 11/1/2019, 11:04 AM
IP address: 85.10.51.86
Sign-in location: Zagreb, Grad Zagreb, HR
Sign-in client: Mozilla/5.0 (iPhone; CPU iPhone OS 13_1 like Mac OS X)

Token issuer type: Azure AD

Identity Protection – Risky sign-ins


Microsoft Azure
Search resources, services, and docs (G+/)
chris@fourthcoffee.club
FOURTH COFFEE
Home > Fourth Coffee > Security > Identity Protection - Risky users > Clara Pinto - Risky sign-ins > Clara Pinto - Risk detections

Clara Pinto - Risk detections

Learn more
Download
Refresh
Columns
Got feedback?

Welcome to Azure AD Identity Protection's advanced 'Risk detections' view. Click to go back to the old experience. →

Detection time : **Last 1 month** | Show dates as: **Local** | User : **Clara Pinto** | Detection type : **None Selected** | Risk state : **5 selected** | Risk level : **None Selected** | Add filters

	Detection time	User	IP address	Location	Detection type	Risk state	Risk level	Request ID	
☑	11/1/2019, 11:04:51 AM	Clara Pinto	85.10.51.86	Zagreb, Grad Zagreb, HR	Anonymous IP address	Remediated	Medium	b7d0827f-6ee7-40ae-bc54-40a...	•••
□	11/1/2019, 11:04:46 AM	Clara Pinto	85.10.51.86	Zagreb, Grad Zagreb, HR	Anonymous IP address	Remediated	Medium	550a044d-d36f-4c8d-9766-da...	•••
□	10/30/2019, 5:55:53 PM	Clara Pinto	85.10.51.12	Zagreb, Grad Zagreb, HR	Anonymous IP address	Remediated	Medium	bbbb6941-f29c-43d9-b793-5a...	•••
□	10/30/2019, 5:55:48 PM	Clara Pinto	85.10.51.12	Zagreb, Grad Zagreb, HR	Anonymous IP address	Remediated	Medium	60336bfa-702f-49ff-bf20-9896...	•••
□	10/30/2019, 4:58:13 PM	Clara Pinto	192.154.196.13	Guadalajara, Jalisco, MX	Anonymous IP address	Remediated	Medium	92657fc4-d1a6-4a2e-a194-578...	•••
□	10/30/2019, 4:58:12 PM	Clara Pinto	192.154.196.13	Guadalajara, Jalisco, MX	Anonymous IP address	Remediated	Medium	3e91319f-5e97-4039-bd65-cb...	•••
□	10/30/2019, 4:58:09 PM	Clara Pinto	192.154.196.13	Guadalajara, Jalisco, MX	Anonymous IP address	Remediated	Medium	5bafa9a1-2e1c-40e9-abd4-b3f...	•••
□	10/30/2019, 1:36:38 PM	Clara Pinto	37.120.143.222	Brussels, Brussels, BE	Anonymous IP address	Remediated	Medium	a5c23c62-07de-4054-8f9d-788...	•••
□	10/30/2019, 11:57:58 AM	Clara Pinto	37.120.143.222	Brussels, Brussels, BE	Anonymous IP address	Remediated	Medium	a48a5d56-8ac5-4338-89d2-c5f...	•••
□	10/30/2019, 11:57:51 AM	Clara Pinto	37.120.143.222	Brussels, Brussels, BE	Anonymous IP address	Remediated	Medium	4f3ba711-80ed-48c7-aa36-c54	•••

Details

Detection type	Anonymous IP address	**Activity**	Sign-in	**Sign-in time**	11/1/2019, 11:04 AM
Risk state	Remediated	**Detection time**	11/1/2019, 11:04 AM	**IP address**	85.10.51.86
Risk level	Medium	**Detection last updated**	11/1/2019, 5:04 PM	**Sign-in location**	Zagreb, Grad Zagreb, HR
Risk detail	User performed secured password change	**Token issuer type**	Azure AD	**Sign-in client**	Mozilla/5.0 (iPhone; CPU iPhone OS 13_1 like Mac OS X)
Source	Identity Protection			**Sign-in request id**	b7d0827f-6ee7-40ae-bc54-40a7771e0200
Detection timing	Real-time			**Sign-in correlation id**	82b62279-0fae-4b48-95a0-f0cc9c6c8da3

Identity Protection – Risk detections

Privileged Identity Management

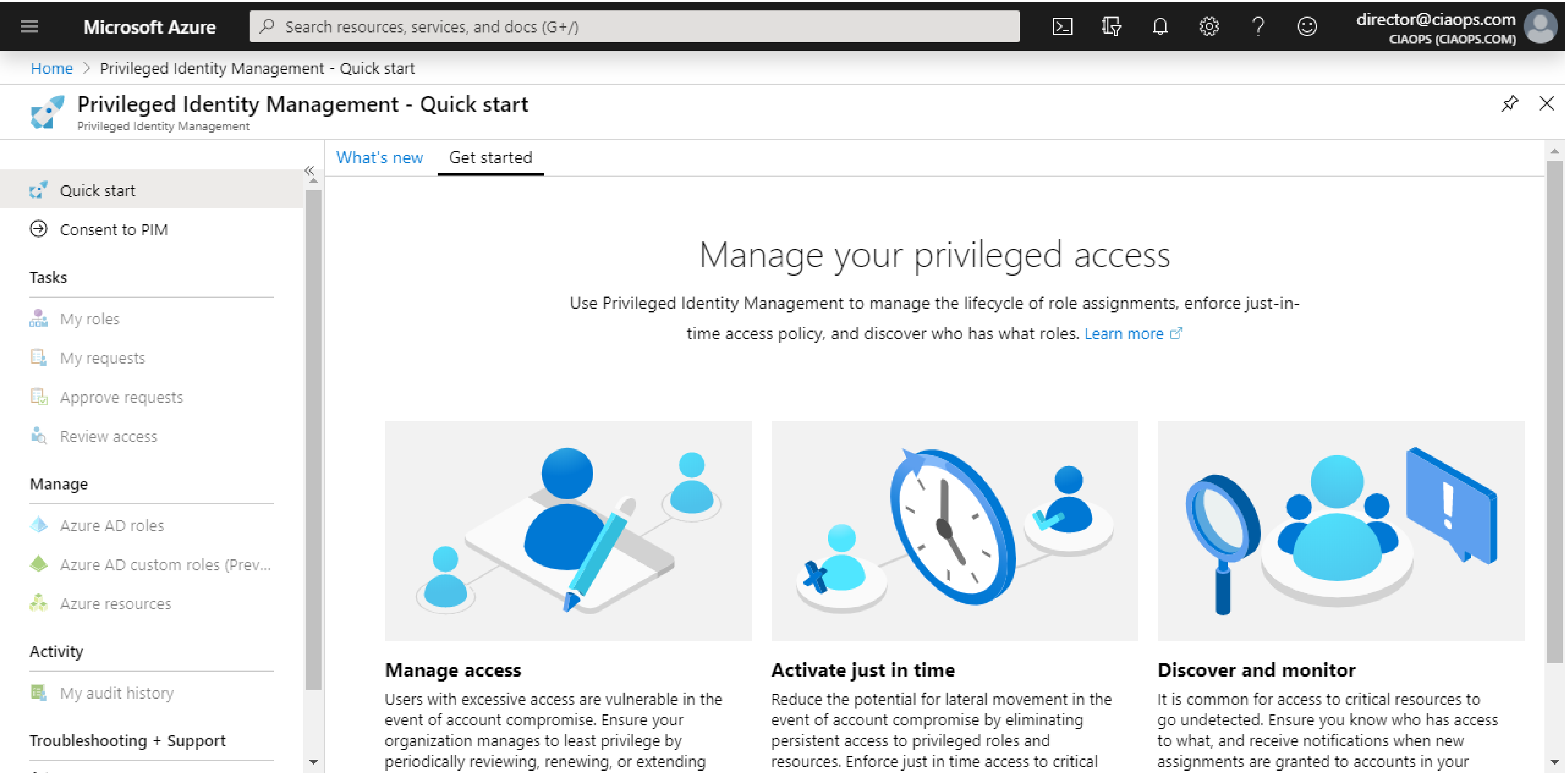
Privileged role membership only granted for a limited amount of time

Roles can be configured to require staff to perform MFA prior to elevation of privilege

Roles can be granted automatically or after review by one or more approvers

All role requests for and role approvals are automatically recorded in logs or by email

Almost all roles should be managed by PIM, with a “break glass” permanent account for critical roles just in case


Microsoft Azure
Search resources, services, and docs (G+/)
director@ciaops.com
CIAOPS (CIAOPS.COM)
Home > Privileged Identity Management - Quick start
Privileged Identity Management - Quick start
Privileged Identity Management
Quick start
Consent to PIM
Tasks
My roles
My requests
Approve requests
Review access
Manage
Azure AD roles
Azure AD custom roles (Prev...
Azure resources
Activity
My audit history
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

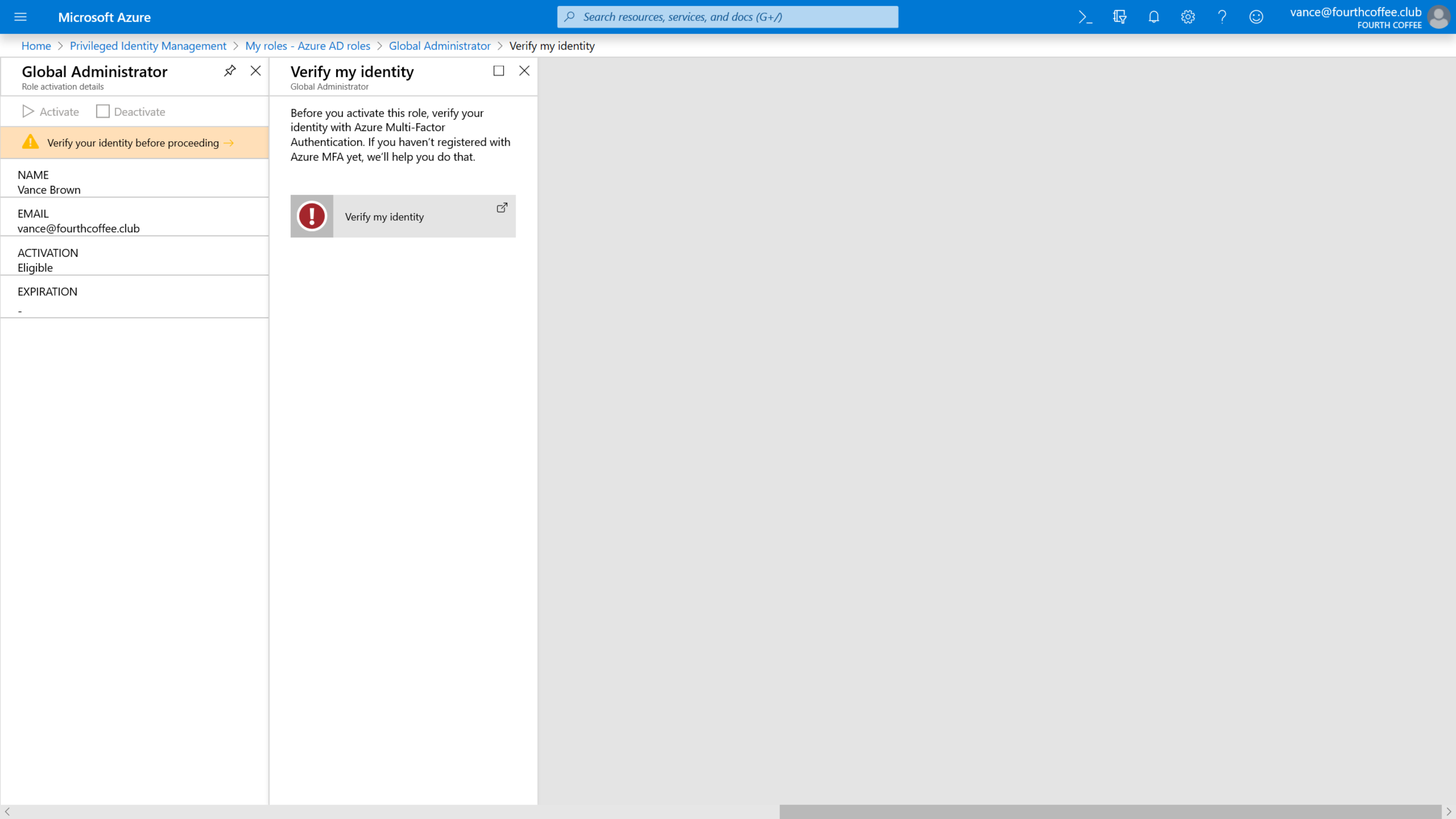
Activate just in time

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

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

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure


Microsoft Azure
Search resources, services, and docs (G+/)
vance@fourthcoffee.club
FOURTH COFFEE
Home > Privileged Identity Management > My roles - Azure AD roles > Global Administrator > Verify my identity

Global Administrator

Role activation details

⚠ Verify your identity before proceeding →

NAME
Vance Brown

EMAIL
vance@fourthcoffee.club

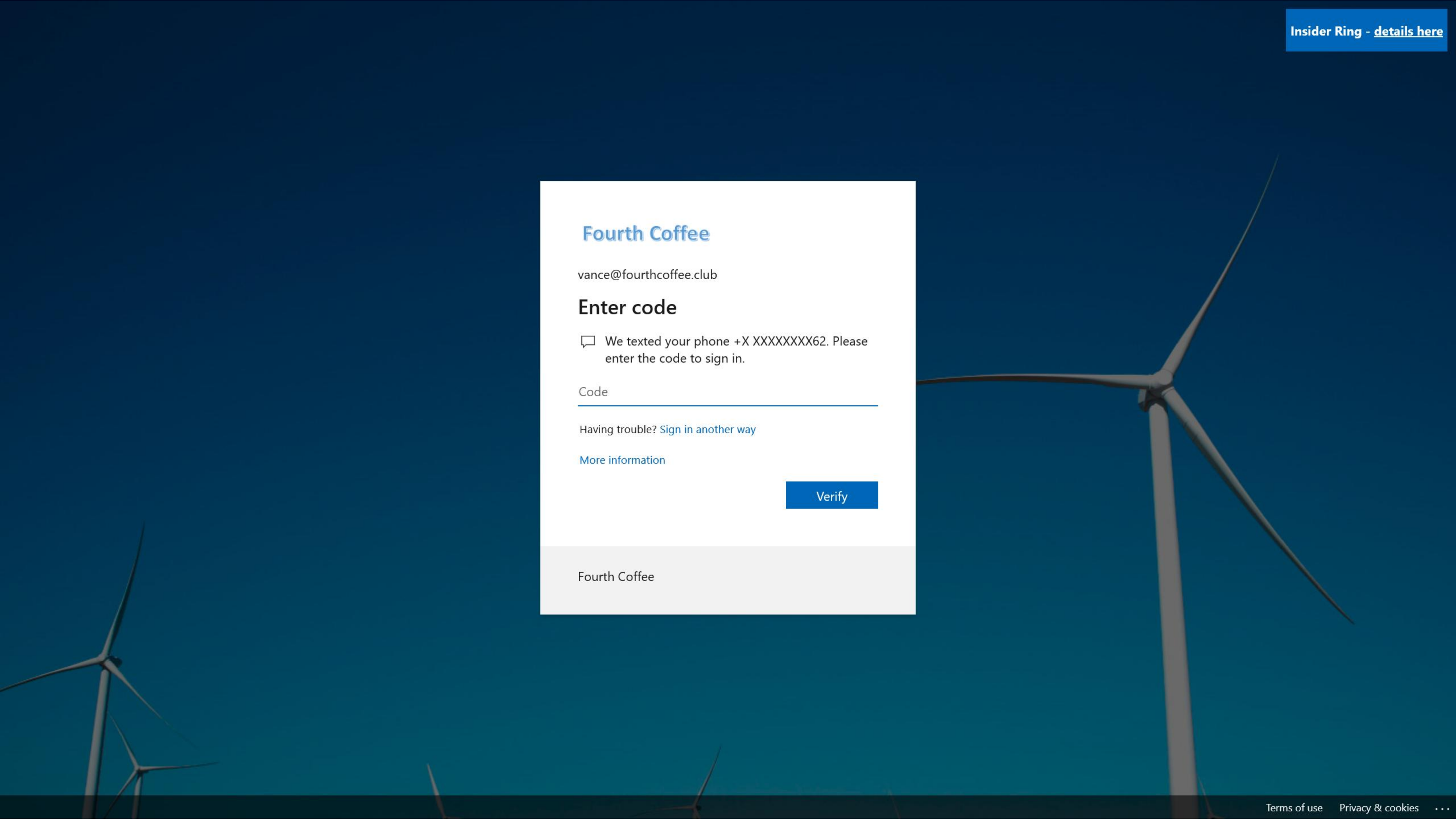
ACTIVATION
Eligible

EXPIRATION
-

Verify my identity

Global Administrator

Before you activate this role, verify your identity with Azure Multi-Factor Authentication. If you haven't registered with Azure MFA yet, we'll help you do that.



Fourth Coffee

vance@fourthcoffee.club

Enter code

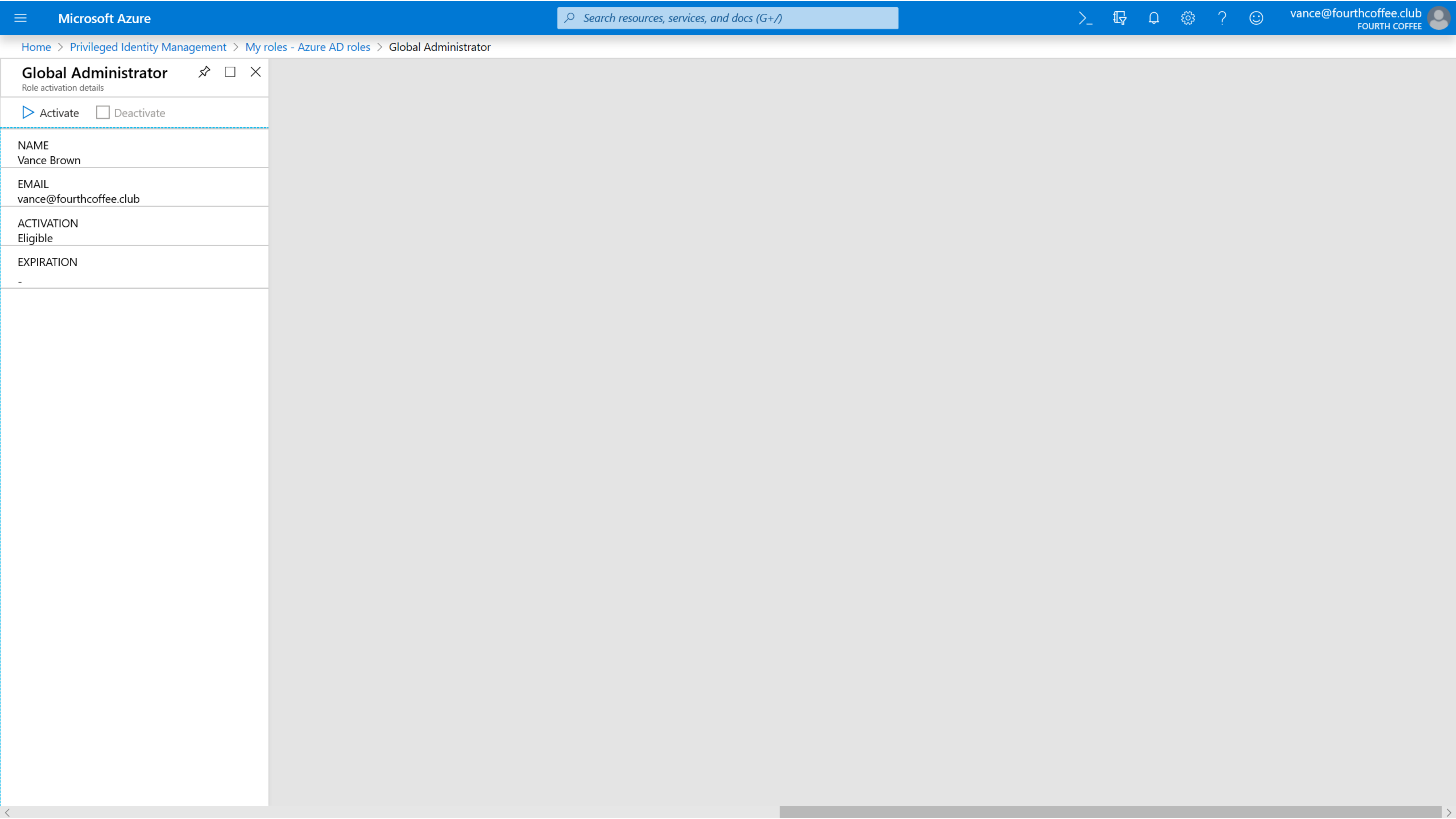
We texted your phone +X XXXXXXXX62. Please enter the code to sign in.

Code

Having trouble? Sign in another way

More information

Fourth Coffee



Microsoft Azure
Search resources, services, and docs (G+/)
vance@fourthcoffee.club
FOURTH COFFEE
Home > Privileged Identity Management > My roles - Azure AD roles > Global Administrator
Activate
Deactivate

Global Administrator

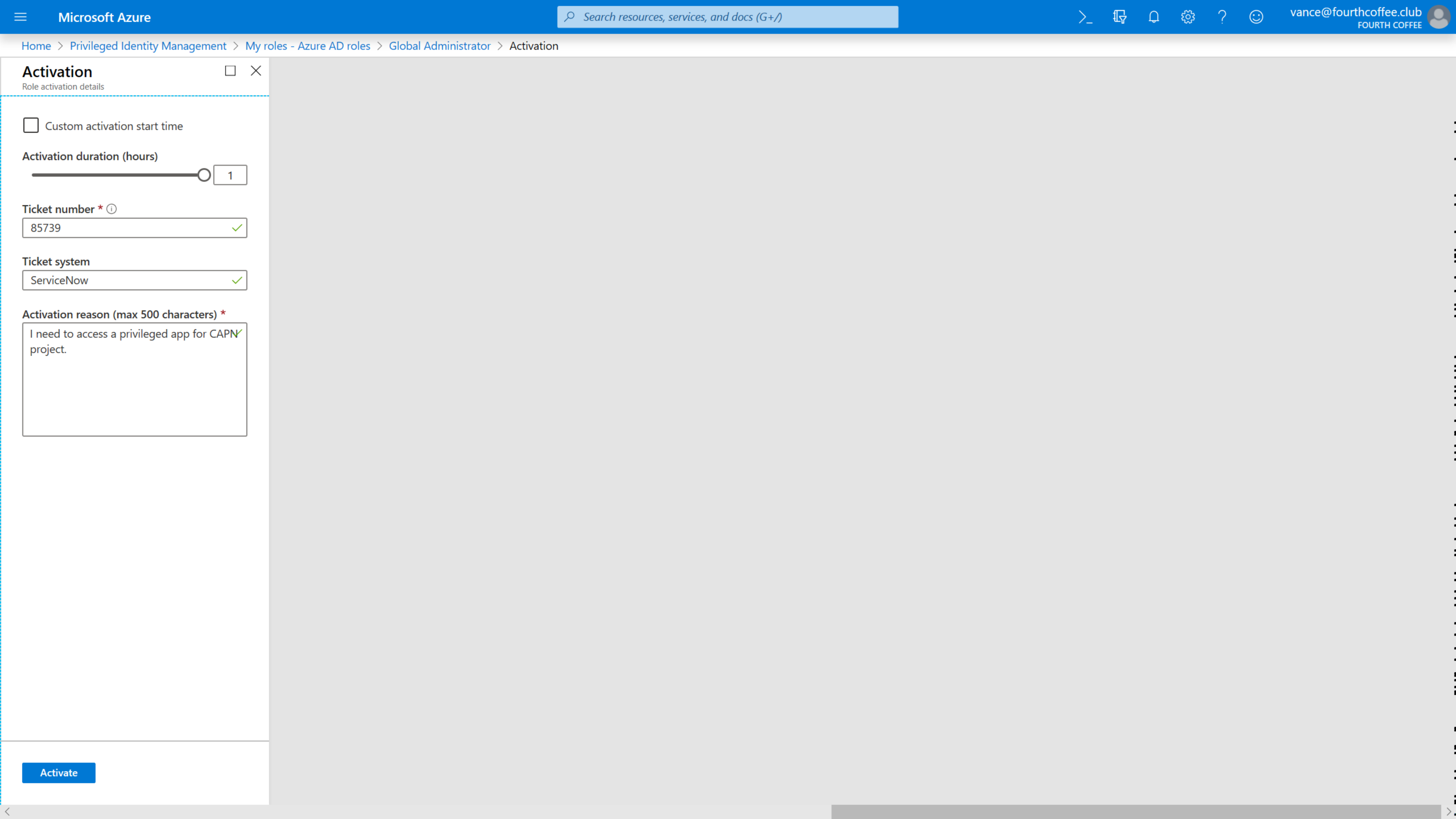
Role activation details

NAME
Vance Brown

EMAIL
vance@fourthcoffee.club

ACTIVATION
Eligible

EXPIRATION
-


Microsoft Azure
Search resources, services, and docs (G+/)
vance@fourthcoffee.club
FOURTH COFFEE
Home > Privileged Identity Management > My roles - Azure AD roles > Global Administrator > Activation
Activate

Activation

Role activation details

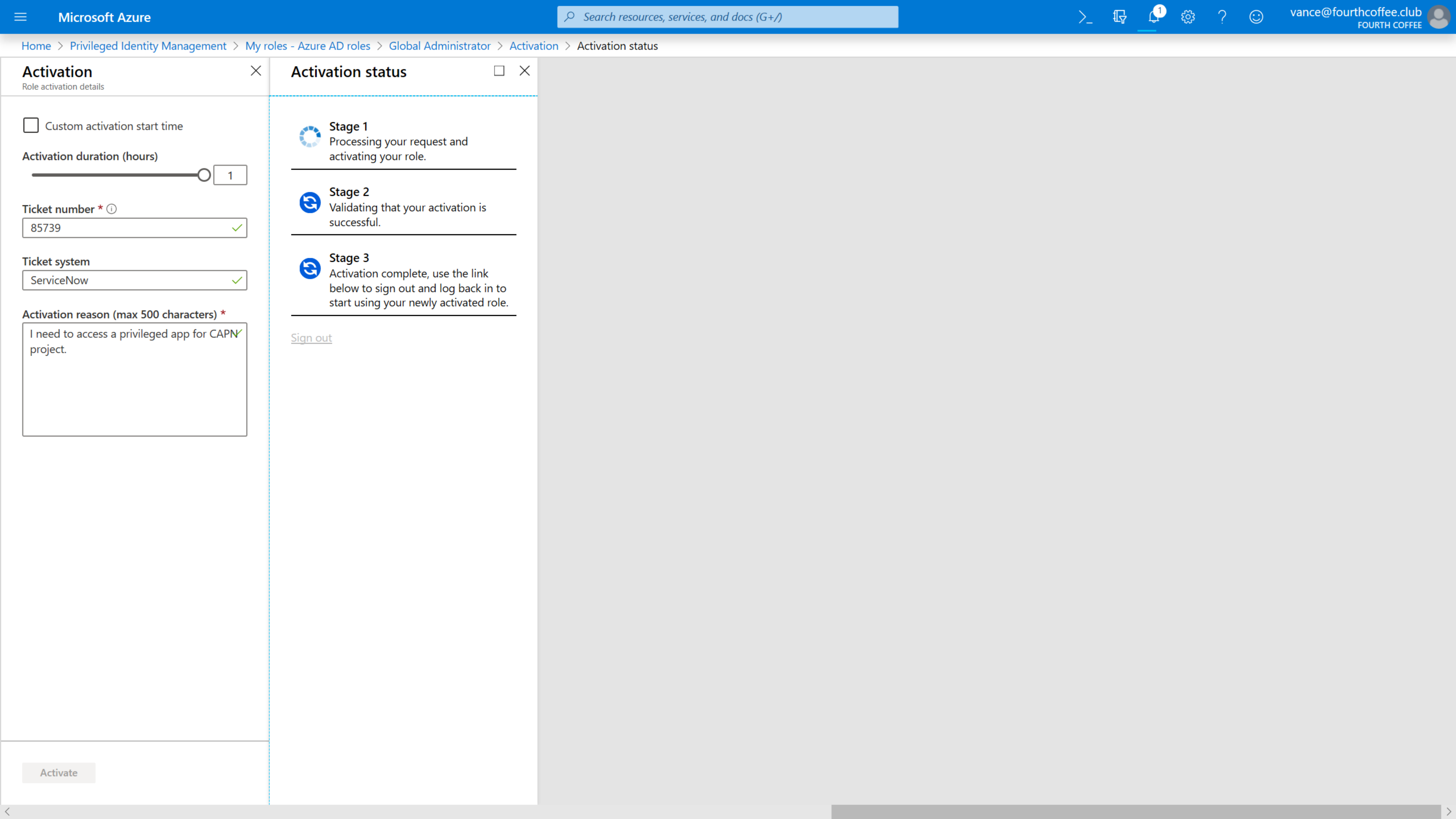
☐ Custom activation start time

Activation duration (hours): 1

Ticket number *: 85739 ✓

Ticket system: ServiceNow ✓

Activation reason (max 500 characters) *: I need to access a privileged app for CAPN project. ✓



Home > Privileged Identity Management > My roles - Azure AD roles > Global Administrator > Activation > Activation status

Activation

Role activation details

□ Custom activation start time

Activation duration (hours): 1

Ticket number *: 85739 ✓

Ticket system: ServiceNow ✓

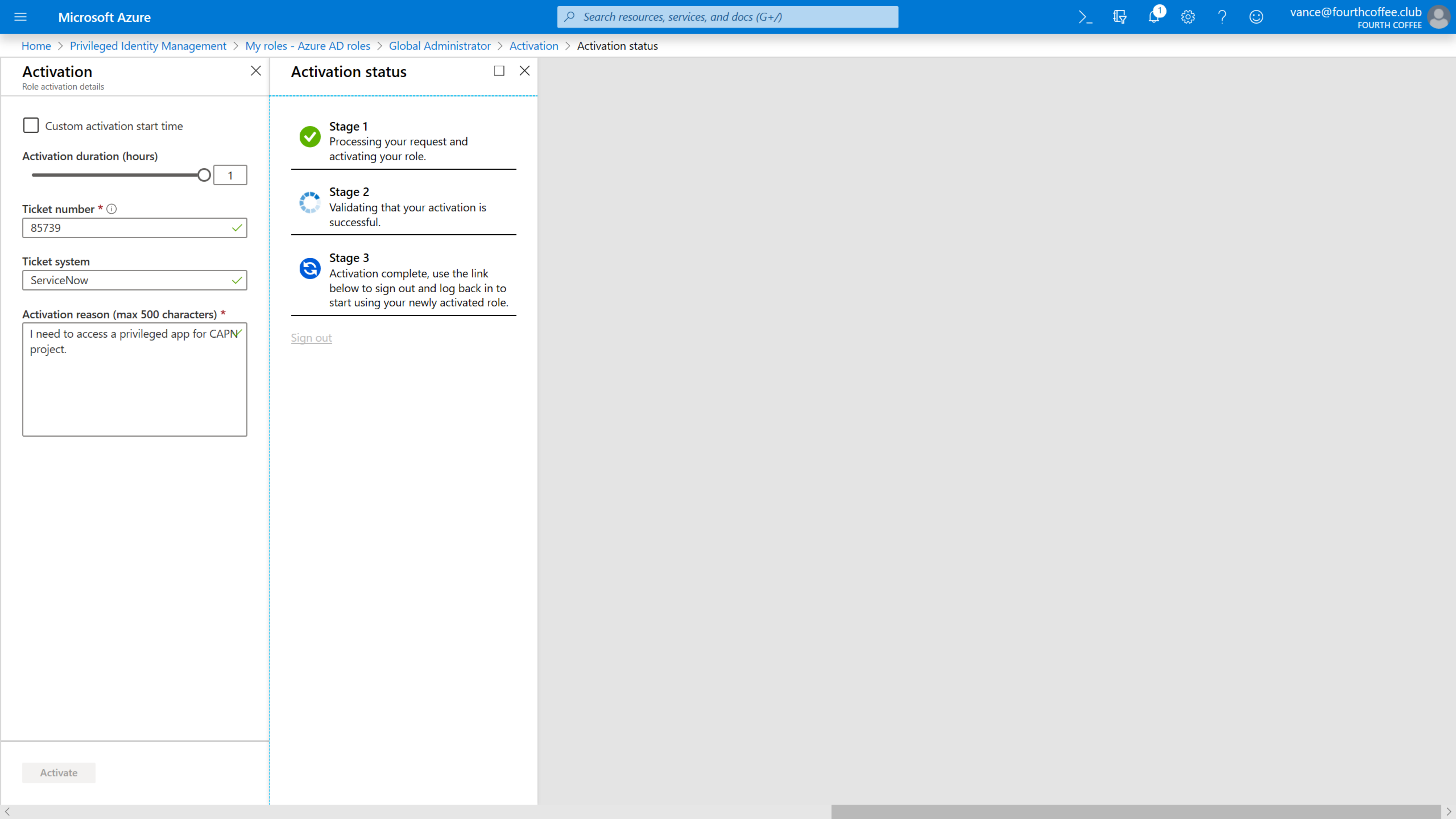
Activation reason (max 500 characters) *: I need to access a privileged app for CAPN project. ✓

Activation status

Stage 1
Processing your request and activating your role.

Stage 2
Validating that your activation is successful.

Stage 3
Activation complete, use the link below to sign out and log back in to start using your newly activated role.



Microsoft Azure
Search resources, services, and docs (G+/)
vance@fourthcoffee.club
FOURTH COFFEE
Home > Privileged Identity Management > My roles - Azure AD roles > Global Administrator > Activation > Activation status

Activation

Role activation details

□ Custom activation start time

Activation duration (hours): 1

Ticket number *: 85739 ✓

Ticket system: ServiceNow ✓

Activation reason (max 500 characters) *: I need to access a privileged app for CAPN project. ✓

Activate

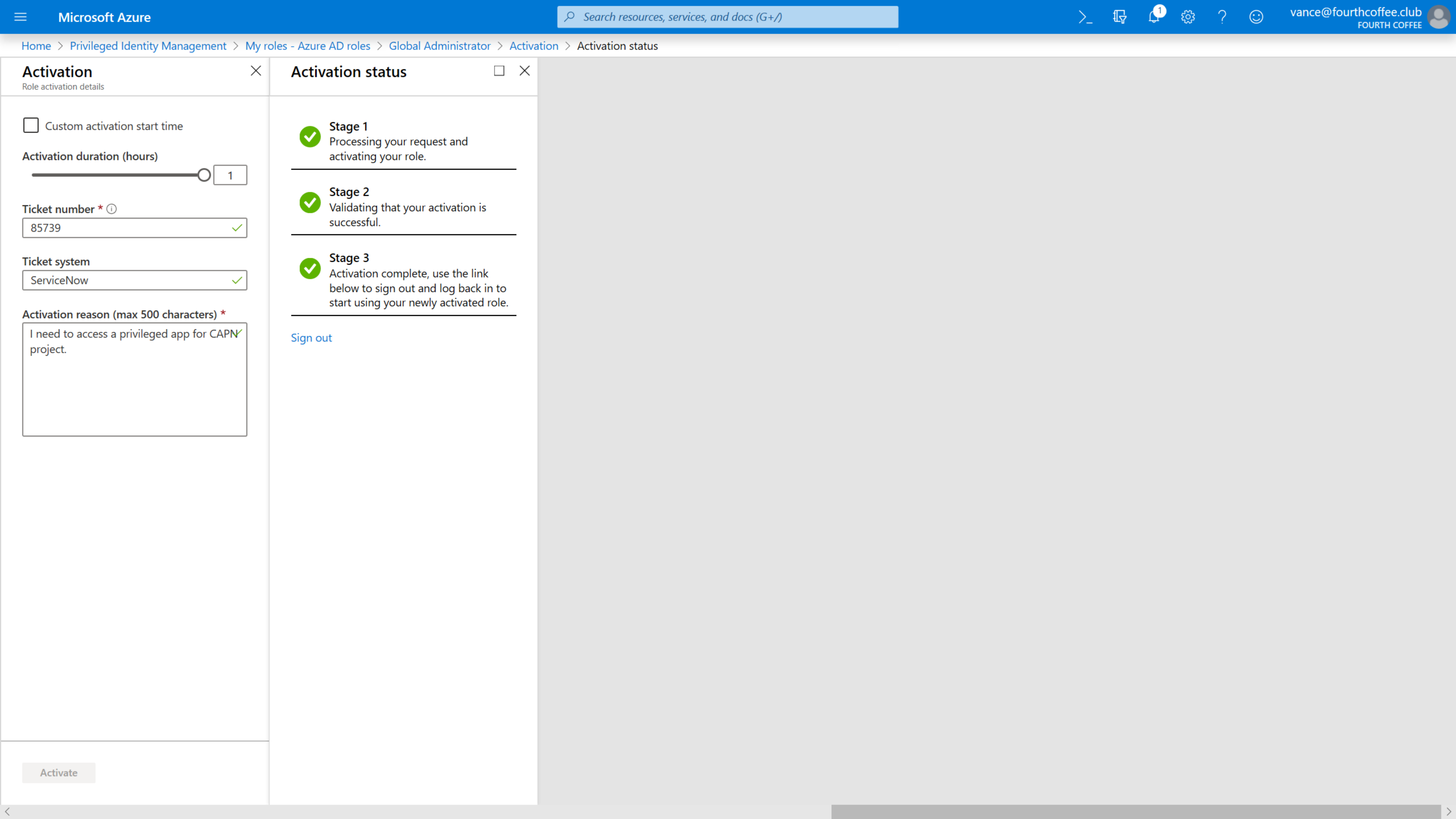
Activation status

✓ Stage 1
Processing your request and activating your role.

Stage 2
Validating that your activation is successful.

Stage 3
Activation complete, use the link below to sign out and log back in to start using your newly activated role.

Sign out



Microsoft Azure
Search resources, services, and docs (G+/)
vance@fourthcoffee.club
FOURTH COFFEE
Home > Privileged Identity Management > My roles - Azure AD roles > Global Administrator > Activation > Activation status

Activation

Role activation details

☐ Custom activation start time

Activation duration (hours): 1

Ticket number *: 85739 ✓

Ticket system: ServiceNow ✓

Activation reason (max 500 characters) *: I need to access a privileged app for CAPN project. ✓

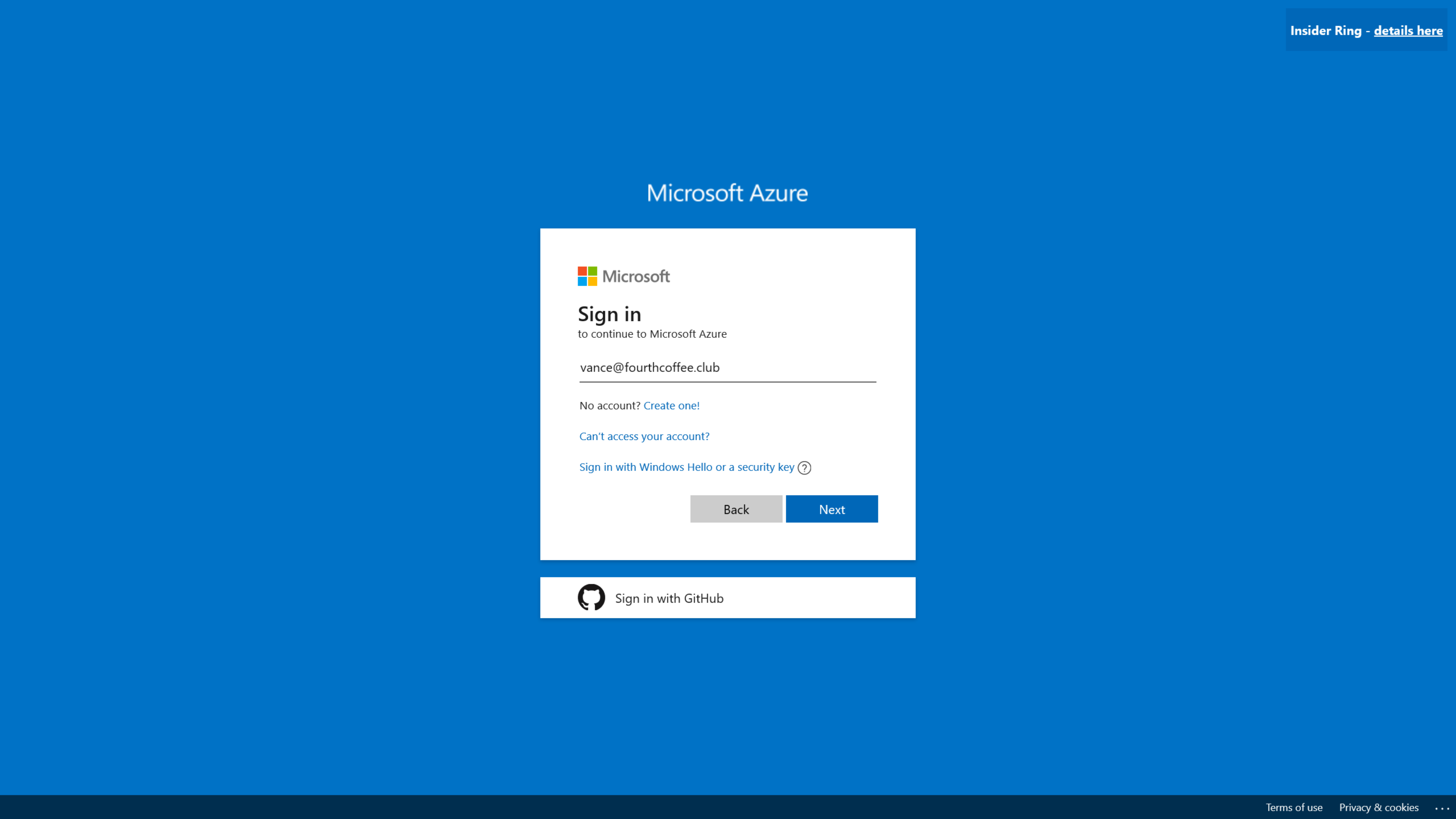
Activation status

✓ **Stage 1**
Processing your request and activating your role.

✓ **Stage 2**
Validating that your activation is successful.

✓ **Stage 3**
Activation complete, use the link below to sign out and log back in to start using your newly activated role.

Sign out



Insider Ring - details here

Microsoft Azure

Microsoft

Sign in

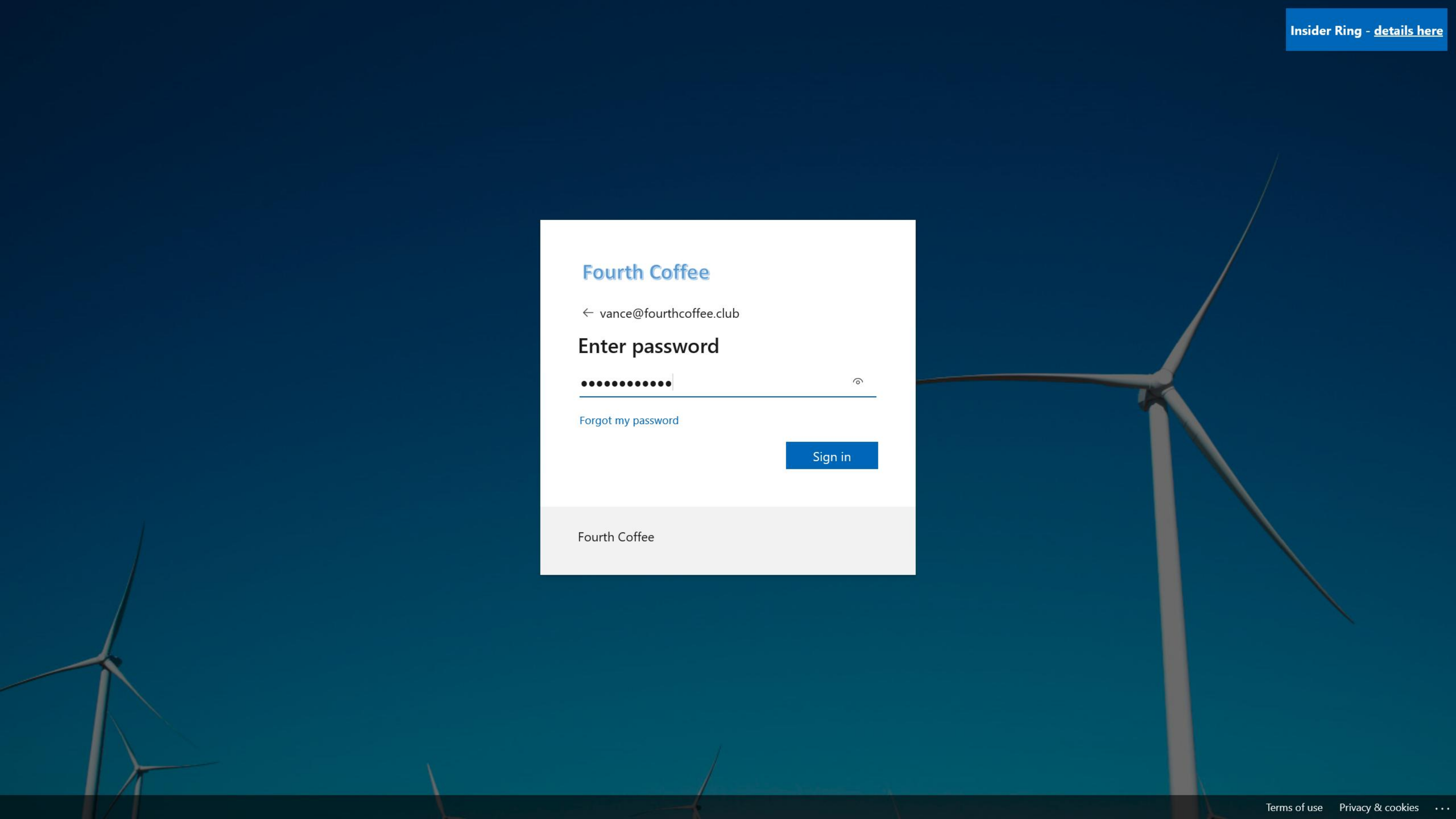
to continue to Microsoft Azure

vance@fourthcoffee.club

No account? Create one!

Can’t access your account?

Sign in with Windows Hello or a security key



Insider Ring - details here

Fourth Coffee

← vance@fourthcoffee.club

Enter password

●●●●●●●●●●●●

Forgot my password

Fourth Coffee