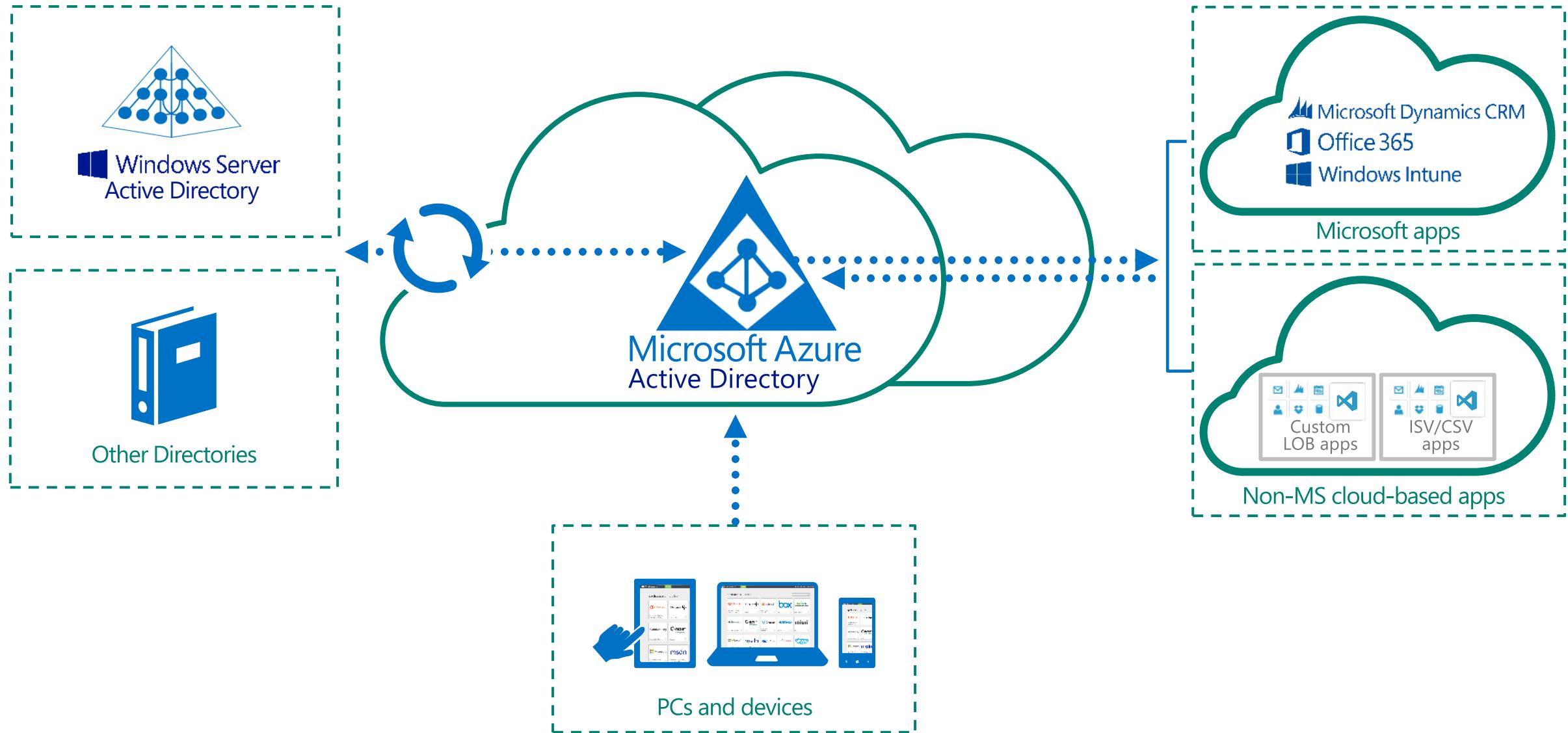


Entra ID as the control point



Azure AD P1

Secure access for a connected world.



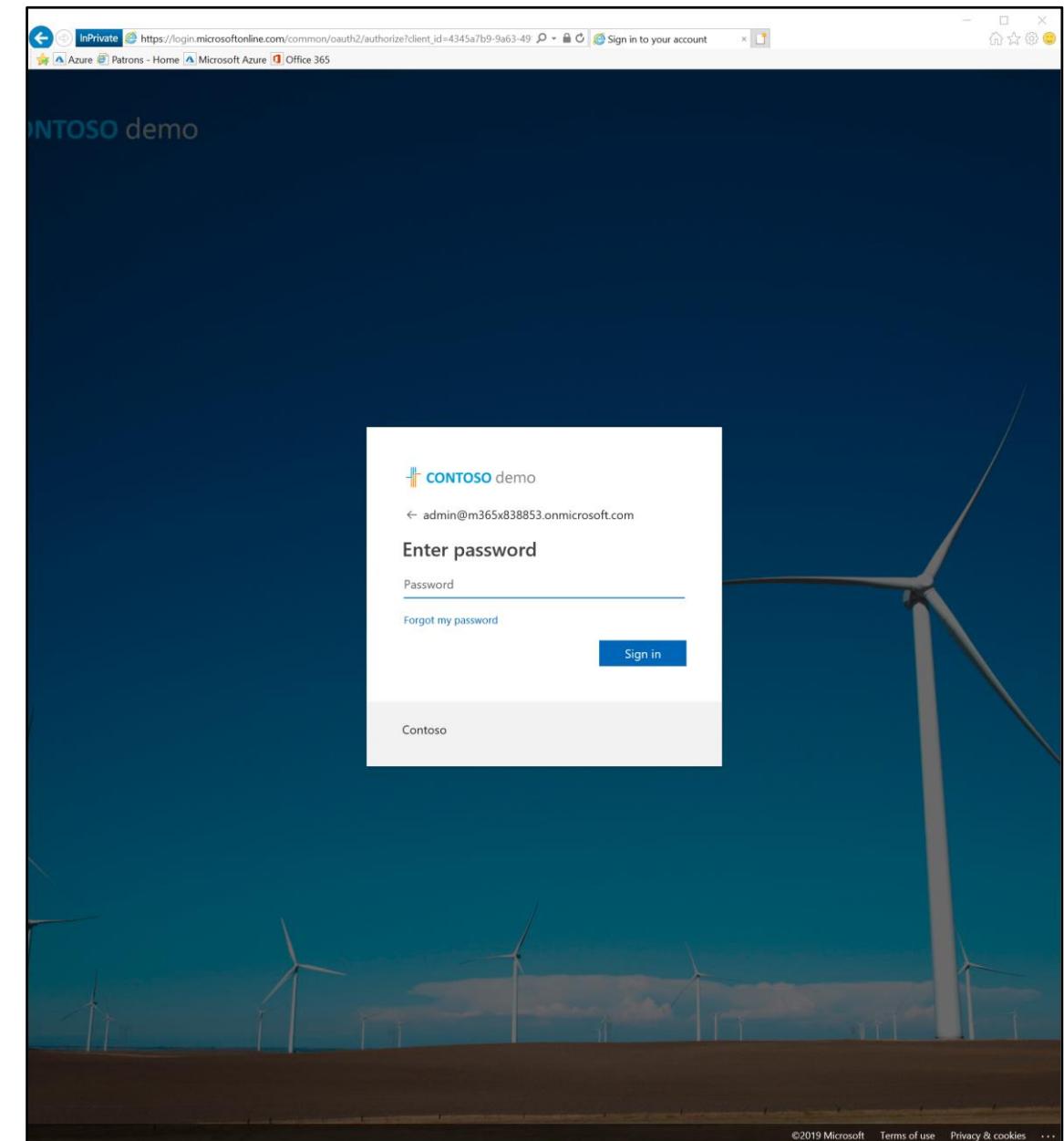
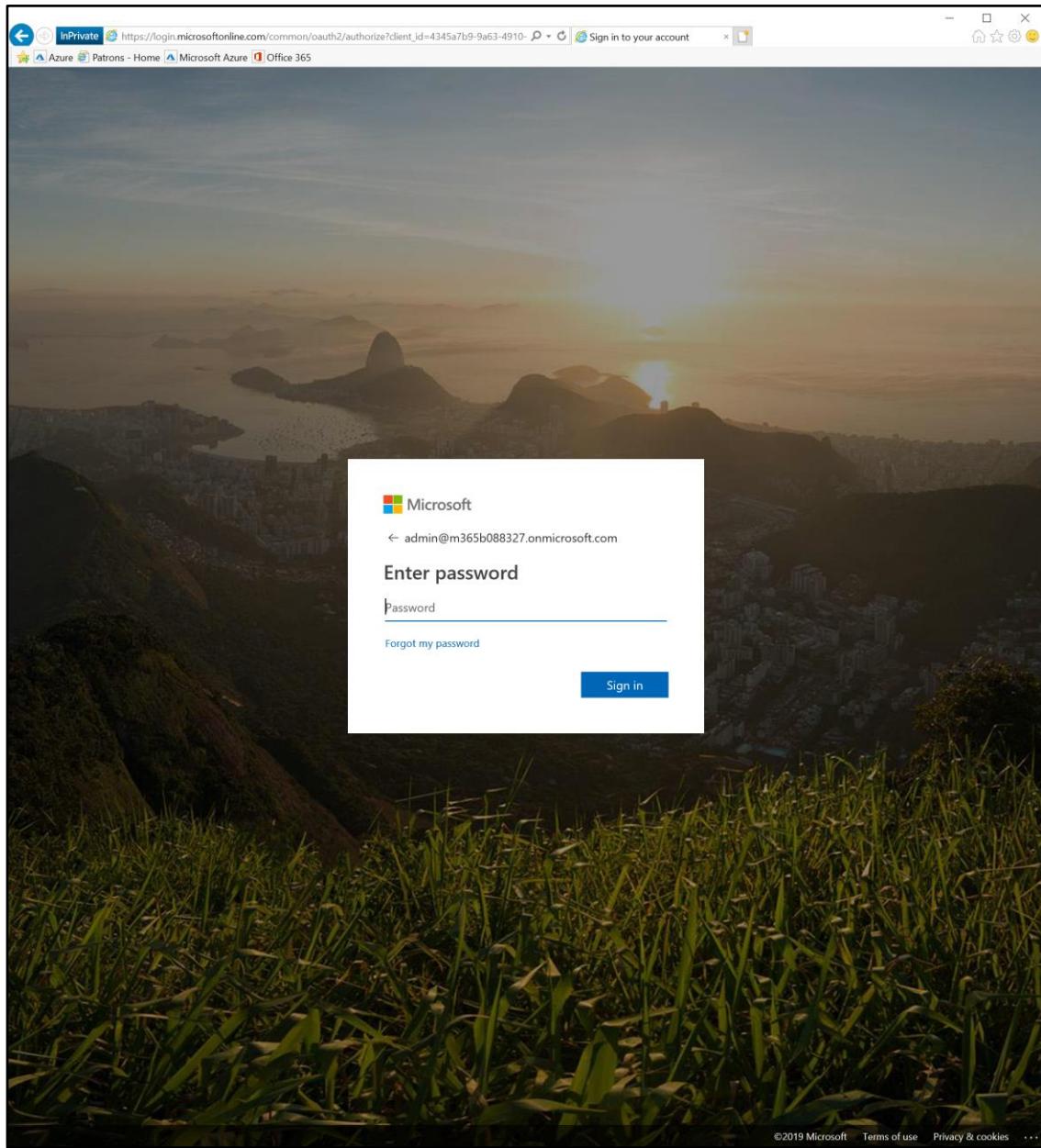
Azure Active Directory

Protect your users, apps, workloads, and devices.

- User directory
- Single sign-on to any app
- User self service
- Multifactor and passwordless authentication
- Conditional Access and Identity Protection
- Hybrid identity management
- Core identity governance
- External and frontline identities

Microsoft 365 Branding

Tenant branding



CIAOPS - Company branding

Azure Active Directory

 Search (Ctrl+/)+ New language Delete ↻

Locale

 Default

Licenses

Azure AD Connect

Custom domain names

Mobility (MDM and MAM)

Password reset

Company branding

User settings

Properties

Notifications settings

Security

Monitoring

Sign-ins

Audit logs

Provisioning logs (Preview)

Logs

Diagnostic settings

Workbooks

Usage & insights

Edit company branding

Azure Active Directory

Save Discard

Sign-in page background image

Image size: 1920x1080px

File size: <300KB

File type: PNG, JPG, or JPEG ⓘRemoveSelect a file Browse

Banner logo

Image size: 280x60px

File size: 10KB

File type: Transparent PNG, JPG, or JPEG ⓘRemoveSelect a file BrowseUsername hint ⓘ ⓘSign-in page text ⓘ Need to Know ⓘ

Advanced settings

Sign-in page background color ⓘ

#CCCCCC

Single Sign On (SSO) Web Portal

Add an application

The screenshot shows the Azure Active Directory (aad.portal.azure.com) interface. On the left, there's a sidebar with various management options like 'Users and groups', 'Enterprise applications', 'App registrations', etc. A large orange arrow points from the 'Enterprise applications' link in the sidebar to the 'All applications' link in the main content area. In the main content area, there's a table titled 'Enterprise applications - All applications'. At the top of this table, there's a 'Columns' dropdown, a search bar, and two buttons: 'Add' and 'Reset'. Another orange arrow points from the 'Add' button in the top right of the table to the 'Add' button in the top left of the table header. The table lists several applications with columns for Homepage URL, Object ID, Application ID, and Publisher.

Homepage URL	Object ID	Application ID	Publisher	
Boomerang	8cd14863-7bfe-4259-8b25-9...	e691bce4-6612-4025-b94c-8...	Microsoft Accounts	
Citrix GoToMeeting	http://www.gotomeeting.com/	29bae620-2006-467e-b06c-6...	9efc94c4-b491-4f36-9779-3a...	Active Directory Application R...
CollabDBService	dc019c32-23e8-42d5-8bd2-8...	166f1b03-5b19-416f-a94b-1d...	Microsoft Corporation	
Discover Hub Api	https://discoverhub.onmicrosoft...	1544d762-9c95-41ec-b797-6...	b2cef57-1bea-43e0-bcab-c6...	Discover Hub
Dropbox for Business	http://www.dropbox.com/	4a342c00-b949-479e-87f6-3a...	97e0a159-74ec-4db1-918a-c0...	Active Directory Application R...
Evernote	https://www-evernote.com/	0b97442e-c0b9-4ba6-b050-d...	45fdee2e-85a2-42be-b2b3-8...	Active Directory Application R...
harmon.ie for Outlook	8c26b05a-e7d7-4347-aab4-2...	170cef4c-862a-443c-b02a-c5...	harmon.ie	
harmon.ie for Outlook	107e2a35-1290-42bf-936e-fd...	46a77f77-a976-4960-9b44-06...	harmon.ie	
iGlobe Planner	https://outlooktool.azurewebs...	f72c7db2-100c-4c93-9356-eb...	a6f5c2f4-0bc2-48bf-8afe-6c9...	iGlobe
LinkedIn	https://www.linkedin.com/	2fb9543-3c05-4764-a275-7b...	4d57f64e-9941-4df2-bb70-8d...	Active Directory Application R...

Add an application

Categories

- All (2854)
- Business management (237)
- Collaboration (372)
- Construction (7)
- Consumer (39)
- Content management (113)
- CRM (138)
- Data services (134)
- Developer services (100)
- E-commerce (70)
- Education (109)
- ERP (60)
- Finance (250)
- Health (53)
- Human resources (237)

Add an application

Add your own app

- Application you're developing**
Register an app you're working on to integrate it with Azure AD
- On-premises application**
Configure Azure AD Application Proxy to enable secure remote access
- Non-gallery application**
Integrate any other application that you don't find in the gallery

Add from the gallery

Enter a name

Featured applications

- Box
- Citrix GoToMeet...
- Concur
- Docusign
- ...
- ...
- ...

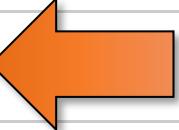
Add an application

Add from the gallery

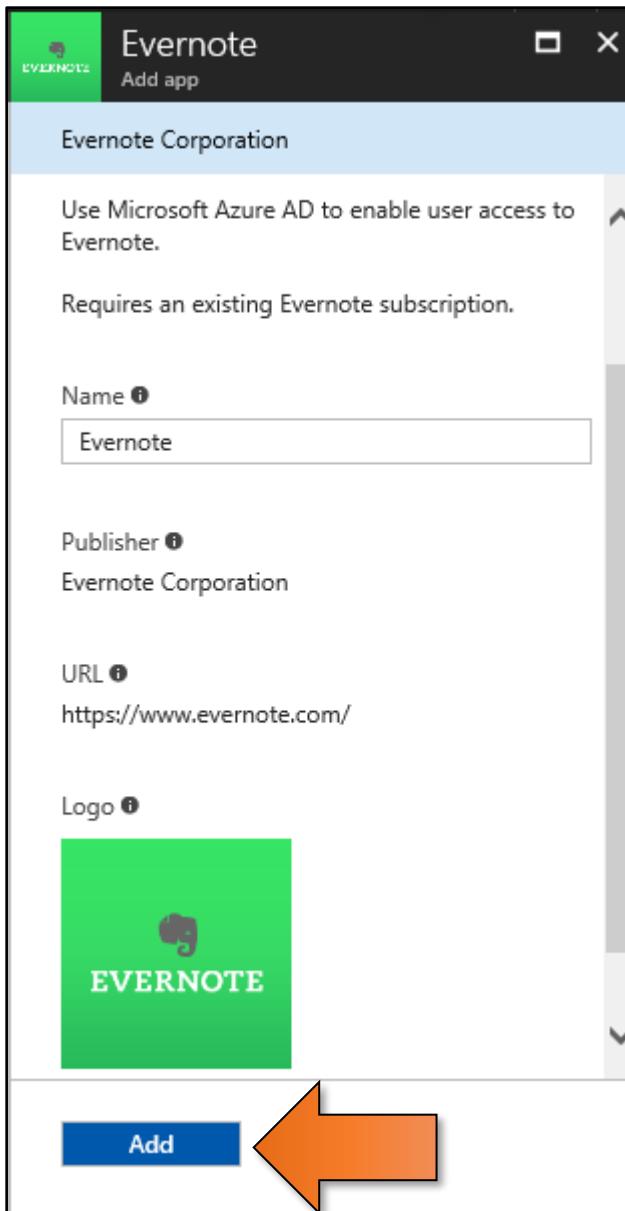
evernote X ✓

1 applications matched "evernote". Choose one below or

NAME	CATEGORY
 Evernote	Collaboration



Add an application



Add an application

Evernote - Quick start
Enterprise Application

Quick start

MANAGE

- Properties
- Users and groups
- Single sign-on
- Provisioning
- Self-service

SECURITY

- Conditional access
- Permissions

ACTIVITY

- Sign-ins
- Analytics

Overview (recommended)

Learn about the steps and concepts required to integrate Evernote with Azure AD.

Assign a user for testing (required)

Choose a single user account under your control to test single sign-on to Evernote.

Configure single sign-on (required)

Configure your instance of Evernote to use Azure AD as its identity provider.

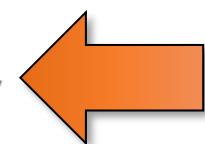
Set up conditional access (optional)

Configure when and how users are prompted for multi-factor authentication.

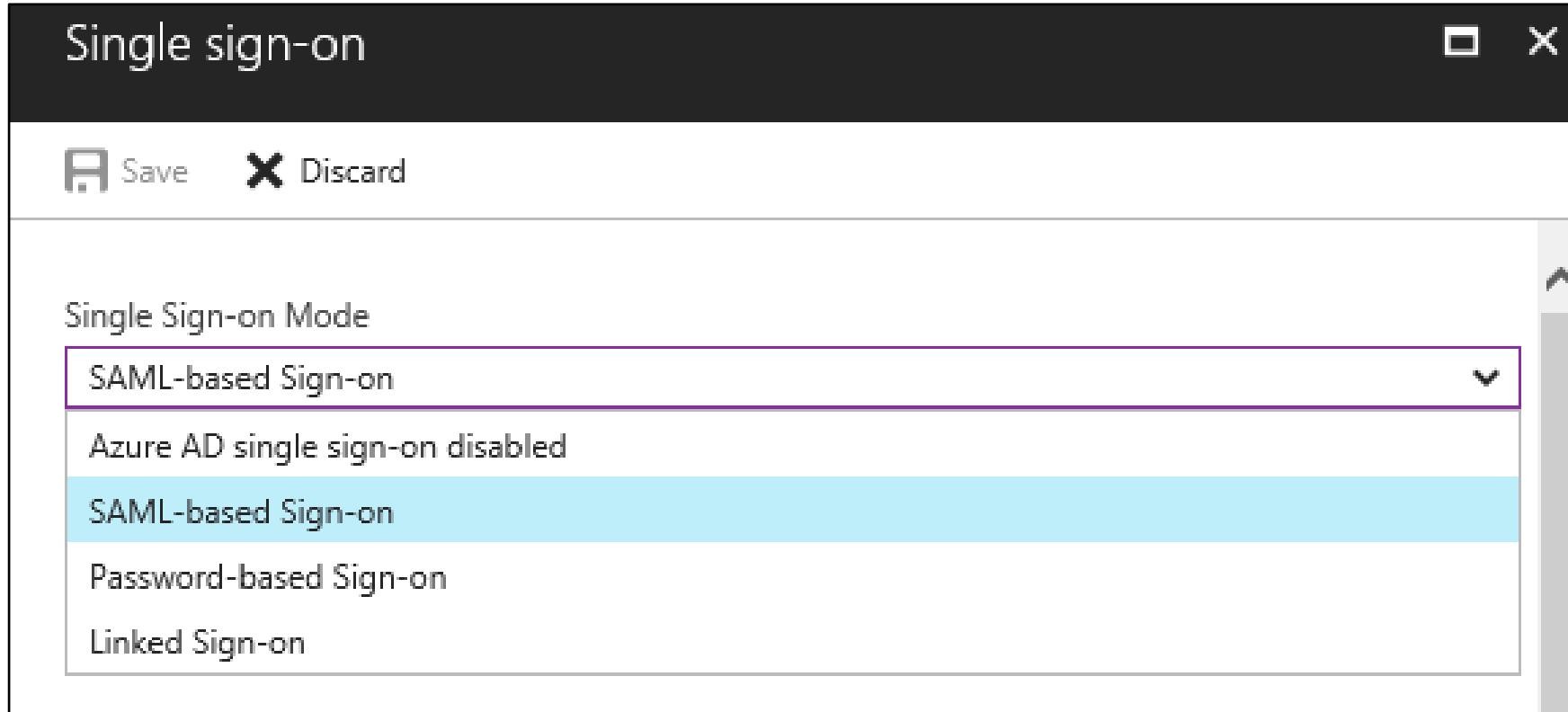
Configure self-service (optional)

Configure the ability for users to request access to this app.

Deploy single sign-on to users and groups (recommended)



Add an application



Add an application

Evernote - Quick start
Enterprise Application

Quick start

MANAGE

- Properties
- Users and groups
- Single sign-on
- Provisioning
- Self-service

SECURITY

- Conditional access
- Permissions

ACTIVITY

- Sign-ins
- Analytics

Overview (recommended)

Learn about the steps and concepts required to integrate Evernote with Azure AD.

Assign a user for testing (required)

Choose a single user account under your control to test single sign-on to Evernote.

Configure single sign-on (required)

Configure your instance of Evernote to use Azure AD as its identity provider.

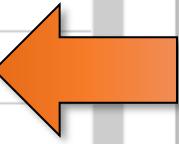
Set up conditional access (optional)

Configure when and how users are prompted for multi-factor authentication.

Configure self-service (optional)

Configure the ability for users to request access to this app.

Deploy single sign-on to users and groups (recommended)



Add an application

Add Assignment
ciaops

 Groups are not available for assignment due to your Active Directory plan level.

Users
None Selected >

Select Role
Default Access >

Assign

Users

+ Invite

Select  a  

 RC	Robert Crane admin@ciaops365.com
 SA	Skykick Admin skykick@ciaops365.com
 TS	Tony Stark tony.stark@ciaops365.com
 YA	Yammer Admin yammer.admin@kumoalliance.net

Selected
None >

Select

Add an application

Add Assignment

ciaops

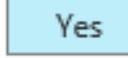
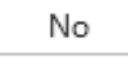
 Groups are not available for assignment due to your Active Directory plan level.

Users
1 user selected.

Select Role
Default Access

Assign Credentials

Assign Credentials

Assign credentials on behalf of the user?  

User Name

Password

Add an application

Evernote - Users and groups
Enterprise Application

Quick start

MANAGE

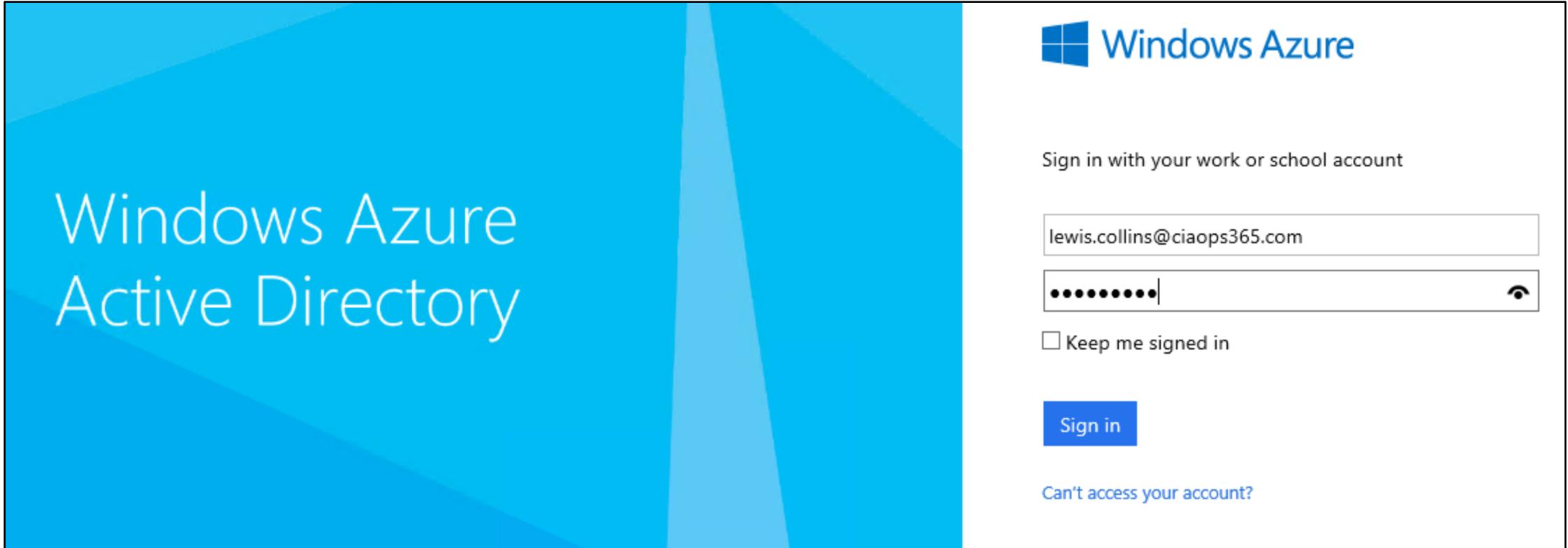
- Properties
- Users and groups**
- Single sign-on
- Provisioning
- Self-service

+ Add user Edit X Remove Update Credentials

First 200 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
Robert Crane	User	Default Access

Add an application



<http://myapps.microsoft.com>

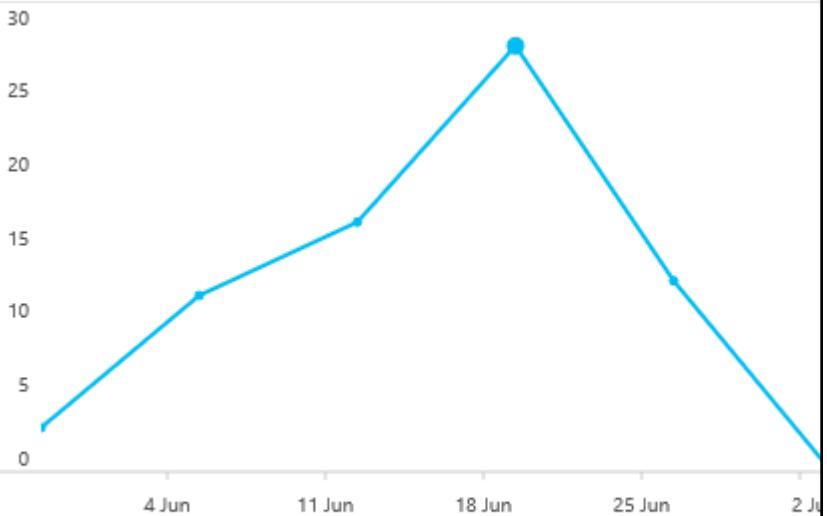
Add an application

The screenshot shows the Microsoft Azure portal interface. At the top left is the CIAOPS logo. On the right, the user profile is shown with the name "Robert CIAOPS" and a small user icon. Below the header, the word "Apps" is displayed. To its right is a search bar with the placeholder "Search apps". The main area contains several application icons with their names: Boomerang, Calendar, Delve, Azure portal, Dynamics 365, Evernote, and Excel. An orange arrow points from the "Evernote" icon towards the "Calendar" icon.

App	Icon	Description
Boomerang	Blue cube icon	A productivity app for managing email and tasks.
Calendar	Purple calendar icon	A calendar application.
Delve	Blue document icon with a gear	A knowledge management tool.
Azure portal	Cloud icon with gears	The central management interface for Azure services.
Dynamics 365	Blue triangle icon	A suite of business applications for sales, customer service, and marketing.
Evernote	Green note icon with a brain	A note-taking and productivity app.
Excel	Green spreadsheet icon	A spreadsheet application.

Add an application – Reporting

App usage between 3/06/2017 and 3/07/2017



OFFICE 365 SHAREPOINT...
10 SIGN-INS

Activity Details: Audit log

Activity

Date : 30/06/2017 1:24:25 PM

Name : Set Company Information

CorrelationId : 12e22e01-bdb9-44fa-88fd-9529bbcd7cbb

Category : Core Directory

Activity Status

Status : N/A

Reason : N/A

Initiated By (Actor)

Type : Application

Name : Microsoft.SharePoint

ObjectId : bbd146ec-a40e-4094-9e7d-d32c2a4f4b42

Spn : 00000003-0000-0ff1-ce00-000000000000

Target(s)

Target

Type : Directory

Name : CIAOPS

ObjectId : 5243d63d-7632-4d07-a77e-de0fea1b77a4

Additional Details

ownload Troubleshoot

User

Enter user name or upn

Application

Office 365 SharePoint Online

Client

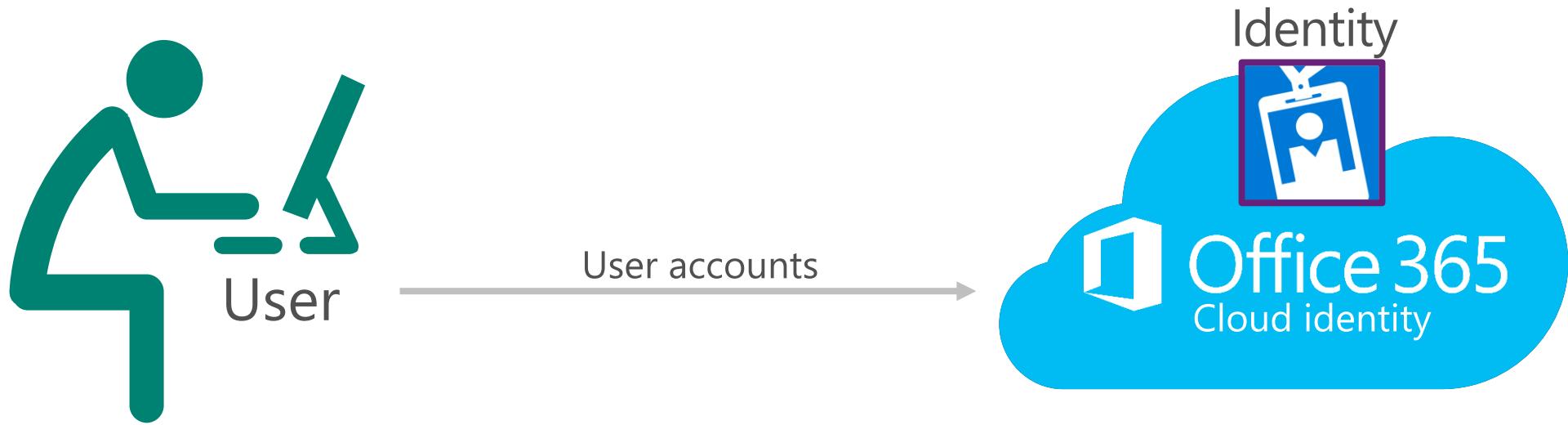
Enter client name

status or IP address. Search requires exact text.

SIGN-IN STATUS	DATE
Success	2/07/2017 8:32:20 AM
Success	30/06/2017 4:40:48 PM
Success	30/06/2017 2:07:04 PM
Success	30/06/2017 2:06:52 PM
Success	30/06/2017 1:07:31 PM
Success	30/06/2017 10:27:11 AM
Success	29/06/2017 7:11:44 PM
Success	28/06/2017 10:05:46 AM
Success	28/06/2017 10:05:15 AM

Cloud Password Reset Portal

Cloud identity model



Enable reset policy

Home > CIAOPS > Password reset - Properties

Password reset - Properties

CIAOPS - Azure Active Directory

Manage

- Properties
- Authentication methods
- Registration
- Notifications
- Customization
- On-premises integration

Activity

- Audit logs

Troubleshooting + Support

- Troubleshoot
- New support request

Save Discard

Self service password reset enabled ⓘ

None Selected All

i These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. Click here to learn more about administrator password policies.

User request password reset

 CIA
OPS

Reset your password

User verification

To reset your password, begin by entering your user ID and the characters in the picture or audio below.

* User ID:

X

Example: user@contoso.onmicrosoft.com or user@contoso.com

Enter the characters in the picture or the words in the audio.

Next Cancel

User verifies identity



Reset your password

verification step 1 > choose a new password

Please choose the contact method we should use for verification:

<input checked="" type="radio"/> Email my alternate email	We've sent an email message containing a verification code to your inbox.
<input type="radio"/> Text my mobile phone	
<input type="radio"/> Call my mobile phone	
<input type="radio"/> Answer my security questions	

Enter your verification code

Next

[Cancel](#)

User selects new password



Reset your password

verification step 1 ✓ > **choose a new password**

* Enter new password:

>Password strength

* Confirm new password:

A strong password is required. Strong passwords are 8 to 16 characters and must combine uppercase and lowercase letters, numbers, and symbols. They cannot contain your username.

Finish [Cancel](#)

Reporting

Audit logs

ciaops - Audit logs
Azure Active Directory

User settings Properties Notifications settings

SECURITY

Conditional access Users flagged for risk Risky sign-ins

ACTIVITY

Sign-ins **Audit logs**

TROUBLESHOOTING + SUPPORT

Troubleshoot New support request

Columns Refresh Download Troubleshoot

Category All Activity Resource Type All Activity All

Date Range 7 Days Target Enter target name or upn Initiated By (Actor) Enter actor name or upn

Apply

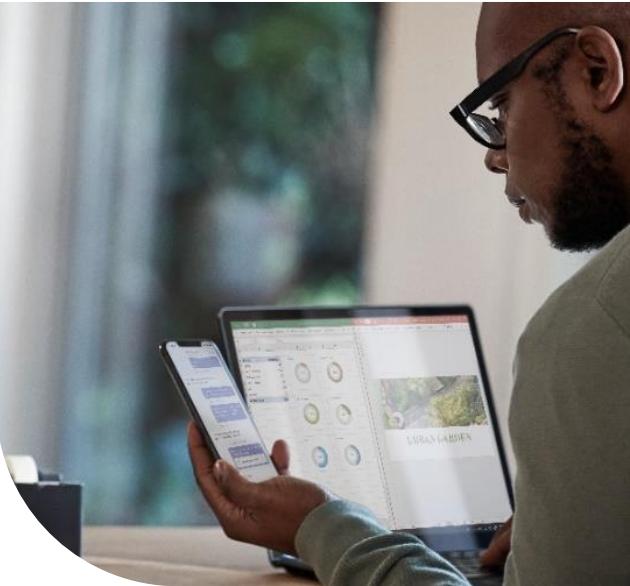
Search to filter items...

DATE	TARGET(S)	INITIATED BY (ACTOR)	ACTIVITY
3/07/2017 3:02:22 PM	Directory : b75e7296-a058-4707-acb8...	Microsoft Azure AD Internal	Update external secrets
3/07/2017 3:02:21 PM	User : admin@ciaops365.com	admin@ciaops365.com	Update user
3/07/2017 3:02:21 PM	ServicePrincipal : Evernote, User : admi...	admin@ciaops365.com	Add app role assignment grant to user
3/07/2017 2:59:13 PM	Directory : Evernote	Microsoft Azure AD Internal	Update external secrets
3/07/2017 2:59:12 PM	ServicePrincipal : Evernote	admin@ciaops365.com	Update service principal
3/07/2017 2:53:32 PM	ServicePrincipal : Evernote	admin@ciaops365.com	Update service principal
3/07/2017 2:53:32 PM	ServicePrincipal : Evernote	admin@ciaops365.com	Update service principal
3/07/2017 2:52:53 PM	ServicePrincipal : Evernote	admin@ciaops365.com	Add service principal
3/07/2017 2:52:52 PM	Application : Evernote	admin@ciaops365.com	Add application

Multi Factor

Enforce Multi-factor authentication

Verify user identities with strong authentication



We support a **broad range of multi-factor authentication options**

Including passwordless technology



Microsoft
Authenticator



Windows
Hello



FIDO2
Security key



Biometrics



Push
Notification



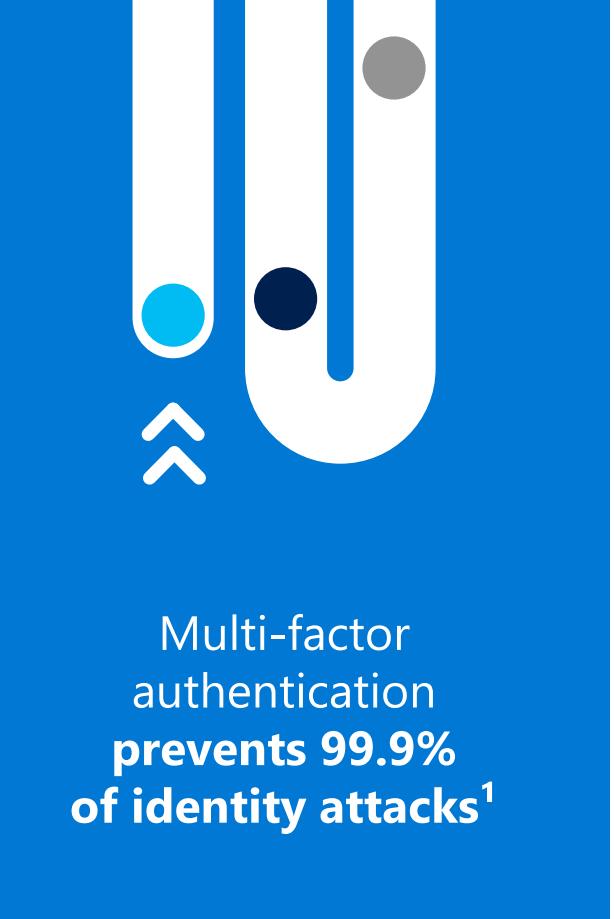
Soft
Tokens OTP



Hard
Tokens OTP



SMS,
Voice



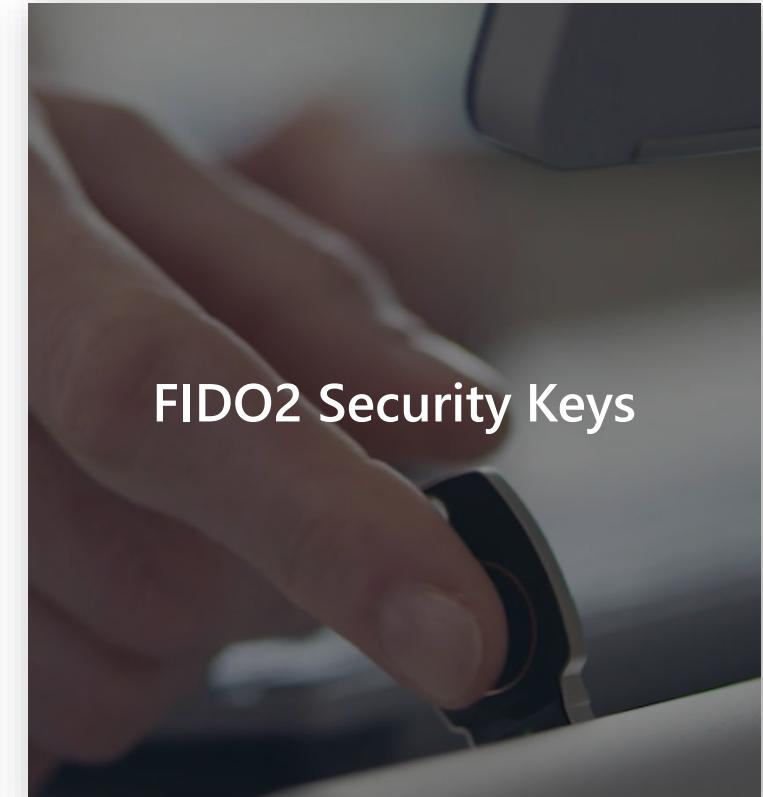
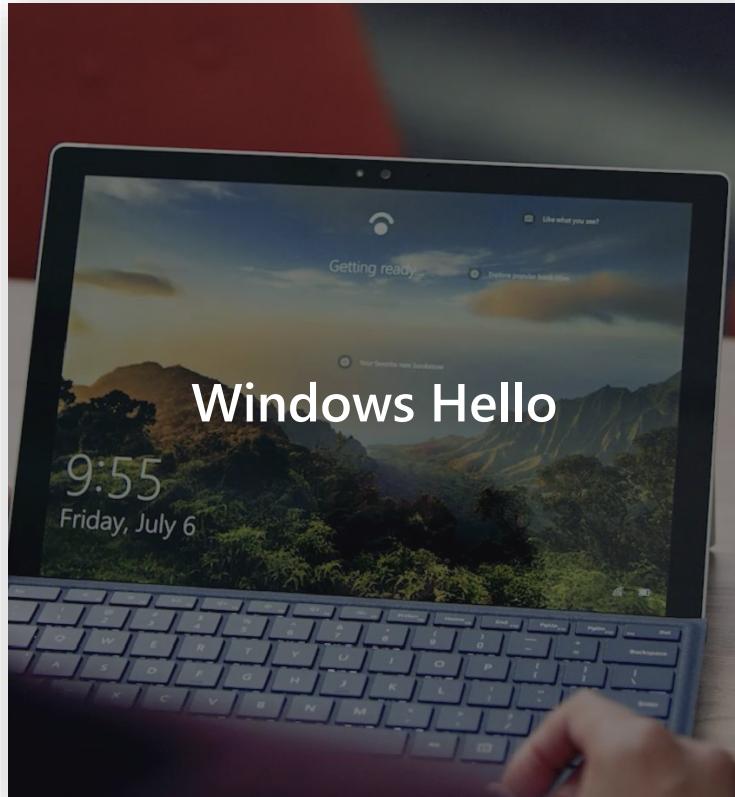
1. "Your Password Doesn't Matter" July 2019, Microsoft Tech Community Research Article

MFA and Password-less



Secure authentication

Getting to a world without passwords



Secure authentication

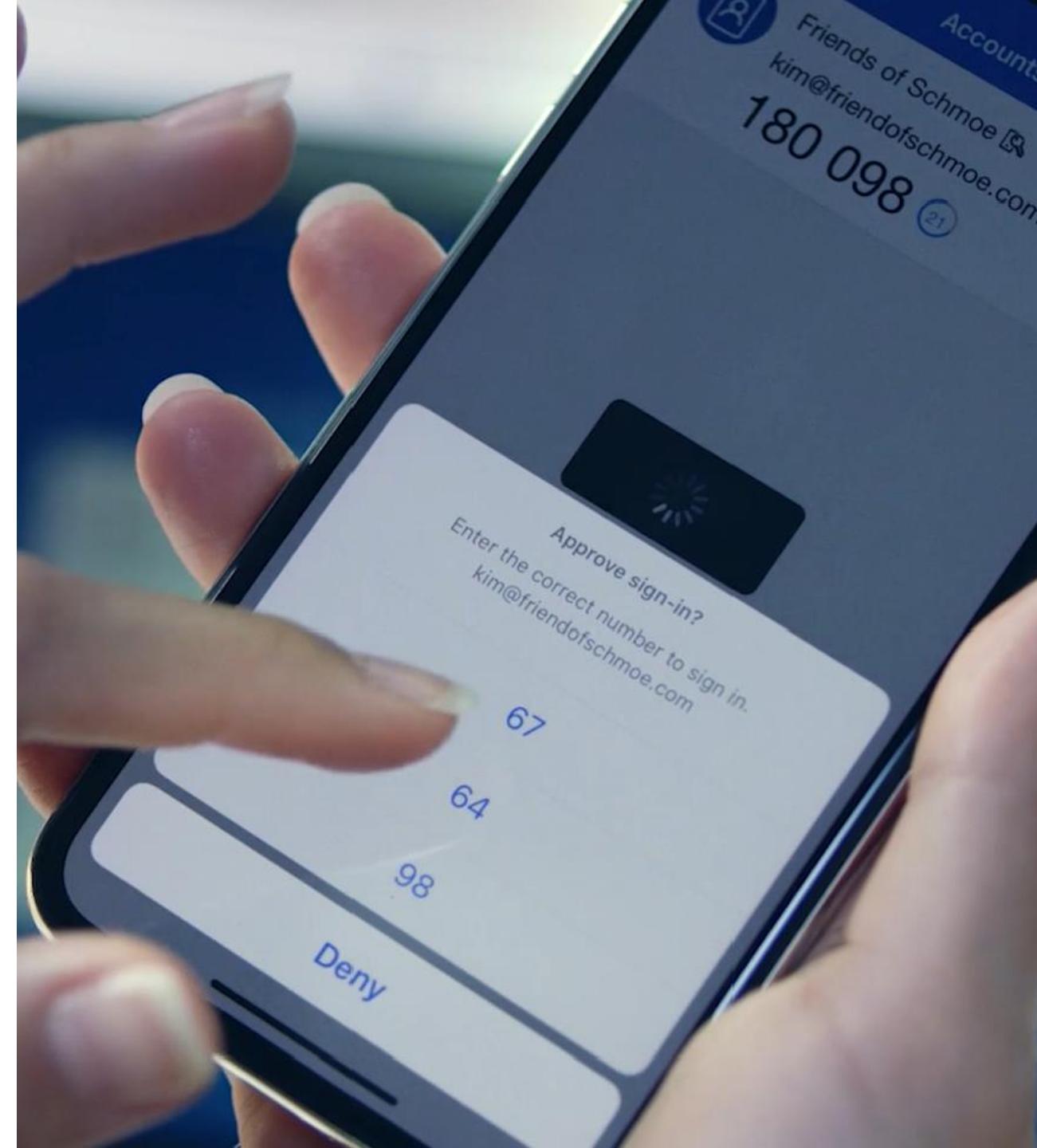
Microsoft Authenticator

MFA for enterprise and consumer accounts and applications

Device registration (workplace join)

Single sign-on to native mobile apps

Certificate-based SSO



Are you trying to sign in?

CIAOPS
admin@ciaops365.com

Enter the number shown to sign in.

App
OfficeHome

Location
NSW, Australia



Enter number here

No, it's not me

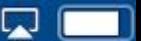
Yes

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context>

iPod



8:34 AM



Accounts



Contoso M365x50...



MeganB@soseman.org

986 442

Approve sign-in?

Contoso M365x505060
MeganB@soseman.org

Deny

Approve

Multi-Factor Authentication Methods



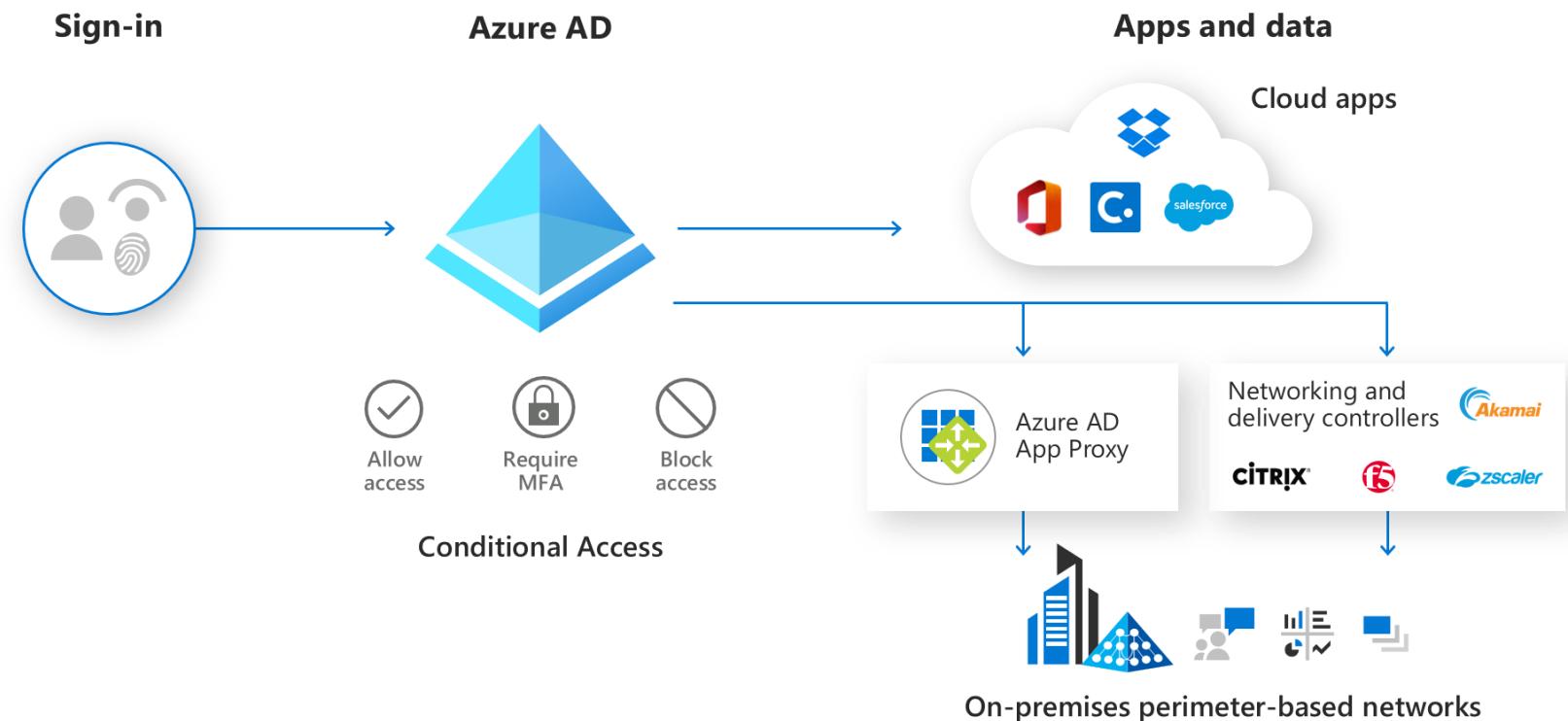
Secure access to work apps – with Azure Active Directory

Azure AD Premium P1 is now included with Microsoft 365 Business Premium

Enable your employees to remotely access on-premises apps without opening broad access to your network with App Proxy¹

Control “where, when and who” connects to Office apps with Conditional Access

Automatically add/remove users to security groups and reduce IT overhead with Dynamic Groups



Set up identity security with MFA

The problem:

Passwords are vulnerable¹

- 90% of passwords can be cracked in less than six hours¹
- Two-thirds of people use the same password everywhere¹
- Criminals are getting more effective in stealing passwords through phishing and social engineering

The solution:

Multi-factor authentication (MFA)

MFA is enabled by default any Microsoft 365 customer using security defaults

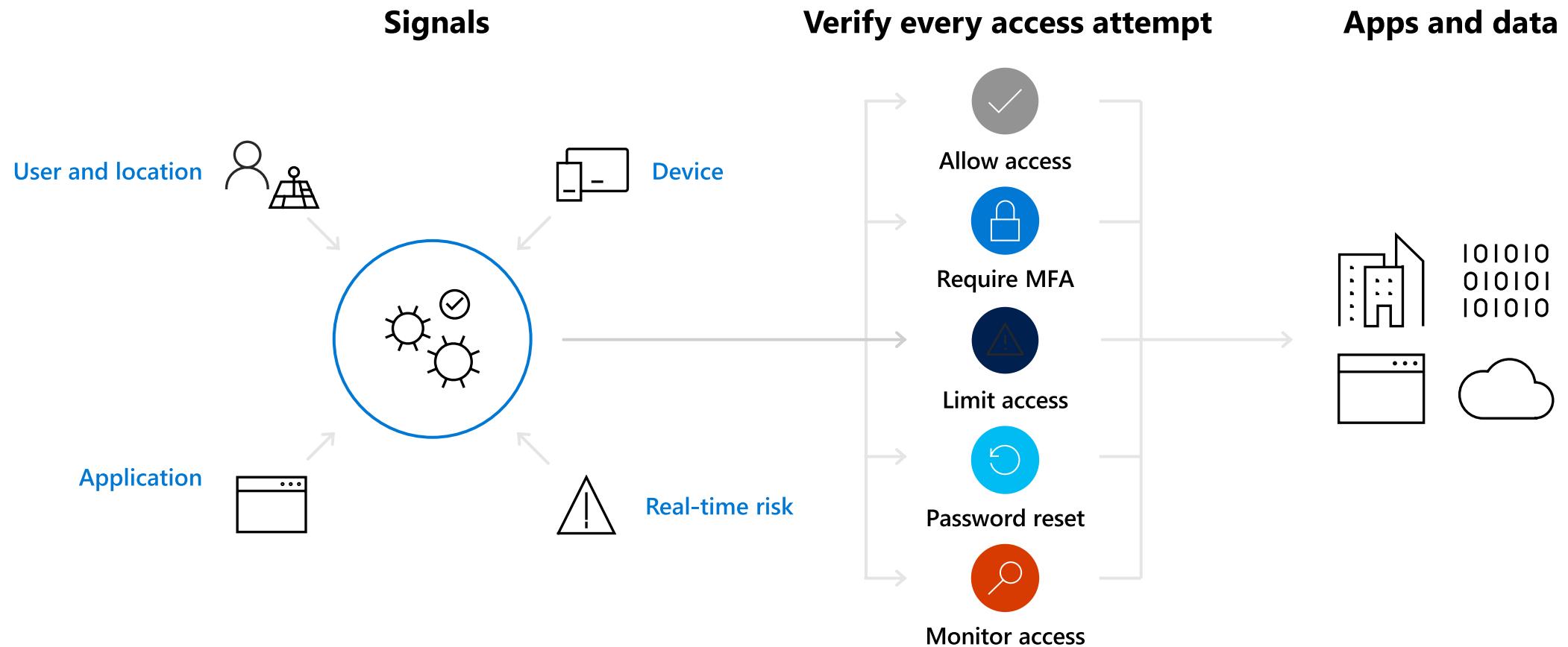
Partners **should** enable MFA for Microsoft 365 Business Premium customers by using conditional access policies

Partners **should** use passwordless MFA authentication methods when possible

¹ <https://secureswissdata.com/two-factor-authentication-importance/>

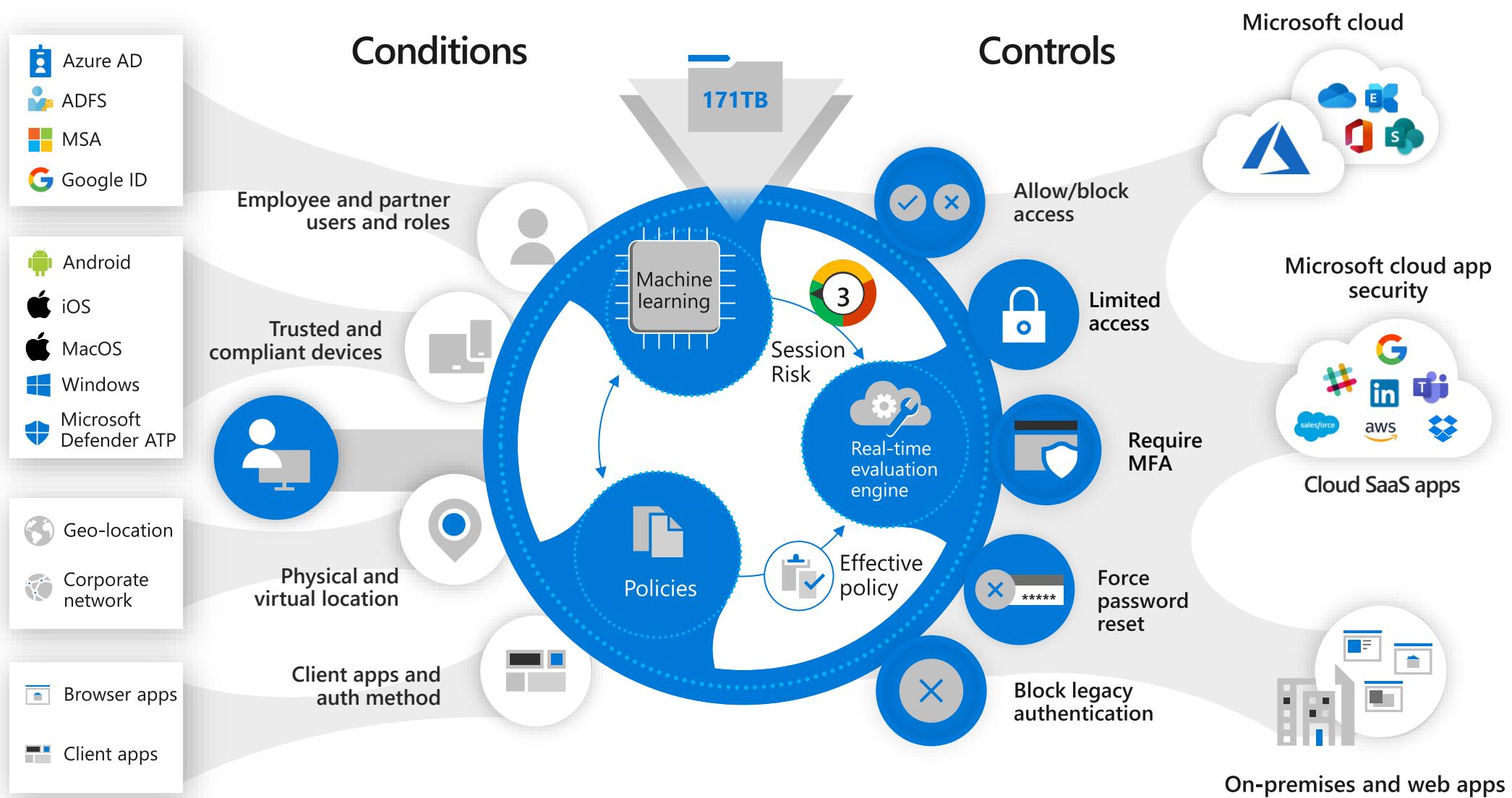
Protect resources with Conditional Access

Configure adaptive access policies based on context and risk

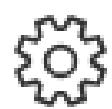


Conditional access and identity protection

Real-time risk-based access control



Enterprise State Roaming



Devices | Enterprise State Roaming

...

CIAOPS - Microsoft Entra ID



Save



Discard



Got feedback?

 [Overview](#)Users may sync settings and app data across devices [\(i\)](#) [All devices](#)[All](#)[Selected](#)[None](#) [Manage](#)

Selected

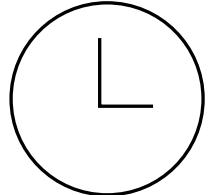
 [Device settings](#)

No member selected

 [Enterprise State Roaming](#) [BitLocker keys \(Preview\)](#) [Local administrator password recovery](#) [Activity](#)

Privileged Identity Management (PIM)

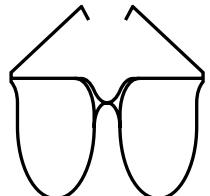
Privileged Identity Management



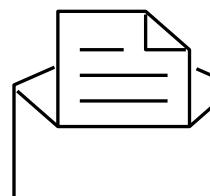
Privileged role membership only granted for a limited amount of time



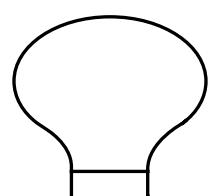
Roles can be configured to require staff to perform MFA prior to elevation of privilege



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

 Privileged Identity Management - Quick start
Privileged Identity Management

[What's new](#) [Get started](#)

- ## 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

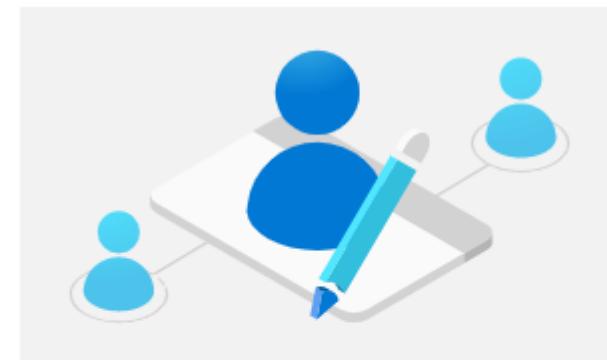
Activity

- ## My audit history

Troubleshooting + Support

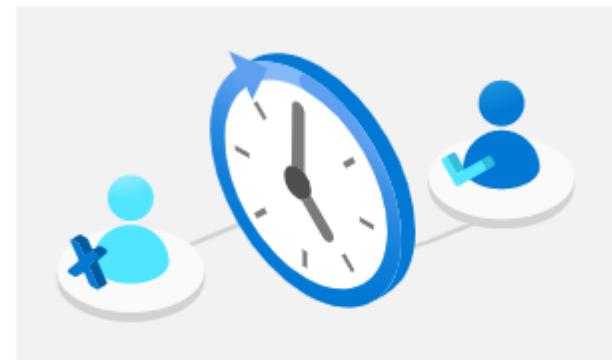
Manage your privileged access

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](#)



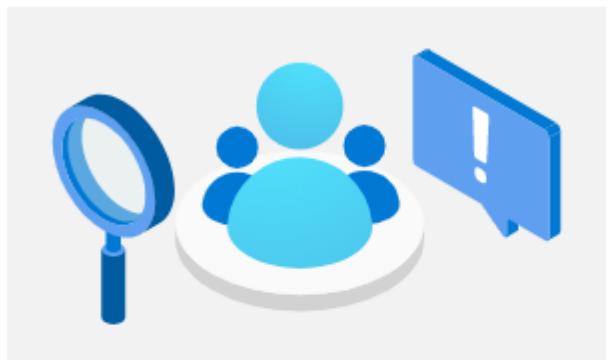
Manage access

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

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 X

Role activation details

Activate Deactivate

! Verify your identity before proceeding →

NAME
Vance Brown

EMAIL
vance@fourthcoffee.club

ACTIVATION
Eligible

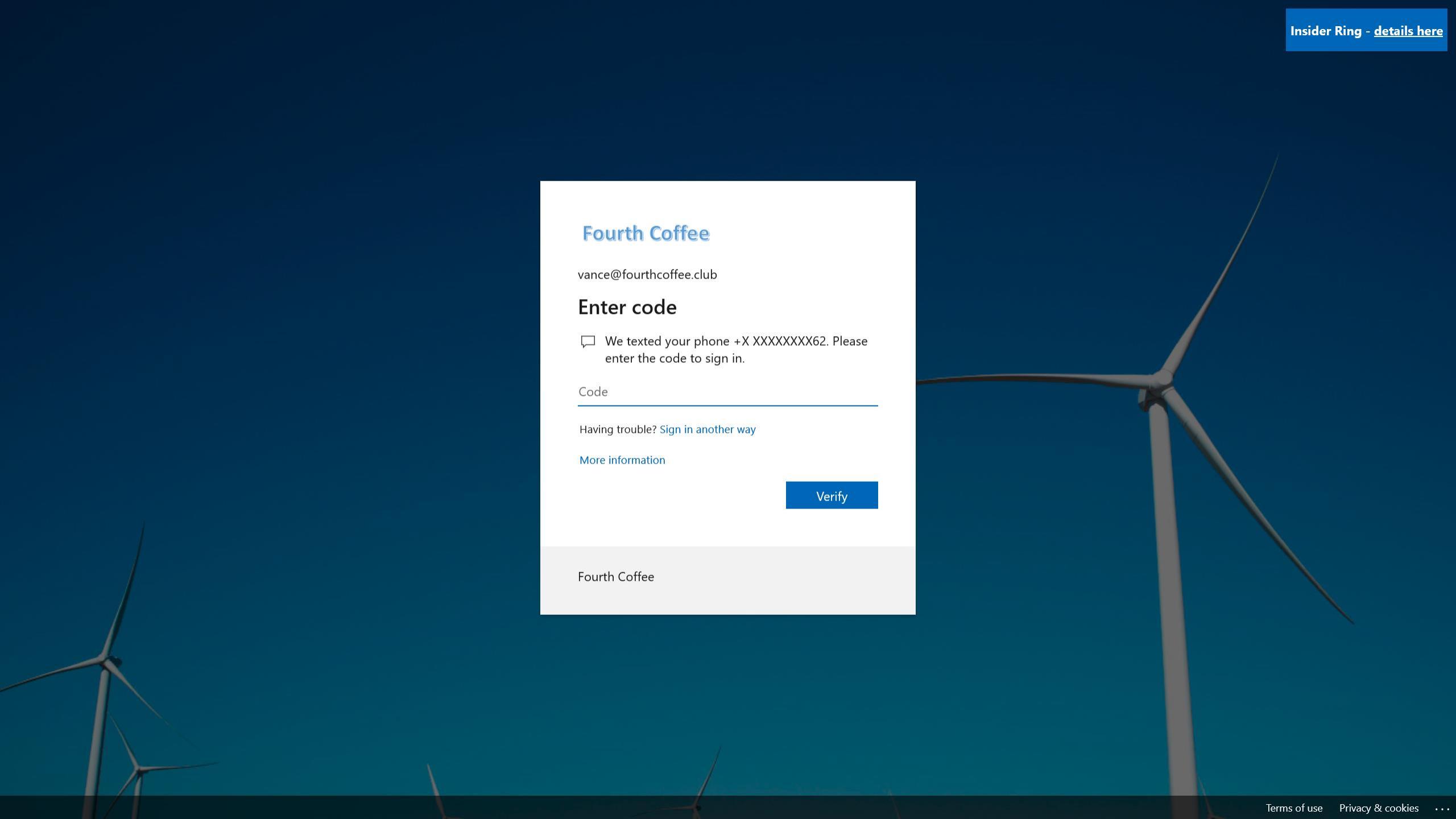
EXPIRATION
-

Verify my identity X

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.

! Verify my identity X



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](#)

Verify

Fourth Coffee

Microsoft Azure

Search resources, services, and docs (G+)

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

Global Administrator X □ ×

Role activation details

Activate Deactivate

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

Activation

Role activation details

Custom activation start time

Activation duration (hours)

Ticket number * ⓘ ✓

Ticket system ✓

Activation reason (max 500 characters) *

I need to access a privileged app for CAPN project.

Activate

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)

Ticket number * 

Ticket system 

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](#)

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)

Ticket number * 

Ticket system 

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](#)

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)

Ticket number *

Ticket system

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](#)

Activate

Microsoft Azure

 Microsoft

Sign in
to continue to Microsoft Azure

vance@fourthcoffee.club

No account? [Create one!](#)

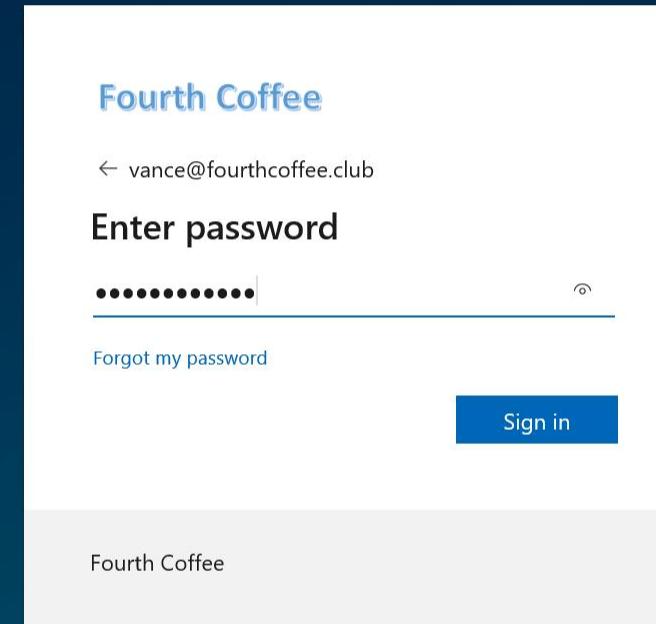
[Can't access your account?](#)

[Sign in with Windows Hello or a security key](#) ⓘ

[Back](#) [Next](#)



[Sign in with GitHub](#)



Fourth Coffee

← vance@fourthcoffee.club

Enter password

••••••••••| ↶

[Forgot my password](#)

Sign in

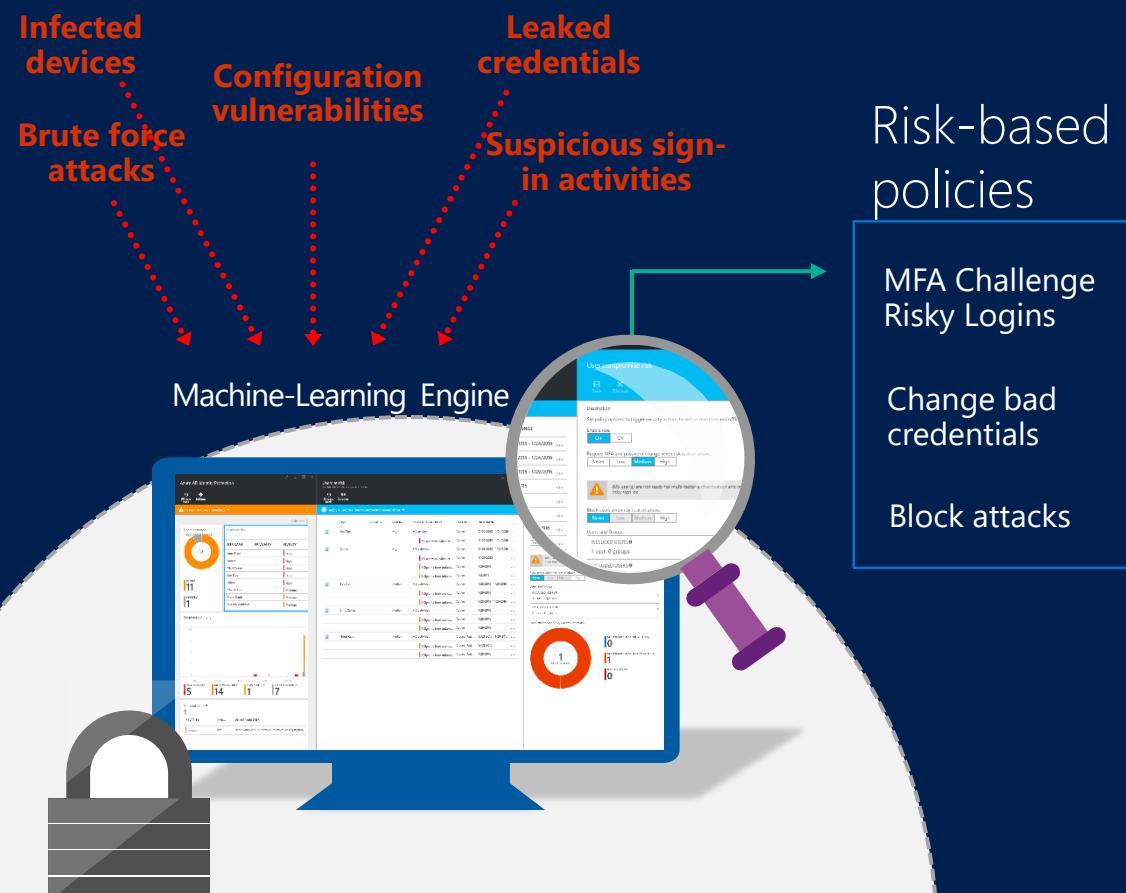
Fourth Coffee

Identity Protection

Entra ID Identity Protection

Identity Protection at its best

- ▶ Gain insights from a consolidated view of machine learning based threat detection
- ▶ Remediation recommendations
- ▶ Risk severity calculation
- ▶ Risk-based conditional access automatically protects against suspicious logins and compromised credentials



Identity Protection - Overview

 Search (Ctrl+/)[Learn more](#)

Refresh

Got feedback?

[Overview](#)

Date range = 30 days

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

New risky users detected

User risk level = All

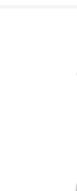
01/04 01/11 01/18 01/25

[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.

Microsoft Azure

 Microsoft

Sign in

to continue to Microsoft Azure

clara@fourthcoffee.club| X

No account? [Create one!](#)

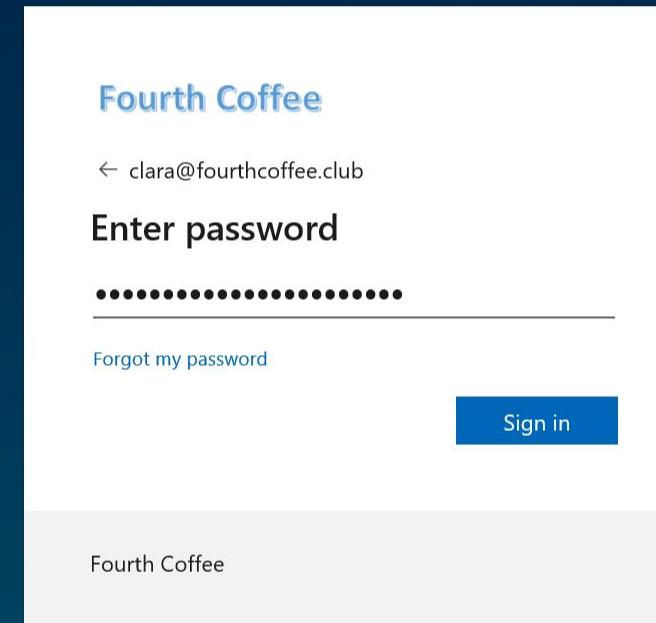
[Can't access your account?](#)

[Sign in with Windows Hello or a security key](#) ⓘ

Back Next



[Sign in with GitHub](#)



Fourth Coffee

← clara@fourthcoffee.club

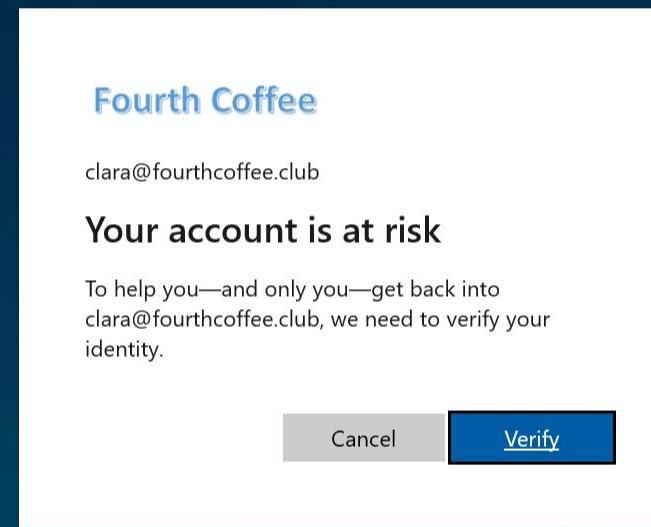
Enter password

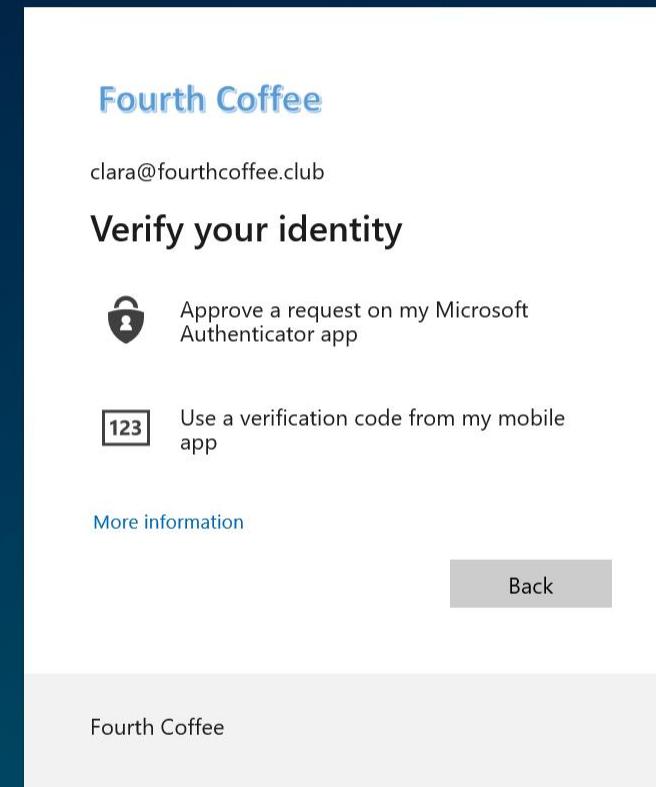
••••••••••••••••

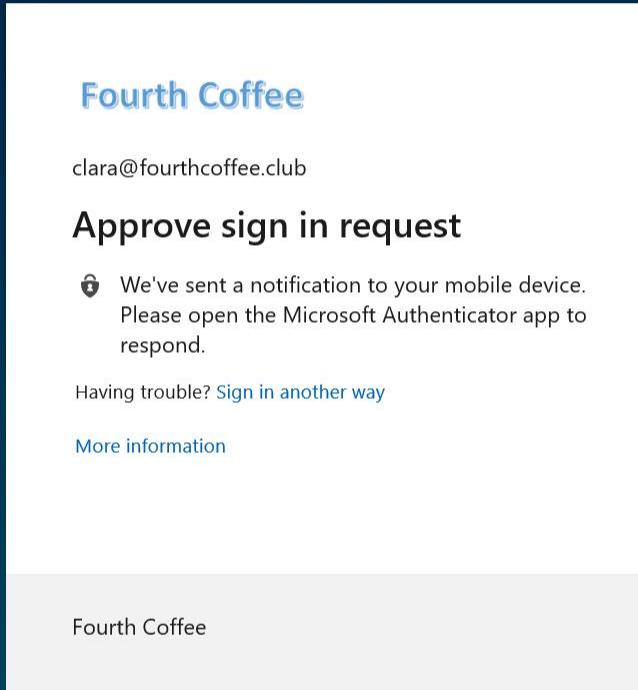
[Forgot my password](#)

Sign in

Fourth Coffee







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](#)

[Cancel](#)

Fourth Coffee

Microsoft Azure

Search resources, services, and docs (G+)

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

Identity Protection - Risky users

Search (Ctrl+ /) | Learn more | Download | Select all | Confirm user(s) compromised | Dismiss user(s) risk | Refresh | Columns | Got feedback?

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
<input type="checkbox"/> Dominic Jones	At risk	High	11/1/2019, 3:14:05 PM
<input checked="" type="checkbox"/> Clara Pinto	At risk	High	11/1/2019, 3:14:05 PM

Details

User's sign-ins User's risky sign-ins User's risk detections | Reset password Confirm user compromised Dismiss user risk Block user Investigate with Azure ATP

Basic info Recent risky sign-ins Detections not linked to a sign-in Risk history

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

Identity Protection - Risky users

 Search (Ctrl+/)Learn more Download Select all Confirm user(s) compromised Dismiss user(s) risk Refresh Columns Got feedback?

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
<input type="checkbox"/> Dominic Jones	At risk	High	11/1/2019, 3:14:05 PM
<input checked="" type="checkbox"/> Clara Pinto	At risk	High	11/1/2019, 3:14:05 PM

Details

User's sign-ins User's risky sign-ins User's risk detections Reset password Confirm user compromised Dismiss user risk Block user Investigate with Azure ATP

Basic info Recent risky sign-ins Detections not linked to a sign-in Risk history

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

Microsoft Azure

Search resources, services, and docs (G+)

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

Identity Protection - Risky users

Search (Ctrl+/)

Learn more Download Select all Confirm user(s) compromised Dismiss user(s) risk Refresh Columns Got feedback?

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
<input type="checkbox"/> Dominic Jones	At risk	High	11/1/2019, 3:14:05 PM
<input checked="" type="checkbox"/> Clara Pinto	At risk	High	11/1/2019, 3:14:05 PM

Risky users

Risky sign-ins

Risk detections

Vulnerabilities

Users at risk detected alerts

Weekly digest

Troubleshooting + Support

Troubleshoot

New support request

Details

User's sign-ins User's risky sign-ins User's risk detections | Reset password Confirm user compromised Dismiss user risk Block user Investigate with Azure ATP

Basic info Recent risky sign-ins Detections not linked to a sign-in Risk history

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+)

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\(s\) compromised](#) [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 (aggregate)	Risk level (real-time)
<input type="checkbox"/> 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
<input checked="" type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> 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
<input type="checkbox"/> 10/30/2019, 1:36:57 PM	Clara Pinto	Success	71.107.102.210	Kirkland, Washington, US	Windows 10	Chrome 77.0.3865	Remediated	-	Medium

Details

User's risk report User's sign-ins User's risky sign-ins User's risk detections Sign-in's risk detections Confirm sign-in compromised Confirm sign-in safe

Basic info Device info Risk info MFA info Conditional Access Report-only (Preview)

DETECTION TYPE	DETECTION RISK STATE	TIME DETECTED	DETECTION TIMING
Anonymous IP address ⓘ	Remediated	11/1/2019, 11:04 AM	Real-time
Risk level	Medium	Sign-in time 11/1/2019, 11:04 AM	Token issuer type Azure AD
Risk detail	User performed secured password change	IP address 85.10.51.86	
Source	Identity Protection	Sign-in location Zagreb, Grad Zagreb, HR	
Detection last updated	11/1/2019, 5:04 PM	Sign-in client Mozilla/5.0 (iPhone; CPU iPhone OS 13_1 like Mac OS X)	

Identity Protection – Risky sign-ins

Microsoft Azure

Search resources, services, and docs (G+)

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						
<input checked="" type="checkbox"/> 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...						
<input type="checkbox"/> 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...						
<input type="checkbox"/> 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...						
<input type="checkbox"/> 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...						
<input type="checkbox"/> 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...						
<input type="checkbox"/> 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...						
<input type="checkbox"/> 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...						
<input type="checkbox"/> 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...						
<input type="checkbox"/> 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...						
<input type="checkbox"/> 10/30/2019, 11:57:51 AM	Clara Pinto	37.120.143.222	Brussels, Brussels, BE	Anonymous IP address	Remediated	Medium	4f3ha711-80ed-48c7-aa36-c54...						

Details

User's risk report User's sign-ins User's risky sign-ins Linked risky sign-in User's risk detections

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

InPrivate Sign in to your account +

login.microsoftonline.com/login.srf?wa=wsignin1.0&rpsnv=4&ct=1470425754&rvei

CONTOSO

Sign in with your work or school account

sarad@contosobuild.com

••••••••••

Keep me signed in

Sign in

Can't access your account?

© 2016 Microsoft

Terms of use Privacy & Cookies

Microsoft

I'm Cortana. Ask me anything.

Sign in to your account +

https://login.microsoftonline.com/login.srf?wa=wsignin1.0&rpsnv=4&ct=1470425754&rvei

CONTOSO

Sign in with your work or school account

sarad@contosobuild.com

••••••••••

Keep me signed in

Sign in

Can't access your account?

© 2016 Microsoft

Terms of use Privacy & Cookies

Microsoft

InPrivate Sign in to your account +

login.microsoftonline.com/login.srf?wa=wsignin1.0&rpsnv=4&ct=1470427246&rvei

Sign in to your account

New Identity Ctrl+Shift+U
New Tor Circuit for this Site Ctrl+Shift+L
Tor circuit for this site (microsoftonline.com):
Privacy and Security Settings...
Tor Network Settings...
Check for Tor Browser Update...
This browser
Netherlands (84.245.32.195)
Canada (159.203.16.251)
Romania (109.163.234.2)
Internet

CONTOSO

Sign in with your work or school account

sarad@contosobuild.com

••••••••••

Keep me signed in

Sign in Back

Can't access your account?

Welcome EBC Attendees

© 2016 Microsoft Microsoft

Terms of use Privacy & Cookies

I'm Cortana. Ask me anything.

Windows Start button

Back Forward Stop Refresh Home Address Search

CONTOSO

Sign in to your account

https://login.microsoftonline.com/common/reprocess?prompt=select_account

Search

Sign in with your work or school account

sarad@contosobuild.com

••••••••••

Keep me signed in

Sign in

Can't access your account?

Welcome EBC Attendees

© 2016 Microsoft Microsoft

Terms of use Privacy & Cookies

The image shows a Microsoft Edge browser window with two tabs open. Both tabs have a background image of a field with several white wind turbines against a clear blue sky.

Left Tab (Active):

- Title Bar:** InPrivate, Sign in to your account, +
- Address Bar:** login.microsoftonline.com/login.srf?wa=wsignin1.0&rpsnv=4&ct=1470425754&rvei
- Content:** CONTOSO logo, "Sign in with your work or school account" text, email input field containing "sarad@contosobuild.com", password input field filled with dots, "Keep me signed in" checkbox, "Sign in" button, and "Can't access your account?" link.
- Bottom:** Welcome EBC Attendees, Microsoft logo, © 2016 Microsoft, Terms of use, Privacy & Cookies links, and a Cortana search bar.

Right Tab:

- Title Bar:** Sign in to your account, +
- Address Bar:** https://login.microsoftonline.com/common/login
- Content:** CONTOSO demo logo, "Your account is blocked" message, "We've detected suspicious activity on your account. Please contact your admin. More details" link, and "Sign out and sign in with a different account" link.

InPrivate

Office Admin center pre +

portal.office.com/AdminPortal/Home?switchtomoderndefault=true#/homepage

Admin center preview

Sara Davis

Home

Contoso Cloud

Search users, groups, settings or tasks

Go to the old admin center

Grow your business

Fill out your Bing places for business profile to help customers find yo

Edit profile

Users >

- + Add a user
- Delete a user
- >Edit a user
- Reset a password

Billing >

Total balance \$0.00

- Change payment details
- View my bill

Office software

- Install my software
- Share the download link
- Software download settings
- Troubleshoot installation

Need help? Feedback

I'm Cortana. Ask me anything.



Sign in to your account

https://login.microsoftonline.com/common/login

CONTOSO demo

Your account is blocked

We've detected suspicious activity on your account. Please contact your admin. [More details](#)

Sign out and sign in with a different account