

# CONDITIONAL ACCESS POLICY TO USE MFA



Resources

Billing

Support

Settings

Domains

Search & intelligence

Org settings

Integrated apps

Directory sync errors

Partner relationships

Setup

Reports

Health

Admin centers

Services

Security & privacy

Organization profile

Name ↑

Description



Microsoft Planner

Choose whether your users can publish plans and assigned



Microsoft Search in Bing homepage

Customize Bing.com page for your signed-in users.



Microsoft Teams

Manage and update your Microsoft Teams settings.



Microsoft To Do

Manage and update your To Do settings.



Microsoft Viva Insights (formerly MyAnalytics)

Manage and update Microsoft Viva Insights (formerly MyA



Microsoft 365 Groups

Manage external sharing.



Modern authentication

Change Exchange Online authentication settings for your e



Multi-factor authentication

Manage multi-factor authentication settings for your users



## **Multi-factor authentication**

Multi-factor authentication provides a second layer of security by requiring users to sign in with more than just their username and password.

[Configure multi-factor authentication](#)

[Learn more about Azure multi-factor authentication](#)

bulk update

View: Sign-in allowed users Multi-Factor Auth status: Any

<input type="checkbox"/>	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	Abbi Skinner	Abbi@M365x21744547.onmicrosoft.com	Disabled
<input checked="" type="checkbox"/>	Abbie Parsons	Abbie@M365x21744547.onmicrosoft.com	Disabled
<input checked="" type="checkbox"/>	Abigail Rees	Abigail@M365x21744547.onmicrosoft.com	Disabled
<input type="checkbox"/>	Ada Russell	Ada@M365x21744547.onmicrosoft.com	Disabled
<input type="checkbox"/>	Adam Hobbs	Adam@M365x21744547.onmicrosoft.com	Disabled
<input type="checkbox"/>	AdatumAdmin	AdatumAdmin@M365x21744547.onmicrosoft.com	Disabled
<input type="checkbox"/>	Adeline Snyder	Adeline@M365x21744547.onmicrosoft.com	Disabled

2 selected

quick steps

Enable

Manage user settings



### About enabling multi-factor auth

Please read the [deployment guide](#) if you haven't already.

If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: <https://aka.ms/MFASetup>



### Updates successful

Multi-factor auth is now enabled for the selected accounts.



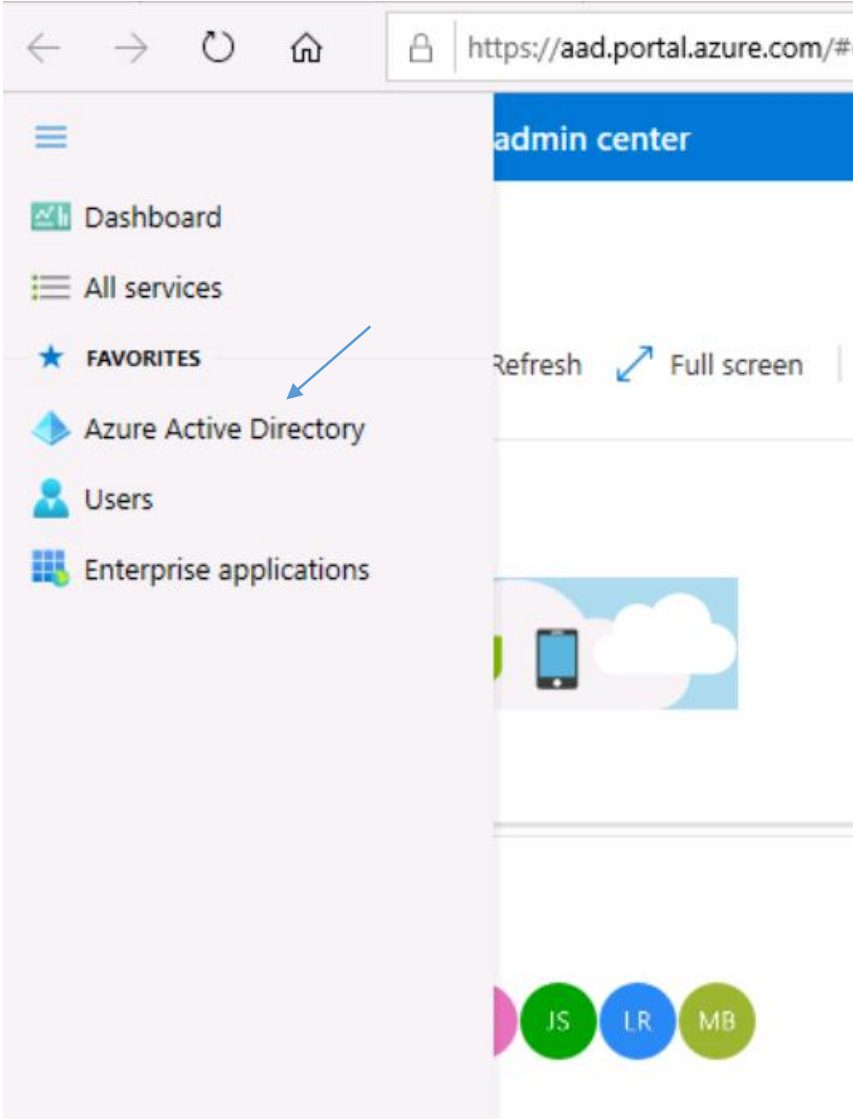
### Manage user settings

- Require selected users to provide contact methods again
- Delete all existing app passwords generated by the selected users
- Restore multi-factor authentication on all remembered devices

save

cancel

# Conditional Multifactor Authentication



The image shows a browser window displaying the Azure AD Admin Center. The address bar shows the URL `https://aad.portal.azure.com`. The page title is "admin center". A "Portal menu" is open on the left side, listing various administrative options. The "Security" option is highlighted with a blue arrow. Below the "Security" option is a section titled "Monitoring" which includes "Sign-in logs".

admin center

Portal menu

view ...

- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Security

**Monitoring**

- Sign-in logs

The image shows a screenshot of the Microsoft Entra admin center portal menu. The menu is displayed on the left side of the screen, with a blue header bar at the top containing a hamburger menu icon and the text "admin center". Below the header, there is a "Portal menu" section with a back arrow icon. A search bar is present with the placeholder text "Search (Ctrl+ /)". The menu items are organized into sections: "Getting started" (highlighted in light blue), "Protect" (with a blue arrow pointing to "Conditional Access"), and "Manage". The "Protect" section includes "Conditional Access", "Identity Protection", "Security Center", and "Verifiable credentials (Preview)". The "Manage" section includes "Identity Secure Score", "Named locations", and "Authentication methods". On the right side of the screen, the text "ing started" is visible, and a vertical scrollbar is present. A blue box highlights the "admin center" text in the top right corner.

admin center

← Portal menu

Search (Ctrl+ /)

Getting started

**Protect**

- Conditional Access
- Identity Protection
- Security Center
- Verifiable credentials (Preview)

**Manage**

- Identity Secure Score
- Named locations
- Authentication methods


ing started



[Dashboard](#) > [Contoso](#) > [Security](#) > [Conditional Access](#)

## Conditional Access | Policies ...

Azure Active Directory

[+](#) New policy  [What If](#) | [Got feedback?](#)

Create new policy 

Create new policy from templates (Preview)

Force access requirements when specific conditions occur. Let's take a few examples

Conditions	Controls
When any user is outside the company network	They're required to sign in with multi-factor authentication
When users in the 'Managers' group sign-in	They are required be on an Intune compliant or domain-joined device

[Want to learn more about Conditional Access?](#)

### Get started

- Create your first policy by clicking "+ New policy"
- Specify policy Conditions and Controls
- When you are done, don't forget to Enable policy and Create

[Interested in common scenarios?](#)

---



[Dashboard](#) > [Contoso](#) > [Security](#) > [Conditional Access](#) >

## New ...

Conditional Access policy

Name \*

MFA policy conditional 

Assignments

Users or workload identities 

0 users or workload identities selected

Enable policy

**Report-only** On Off



Do not block yourself out! This policy impacts the Azure portal and other clients that do not support CAE today.

Create



Dashboard > Contoso > Security > Conditional Access >

## New ...

Conditional Access policy

### Assignments

Users or workload identities ⓘ

All users

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication


**Include** Exclude

- None
- All users
- Select users and groups

All guest and external users ⓘ

Enable policy

Report-only On Off

 Do not block yourself out! This policy impacts the Azure portal and other clients that do not support CAE today.

Create



Dashboard > Contoso > Security > Conditional Access >

## New ...

Conditional Access policy

### Assignments

Users or workload identities ⓘ

All users

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication

Include **Exclude**

Select the users and groups to exempt from the policy

All guest and external users ⓘ

Directory roles ⓘ

Enable policy

Report-only

On

Off



Do not block yourself out! This policy impacts the Azure portal and other clients that do not support CAE tod

Create



Dashboard > Contoso > Security > Conditional Access >

## New ...

Conditional Access policy

Users or workload identities ⓘ

All users included and specific users excluded

✘ "Select users and groups" must be configured

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication

Enable policy

Report-only On Off

⚠ Do not block yourself out! This policy impacts the Azure portal and other

Select the users and groups for the policy

All guest and

Directory role

Users and groups

## Select excluded users

Users and groups

Search



Alex Wilber

AlexW@M365x177088.OnMicrosoft.com



All Company

allcompany@M365x177088.onmicrosoft.com



Allan Deyoung

AllanD@M365x177088.OnMicrosoft.com



Diego Siciliani

DiegoS@M365x177088.OnMicrosoft.com



Isaiah Langer

- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

Dashboard > Contoso > Security

### Contoso | S...

Azure Active Directory

- Overview
- Preview features
- Diagnose and solve problems

#### Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations

## Select excluded users

Users and groups

Search

- Joni Sherman  
JoniS@M365x177088.OnMicrosoft.com
- Lynne Robbins  
LynneR@M365x177088.OnMicrosoft.com  
Selected
- Megan Bowen  
MeganB@M365x177088.OnMicrosoft.com
- Microsoft Service Account  
ms-serviceaccount@M365x177088.OnMicrosoft.com
- MOD Administrator  
admin@M365x177088.onmicrosoft.com
- Nestor Wilke

Select

- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

Dashboard > Contoso > Security > Conditional Access >

## New

Conditional Access policy

### Assignments

Users or workload identities ⓘ

All users included and specific users excluded

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Sign-in risk ⓘ

Not configured

Device platforms ⓘ

Not configured

Locations ⓘ

Not configured

Client apps ⓘ

Not configured

Enable policy

Report-only On Off

⚠ Do not block yourself out! This policy impacts the Azure portal and other clients that do not support CAE today.

Create

Dashboard

All services

FAVORITES

Azure Active Directory

Users

Enterprise applications

Dashboard > Contoso > Security > Conditional Access >

## New

Conditional Access policy

policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*

MFA policy conditional

Assignments

Users or workload identities ⓘ

All users included and specific users excluded

apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps

**Include** Exclude

- None
- All cloud apps
- Select apps

Enable policy

Report-only On Off

⚠ Do not block yourself out! This policy impacts the Azure portal and other clients that do not support CAE today.

Create



- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

Dashboard > Contoso > Security > Conditional Access >

## New

Conditional Access policy

Name \*

MFA policy conditional ✓

Cloud apps

Include **Exclude**

Select the cloud apps to exempt from the policy

Assignments

Users or workload identities ⓘ

All users included and specific users excluded

Select excluded cloud apps

Cloud apps or actions ⓘ

All cloud apps

None

Enable policy

Report-only On Off

⚠️ Do not block yourself out! This policy impacts the Azure portal and other clients that do not support C

Create

- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

Dashboard > Contoso > Security > Conditional Access >

# New

Conditional Access policy

Name \*

MFA policy conditional ✓

Assignments

Users or workload identities ⓘ

All users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Enable policy

Report-only On Off

⚠ Do not block yourself out! This policy impacts the Azure porta

Create

Cloud apps

Include

Select the c policy

Select exclu

None

## Select excluded cloud apps

Cloud apps

Search

- Common Data Service 00000007-0000-0000-c000-000000000000
- DX dxprovisioning-graphapi-client 88a5feff-3213-408f-ab93-fdb7a3f4847b
- DX dxprovisioning-worker-mfa 24bc1ec9-9b62-4426-aaaa-b65021d4401c

### Selected items

- DX dxprovisioning-worker-mfa 24bc1ec9-9b62-4426-aaaa-b65021d4401c Remove

Select

- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

## New

Conditional Access policy

Cloud apps or actions ⓘ

All cloud apps included and 1 app excluded

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Select excluded cloud apps

[dxprovisioning-worker-mfa](#)

**DX** dxprovisioning-worker-mfa  
24bc1ec9-9b62-4426-aaaa-b65021d44...

Enable policy

**Report-only** On Off

**⚠** Do not block yourself out! This policy impacts the Azure portal and other clients that do not support CAE today.

Create

- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

Dashboard > Contoso > Security > Conditional Access >

## New

Conditional Access policy

Cloud apps or actions ⓘ

All cloud apps included and 1 app excluded

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Enable policy

Report-only On Off

⚠ Do not block yourself out! This policy impacts the Azure portal and other clients that

Create

## Grant

Control access enforcement to block or grant access. [Learn more](#)

- Block access
- Grant access
- Require multi-factor authentication ⓘ
- Require device to be marked as compliant ⓘ
- Require Hybrid Azure AD joined device ⓘ
- Require approved client app ⓘ [See list of approved client apps](#)
- Require app protection policy ⓘ [See list of policy protected client apps](#)

Select



- My Dashboard
- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

Dashboard > Contoso > Security > Conditional Access >

## New

Conditional Access policy

Cloud apps or actions ⓘ

All cloud apps included and 1 app excluded

Conditions ⓘ

0 conditions selected

Enable policy

Report-only  On  Off

**⊗** Don't lock yourself out! We recommend applying a policy to a small set of users first to verify it behaves as expected. We also recommend excluding at least one administrator from this policy. This ensures that you still have access and can update a policy if a change is required. Please review the affected users and apps.

- Exclude current user, admin@M365x177088.onmicrosoft.com, from this policy.
- I understand that my account will be impacted by this policy. Proceed anyway.

**⚠** Do not block yourself out! This policy impacts the Azure portal and other clients that do not support CAE today.