



MULTIFACTOR AUTHENTICATION WITH AZURE CONDITIONAL ACCESS

Authentication in Azure



BY
TIMOTHY FABELURIN

Multifactor Authentication

This is a process where user is required to provide an additional form of identification when signing in. Security is increased when this second form of identity is not easy for an attacker to obtain. For example, fingerprint scan, mobile phone code.

With MFA enabled and enforced using conditional access policies, cloud-based applications access was restricted, and all affected users need to authenticate with either SMS, Phone call or Microsoft Authentication App in conjunction with their passwords. Conditional access policy can be applied to only provide access at a particular location or range of IP address or operating system (windows, ios, android, macOS etc). With this measure in place, security is enhanced on the platform.

1. Below indicates different available policy templates that can be implemented.

Care must be taken however, in ensuring that there is an account that can be used to salvage a scenario of total lockout of the platform due to configuration error.

Microsoft Azure

Home > Conditional Access | Policies >

Create new policy from templates (Preview)

Got feedback?

Customize your build **Select template** Review + create

We recommend the following templates based on your response

- ☐ Require multifactor authentication for admins
Require multifactor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as Security Default.
[View policy summary](#)
- ☐ Securing security info registration
Secure when and how users register for Azure AD multifactor authentication and self-service password.
[View policy summary](#)
- ☐ Block legacy authentication
Block legacy authentication endpoints that can be used to bypass multifactor authentication.
[View policy summary](#)
- ☒ **Require multifactor authentication for all users**
Require multifactor authentication for all user accounts to reduce risk of compromise.
[View policy summary](#)
- ☐ Require multifactor authentication for guest access
Require guest users perform multifactor authentication when accessing your company resources.
[View policy summary](#)
- ☐ Require multifactor authentication for Azure management
Require multifactor authentication to protect privileged access to Azure resources.
[View policy summary](#)
- ☐ Require multifactor authentication for risky sign-ins
Require multifactor authentication if the sign-in risk is detected to be medium or high. (Requires an Azure AD Premium 2 License)
[View policy summary](#)

☐ View policy summary
Require password change for high-risk users
Require the user to change their password if the user risk is detected to be high. (Requires an Azure AD Premium 2 License)
[View policy summary](#)

Name your policy
CA004- Require multifactor authentication for all users

Policy state
☐ Off ☒ On ☐ Report-only

⚠ Enabling this policy will enforce multifactor authentication for all your users.
Consideration: Enabling this policy will enforce multifactor authentication for all users.

Create Policy Previous Next

2. Across the whole tenant (Cloud environment), It is possible to individually or collectively either disable, enable, or enforce MFA on users by the admin. General settings was also set up. For instance, "Trusted IP ranges" and verification methods can be configured.

Microsoft fabbiety_gmail.com#EXT#@fabbietygmail.onmicrosoft.com ?

multi-factor authentication

users service settings

Starting Sept. 30th, 2022 Combined registration experiences for MFA and SSPR will be enabled for all tenants. Enable it now. Before you begin, take a look at the multi-factor auth deployment guide.

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

<input type="checkbox"/>	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	315211e9-307b-462f-98da-54	fabbiety@gmail.com	Disabled
<input type="checkbox"/>	Arkie Angel	areathy33@gmail.com	Enabled
<input type="checkbox"/>	gbenz	gbenz@fabbietygmail.onmicrosoft.com	Disabled
<input type="checkbox"/>	ham	ham@fabbietygmail.onmicrosoft.com	Disabled
<input type="checkbox"/>	team	team@fabbietygmail.onmicrosoft.com	Enforced
<input type="checkbox"/>	Tim	Tim@fabbietygmail.onmicrosoft.com	Enabled
<input type="checkbox"/>	tope	tope@fabbietygmail.onmicrosoft.com	Disabled

Select a user

©2022 Microsoft Legal Privacy

Microsoft fabbiety_gmail.com#EXT#@fabbietygmail.onmicrosoft.com ?

multi-factor authentication

users service settings

Starting Sept. 30th, 2022 Combined registration experiences for MFA and SSPR will be enabled for all tenants. Enable it now. app passwords [\(learn more\)](#)

☒ Allow users to create app passwords to sign in to non-browser apps
☐ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(learn more\)](#)

☐ Skip multi-factor authentication for requests from federated users on my intranet
Skip multi-factor authentication for requests from following range of IP address subnets

192.168.1.0/27
192.168.1.0/27
192.168.1.0/27

I

verification options [\(learn more\)](#)

Methods available to users:

- ☒ Call to phone
- ☒ Text message to phone
- ☒ Notification through mobile app
- ☒ Verification code from mobile app or hardware token

remember multi-factor authentication on trusted device [\(learn more\)](#)

☒ Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)
Number of days users can trust devices for:

NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' be sure to extend the duration to 90 or more days. [Learn more about reauthentication prompts.](#)

3. MFA is often used in conjunction with Conditional access. The conditional access policy provide different security settings options by which if any of the conditions are met, there system triggers one or couple of actions before authentication is passed.

Home > Conditional Access

Conditional Access | Policies

Azure Active Directory

Overview (Preview) Policies Insights and reporting Diagnose and solve problems

Manage

- Named locations
- Custom controls (Preview)
- Terms of use
- VPN connectivity
- Authentication context (Preview)
- Classic policies

Monitoring

- Sign-in logs
- Audit logs

Troubleshooting + Support

- Virtual assistant (Preview)
- New support request

What is Conditional Access?

Conditional Access gives you the ability to enforce 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 multifactor 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?

Conditional access policy page on Azure Portal

4. There are diffent levels of decisions that need to be made and this has a lot to do with the organisational policies. Few of those include,
- Types of users – Guest users, all users or specific users
 - Applications to effect this policy on – Office 365, Azure, Power analytics etc
 - Conditions – Places consider as "High-risk" locations, IP address out the Trusted range, types of devices (ios, windows, mac etc), State of device (Domain joined, hybrid joined etc)

- iv. Access Control – This is the point decision to either Grant or Block is decided and what more measure are needed for authentication to be passed.

Below images shows few steps taken when configuring the test scenario.

The screenshot shows the 'New' Conditional Access policy configuration page in the Azure portal. The page is divided into several sections for configuring the policy:

- Name:** All user Authentication (checked)
- Assignments:** Users or workload identities (Specific users included and specific users excluded)
- Cloud apps or actions:** All cloud apps
- Conditions:** 1 condition selected. With "Selected locations" you must choose at least one location.
- Access controls:** Grant (0 controls selected)
- Session:** 0 controls selected

The right-hand side of the page shows the configuration for the selected condition, specifically the 'Locations' section. It includes a 'Configure' toggle set to 'Yes', and a 'Select' dropdown menu with options: 'None' and 'Choose at least one location'.

The 'Select' dialog box is open, showing a table of locations:

Name	Location type	Trusted
Multifactor authentication trusted IPs	IP ranges	Yes

Home > Conditional Access | Policies >

New Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
All user Authentication ✓

Assignments

Users or workload identities ⓘ
Specific users included and specific users excluded

Cloud apps or actions ⓘ
All cloud apps

Conditions ⓘ
3 conditions selected

Access controls

Grant ⓘ
0 controls selected

Session ⓘ
0 controls selected

User risk level ⓘ
1 included

Sign-in risk level ⓘ
1 included

Device platforms ⓘ
Not configured

Locations ⓘ
Any location and 1 excluded

Client apps ⓘ
Not configured

Filter for devices ⓘ
Not configured

Filter for devices

Configure a filter to apply policy to specific devices. [Learn more](#)

Configure ⓘ
Yes No

Devices matching the rule:
☒ Include filtered devices in policy
☐ Exclude filtered devices from policy

You can use the rule builder or rule syntax text box to create or edit the filter rule.

And/Or	Property	Operator	Value
And	<Choose a property>	<Choose an operator>	<Pick a property and operator first>
			<Pick a property and operator first>

+ Add expression

Rule syntax ⓘ

Home > Conditional Access | Policies >

New Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *
All user Authentication ✓

Assignments

Users or workload identities ⓘ
Specific users included and specific users excluded

Cloud apps or actions ⓘ
All cloud apps

Conditions ⓘ
3 conditions selected

Access controls

Grant ⓘ
0 controls selected

Session ⓘ
0 controls selected

Grant ⓧ

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

☐ Block access
☒ Grant access

☒ Require multifactor 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
☐ Require password change ⓘ

For multiple controls
☒ Require all the selected controls
☐ Require one of the selected controls

- Using a user (tim@fabbietygmail.onmicrosoft.com) in the tenant as a use case, additional verification information was required at the instance of login into azure application, being the first time after the settings were effected.

Microsoft

Additional security verification

Secure your account by adding phone verification to your password. [View video](#) to know how to secure your account.

Step 1: How should we contact you?

Authentication phone ▼

United Kingdom (+44) ▼ 74237

Method

☒ Send me a code by text message

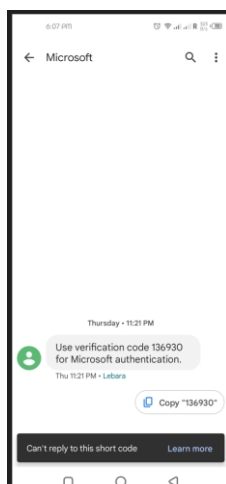
☐ Call me

Next

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2022 Microsoft Legal Privacy

6. Text message for verification code from microsoft as that was te choice of verification method selected. This is required for a successful authentication even after the user has provided correct password.



Microsoft Azure


Search resources, services, and docs (0/0)

Tim@fabbietygmail.com...
Create a new resource

Sign out

Welcome to Azure!


Don't have a subscription? Check out the following options.



Start with an Azure free trial

Get \$200 free credit toward Azure products and services, plus 12 months of popular free services.


[Start](#) [Learn more >](#)



Manage Azure Active Directory

Manage access, set smart policies, and enhance security with Azure Active Directory.

[View](#) [Learn more >](#)



Access student benefits

Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status.

[Explore](#) [Learn more >](#)

Azure services

Create a resource

Quickstart Center

Virtual machines

App Services

Storage accounts

SQL databases

Azure Cosmos DB

Kubernetes services

Function App

More services

Resources

Recent

Favorite

Name	Type	Last Viewed
<div>No resources have been viewed recently</div> <div>View all resources</div>		