



# Microsoft Entra

## The Comprehensive Guide to Secure Azure AD & User Identities

By: Mohamed Mokhtar

<https://mokhtar.cloud>

version: 1.2

Updated February 2023

## Contents

1) Define at least two emergency access accounts .....	3
2) Require multifactor authentication for administrative roles .....	14
3) Ensure all Users can complete multifactor authentication .....	18
4) Do not allow Users to grant consent to unreliable applications .....	19
5) Enable Self-Service Password Reset .....	20
6) Ensure that password protection is Enabled for Active Directory .....	21
7) Enable Conditional Access policies to block legacy authentication.....	22
8) Ensure that password hash sync is Enabled for hybrid deployments .....	24
9) Enable Azure AD Identity Protection sign-in risk policies.....	25
10) Enable Azure AD Identity Protection User risk policies .....	26
11) Use Just in Time privileged access to Office 365 roles .....	27
12) Ensure Security Defaults are disabled on Azure AD .....	34
13) Ensure that LinkedIn contact synchronization is disabled.....	35
14) Ensure Sign-in frequency is Enabled, and browser sessions are not persistent for Administrative Users. ....	36
15) Ensure the option to remain signed in is hidden.....	38
16) Do not expire passwords .....	39
17) Ensure Administrative accounts are separate and cloud-only .....	40
18) Passwordless sign-in with the Microsoft Authenticator app.....	41
19) Passwordless: Windows Hello for Business.....	42
20) New feature: Azure AD Authentication Strengths (Preview) .....	50
21) Regularly Check identity secure score .....	54
22) Require trusted location for MFA and SSPR registration .....	55
23) Tenant restrictions.....	58
24) Conditional Access filters for apps.....	60
25) Prevent Users from creating Azure AD tenant .....	63

# 1) Define at least two emergency access accounts

Emergency access accounts are highly privileged, and they are not assigned to specific individuals. Emergency access accounts are limited to emergency or “break glass” scenarios where normal administrative accounts can’t be used.

## Create two or more emergency access accounts.

These accounts should be cloud-only accounts that use the \*.onmicrosoft.com domain and that are not federated or synchronized from an on-premises environment

1. Log in to <https://entra.microsoft.com/>
2. Create Two admin accounts with Global Admin permission
3. Store account credentials safely, if using passwords, make sure the accounts have strong passwords that do not expire the password. Ideally, the passwords should be at least 16 characters long and randomly generated.

You should monitor sign-in activity from the emergency account, by following the below we will use Azure Log Analytics to monitor the sign-in log from the emergency account and it will trigger email and SMS to admin people whenever break glass account sign-in.

## Send Azure AD Sign-in Logs to Azure Monitor

1. Create a **Log Analytics workspace**
2. In the [Azure portal](#), enter **Log Analytics** in the search box. As you begin typing, the list filters based on your input. Select **Log Analytics workspaces**.

The screenshot shows the Azure portal interface for creating a Log Analytics workspace. At the top, there's a search bar with 'log analytics' typed in. Below the search bar, a navigation bar includes 'Home', 'Log Analytics workspace', and other links like 'Services (16)', 'Marketplace (7)', 'Documentation (28)', and 'Azure'. A sidebar on the left shows 'Create Log Analy...' and tabs for 'Basics', 'Tags', and 'Review +'. The main area is titled 'Create Log Analytics workspace' and shows two options: 'Log Analytics query packs' and 'Log Analytics workspaces'. The 'Log Analytics workspaces' option is highlighted with a yellow background. Below these options, a note says 'A Log Analytics workspace is required to receive sign-in logs.' At the bottom of the page, there's a large blue button labeled 'Click Create'.

The screenshot shows the 'Create Log Analytics workspace' page in the Microsoft Azure portal. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below it, the breadcrumb navigation shows 'Home > Log Analytics workspaces > Create Log Analytics workspace'. The main section is titled 'Create Log Analytics workspace' with a '...' button. Below this, there are three tabs: 'Basics' (which is selected), 'Tags', and 'Review + Create'. A note box states: 'A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. [Learn more](#)'.

**Project details**  
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* (dropdown menu)  
Resource group \* (dropdown menu): (New) RG-LogAnalytics  
Create new

**Instance details**  
Name \* (input field): LogAnalytics  
Region \* (dropdown menu): North Europe

- Azure Log Analytics workspace created.
- Then from the Entra Admin Centre go to **Azure Active Directory > Monitoring & Health > Diagnostic settings** -> **Add diagnostic setting**. You can also select **Export Settings** from the **Audit Logs** or **Sign-ins** page to get to the diagnostic settings configuration page.
- In the **Diagnostic settings** menu, select the **Send to Log Analytics workspace** check box and then select **Configure**.

Home > Mo | Diagnostic settings >

### Diagnostic setting ...

The screenshot shows the 'Diagnostic setting' blade for 'AzureADLogs'. In the 'Logs' section, 'AuditLogs' and 'SignInLogs' are selected. In the 'Destination details' section, 'Send to Log Analytics workspace' is checked, and the 'Subscription' dropdown is set to 'LogAnalytics (northeurope)'. Other options like 'Archive to a storage account', 'Stream to an event hub', and 'Send to partner solution' are also listed.

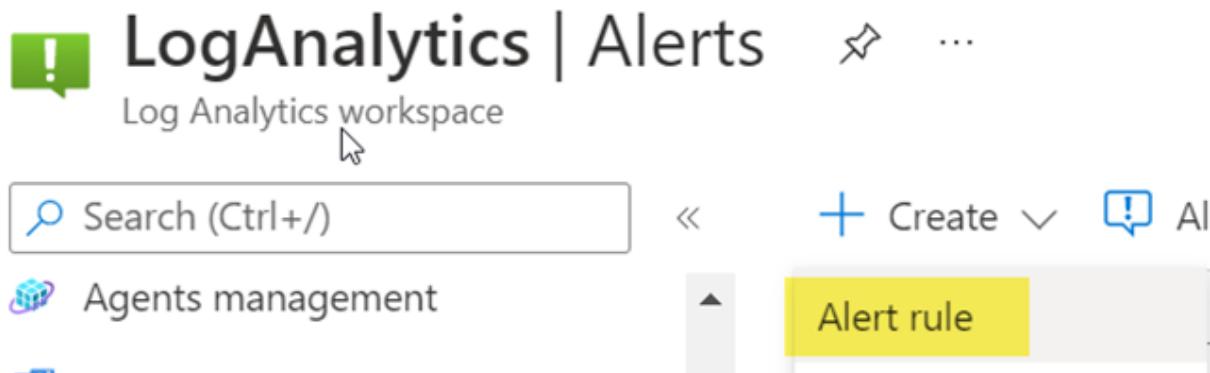
### Obtain Object IDs of the break glass accounts

1. Sign in to the Entra Admin Centre with an account assigned to the User Administrator role.
2. Select **Azure Active Directory > Users > All Users**.
3. Search for the break-glass account and select the user's name.
4. Copy and save the Object ID attribute so that you can use it later.
5. Repeat previous steps for second break-glass account.

User principal name	@elshreef.net	
Object ID	da8eb00b-5649-426f-992a-d9771d98465e	
Created date time	May 30, 2022, 6:16 PM	
User type	Member	

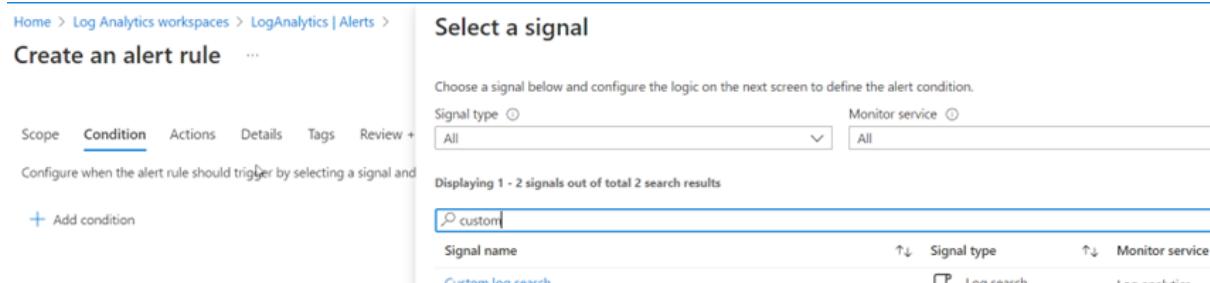
### Create an alert rule

1. Sign in to the [Azure portal](#) with an account assigned to the Monitoring Contributor role in Azure Monitor.
2. Select **All services**, enter “log analytics” in Search and then select **Log Analytics workspaces**.
3. Select a workspace which you created earlier.
4. In your workspace, select **Alerts > New alert rule**.



The screenshot shows the Azure Log Analytics workspace interface. At the top, there's a navigation bar with a search bar, a 'Create' button, and an 'AI' icon. Below the navigation, there's a sidebar with 'Agents management' and a main area titled 'Log Analytics workspace'. On the right side, there's a prominent yellow button labeled 'Alert rule'.

- Under **Resource**, verify that the subscription is the one with which you want to associate the alert rule.
  - Under **Condition**, select **Add**.
  - Select **Custom log search** under **Signal name**.



The screenshot shows the 'Create an alert rule' wizard, step 2: 'Select a signal'. It displays a search results table for 'custom' signals. The table has columns for 'Signal name', 'Signal type', and 'Monitor service'. One row is visible, labeled 'Custom log search'.

- Under **Search query**, enter the following query, inserting the object IDs of the two break glass accounts.

// Search for multiple Object IDs (UserIds)

SigninLogs

```
| project UserId
```

```
| where UserId == "f66e7317-2ad4-41e9-8238-3acf413f7448" or UserId ==
"0383eb26-1cbc-4be7-97fd-e8a0d8f4e62b"
```



The screenshot shows the Log Analytics workspace with a query editor. The query is:

```
1 // Search for multiple Object IDs (UserIds)
2 SigninLogs
3 | project UserId
4 | where UserId == "da8eb00b-5649-426f-992a-d9771d98465e" or UserId == "00e8935c-af48-41f0-990a-e068823ce"
```

Then click continue editing

Under **Alert logic**, enter the following:

- Based on: Number of results
- Operator: Greater than
- Threshold value: 0

**Log query** 

The query to run on this resource's logs. The results returned by this query are used to populate the alert definition below.

Search query \*

```
// Search for multiple Object IDs (UserIds)
SigninLogs
| project UserId
| where UserId == "da8eb00b-5649-426f-992a-d9771d98465e" or UserId == "00e8935c-af48-41f0-990a-e068823ce3c7"
```

 This query doesn't return an Azure resource ID column, so the alert will fire on the entire rule scope [Learn more](#)

[View result and edit query in Logs](#) 

#### Measurement

Select how to summarize the results. We try to detect summarized data from the query results automatically.

Measure 	Table rows 
Aggregation type 	Count 
Aggregation granularity 	5 minutes 

#### Split by dimensions

Resource ID column 	Don't split 
--	---

Use dimensions to monitor specific time series and provide context to the fired alert. Dimensions can be either number or string columns. If you select more than one dimension value, each time series that results from the combination will trigger its own alert and will be charged separately. 

Dimension name	Operator	Dimension values	Include all future values
Select dimension 	= 	0 selected  Add custom value 	<input type="checkbox"/>
<b>Alert logic</b>			
Operator * 	Greater than 		
Threshold value * 	0 		
Frequency of evaluation * 	5 minutes 		

 Estimated monthly cost \$1.50 (USD)

 Advanced options

Then select Done

1. Select **Create an action group**.
2. Enter the action group name and a short name.
3. Verify the subscription and resource group.
4. Under action type, select **Email/SMS/Push/Voice**.
5. Enter an action name such as **Notify global admin**.

6. Select the **Action Type** as **Email/SMS/Push/Voice**.
7. Select **Edit details** to select the notification methods you want to configure and enter the required contact information, and then select **Ok** to save the details.
8. Add any additional actions you want to trigger.
9. Select **OK**.

Home > Log Analytics workspaces > LogAnalytics | Alerts > Create an alert rule >  
Create an action group ...

Basics Notifications Actions Tags Review + create

#### Notifications

Choose how to get notified when the action group is triggered. This step is optional.

Notification type	Name	Selected
Email/SMS message/Push/Voice		Selected

Email/SMS message/Push/Voice  
Add or edit an Email/SMS/Push/Voice action

Email  
Email \*

SMS (Carrier charges may apply)  
Country code \*

Azure mobile app notification  
Azure account email

Voice  
Country code   
Phone number

Enable the common alert schema. [Learn more](#)

Yes  No

**OK**

Then review and create

[Home](#) > [Log Analytics workspaces](#) > [LogAnalytics | Alerts](#) >

## Create an alert rule

[Scope](#)   [Condition](#)   **Actions**   [Details](#)   [Tags](#)   [Review + create](#)

An action group is a set of actions that can be applied to an alert rule. [Learn more](#)

[+ Select action groups](#)   [+ Create action group](#)

Action group name

Contains actions

Break-Glass-AG

1 Email, 1 SMS message

---

[Review + create](#)

[Previous](#)

[Next: Details >](#)

- To customize the email notification sent to the members of the action group, select actions under **Customize Actions**.
- Under **Alert Details**, specify the alert rule name and add an optional description.
- Set the **Severity level** of the event. We recommend that you set it to **Critical(Sev 0)**.
- Under **Enable rule upon creation**, leave it set as **yes**.
- To turn off alerts for a while, select the **Suppress Alerts** check box and enter the wait duration before alerting again, and then select **Save**.
- Click **Create alert rule**.

Home > Log Analytics workspaces > LogAnalytics | Alerts >

## Create an alert rule

Scope Condition Actions **Details** Tags Review + create

### Project details

Select the subscription and resource group in which to save the alert rule.

Subscription \* ⓘ

Resource group \* ⓘ

RG-BG-01

Create new

### Alert rule details

Severity \* ⓘ

0 - Critical

Alert rule name \* ⓘ

Emergency Access

Alert rule description ⓘ

Region \* ⓘ

North Europe

Advanced options

Then select Review and Create

Home > Log Analytics workspaces > LogAnalytics | Alerts >

## Create an alert rule

...

Scope Condition Actions Details Tags [Review + create](#)

### Product Details

Log alerts  
1 Condition  
[Terms of use](#) | [Privacy statement](#)

Total pricing

\$1.50

[Pricing](#)

### Scope

Resource

VPN MSDN Platforms > RG-BG-01 > LogAnalytics

### Condition

#### Search query

Measure  
Aggregation type  
Aggregation granularity

Table rows

Count

5 minutes

### Advanced options

Resource ID column

don't Split

### Alert logic

Operator  
Threshold value  
Frequency of evaluation

Greater Than

5 minutes

### Advanced options

Number of violations  
Evaluation period

1 violations

5 minutes (1 aggregated points)

### Actions

Action group name  
Break-Glass-AG

Contain actions

1 Email, 1 SMS message



### Details

#### Project details

Subscription  
Resource group  
Region

VPN MSDN Platforms

RG-BG-01

northeurope

#### Alert rule details

Severity  
Alert rule name  
Alert rule description

0 - Critical

Emergency Access

#### Advanced options

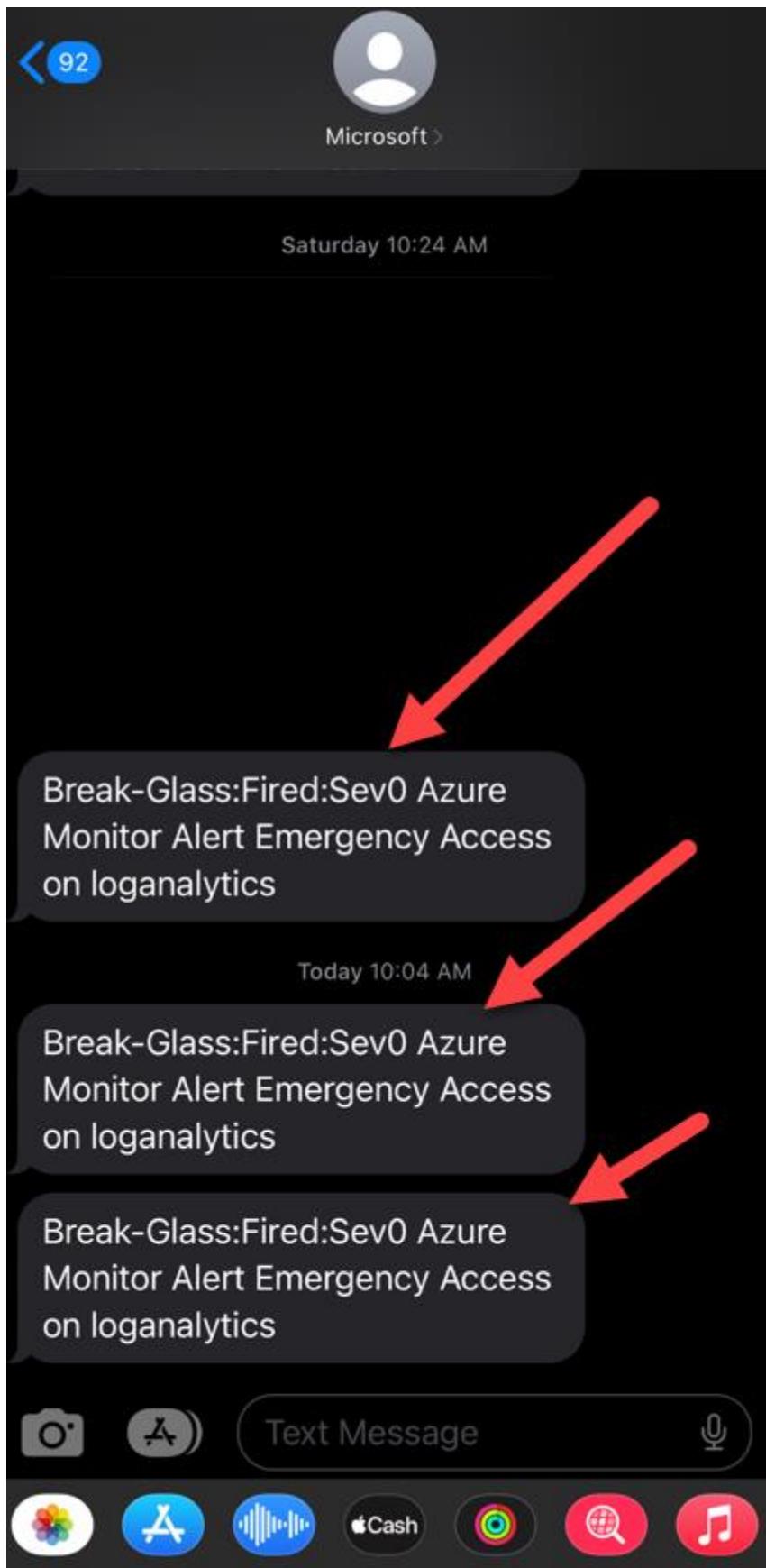
Enable upon creation  
Automatically resolve alerts (preview)  
Require a workspace linked storage



[Create](#)

[Previous](#)

When anyone attempts to login using the emergency admin account, you will receive a SMS and Email as per the below



1 Fired:Sev0 Azure Monitor Alert Emergency  
Access on loganalytics ( microsoft.operationalinsights/workspaces ) at

[View the alert in Azure Monitor >](#)

### Summary

<b>Alert name</b>	Emergency Access
<b>Severity</b>	Sev0
<b>Monitor condition</b>	Fired
<b>Affected resource</b>	<a href="#">loganalytics</a>

## 2) Require multifactor authentication for administrative roles

1. Log in to <https://entra.microsoft.com/>
2. Expand Azure Active Directory
3. Select Protect & Secure, then select Conditional Access.
4. Click New policy and provide the policy name
5. Go to Assignments > Users and groups > Include > Select users and groups > check Directory roles., At a minimum, select the following roles: Billing admin, Conditional Access admin, Exchange admin, Global admin, Helpdesk admin, Security admin, SharePoint admin, and User admin (you can select all roles contain the word admin).

Home > Mo | Security > Security | Conditional Access > 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](#)

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.

[Learn more](#)

Name \*

### Assignments

Users or workload identities 

Specific users included and specific users excluded

Cloud apps or actions 

All cloud apps

Conditions 

0 conditions selected

### Access controls

Grant 

1 control selected

Session 

0 controls selected

What does this policy apply to?

Users and groups 

Include     Exclude

None

All users

Select users and groups

All guest and external users 

Directory roles 

8 selected 

Users and groups

- Exclude Emergency access accounts from MFA

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 \*

Require multifactor authentication for ad...

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.

[Learn more](#)

Assignments

Users or workload identities ⓘ

Specific users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

What does this policy apply to?

Users and groups

Include

Exclude

Select the users and groups to exempt from the policy

All guest and external users ⓘ

Directory roles ⓘ

Users and groups

Select excluded users and groups

- Go to Cloud apps or actions > Cloud apps > Include > select All cloud apps (and don't exclude any apps).

## 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 \*

Require multifactor authentication for ad... ✓

Assignments

Users or workload identities ⓘ

Specific users included and specific users excluded

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps

**Include**

Exclude

None

All cloud apps

Select apps



Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal.

Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected.

- Under Access controls > Grant > select Grant access > check Require multifactor authentication (and nothing else).
- Create.

## 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 \*

Require multifactor authentication for ad... 

### Assignments

Users or workload identities 

Specific users included and specific users excluded

Cloud apps or actions 

All cloud apps

Conditions 

0 conditions selected

### Access controls

Grant 

1 control selected

Session 

0 controls selected

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

# 3) Ensure all Users can complete multifactor authentication

1. Log in to <https://entra.microsoft.com/>
2. Select Protect & Secure, then select Conditional Access.
3. Create a policy which require MFA authentication from all users

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is collapsed, and the main area shows the 'Conditional Access Policies' page. A policy named 'Require MFA for all users' is selected. The 'Grant' tab is active, displaying settings for access enforcement. Under 'Grant', 'Grant access' is selected, and 'Require multifactor authentication' is checked. Other options like 'Block access' and 'Require authentication strength' are present but grayed out. The 'Conditions' and 'Access controls' sections are also visible. At the bottom, there's an 'Enable policy' switch set to 'On' and a 'Save' button.

## 4) Do not allow Users to grant consent to unreliable applications

1. Log in to <https://entra.microsoft.com/>
2. Go to Azure Active Directory > Applications > Enterprise applications > Consent and permissions

The screenshot shows the 'Consent and permissions' page in the Azure portal. The left sidebar has 'Manage' selected, and 'User consent settings' is highlighted. The main content area is titled 'User consent for applications' with a sub-instruction: 'Configure whether users are allowed to consent for applications to access your organization's data. Learn more'. Three options are listed: 'Do not allow user consent' (selected, indicated by a green dot), 'Allow user consent for apps from verified publishers, for selected permissions (Recommended)', and 'Allow user consent for apps'. A note at the bottom states: 'When user consent for applications is disabled, users may still be able to connect their work or school accounts with LinkedIn. You can manage LinkedIn account connects in [User Settings](#)'.

## 5) Enable Self-Service Password Reset

1. Create a Group called SSPR or any other name
2. Log in to <https://entra.microsoft.com/>
3. Choose Protect & Secure then Password reset.
4. On the Properties page, select the SSPR group which you created at step1
5. Select Save.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar has a 'Protect & secure' section with 'Password reset' selected. The main content area is titled 'Password reset | Properties' for the 'Mokhtar.Cloud - Azure Active Directory' tenant. Under the 'Manage' tab, the 'Self service password reset enabled' dropdown is set to 'Selected'. A yellow box highlights the 'SSPR' group under 'Select group'. A note at the bottom states: 'These settings only apply to end users in your organization. Admins are always enabled and are required to use two authentication methods to reset their password. Click here to learn more about password policies.'

Now any user part of the above group SSPR, he will be able to use the self-service portal to reset his account.

# 6) Ensure that password protection is Enabled for Active Directory

To setup Azure Active Directory Password Protection, use the following steps:

1. Download and install the Azure AD Password Proxies and DC Agents from the below  
link: <https://www.microsoft.com/download/details.aspx?id=57071>
2. Log in to <https://entra.microsoft.com/>
3. Select Protect & Secure then Authentication Methods
4. Select Password protection and toggle Enable password protection on Windows Server Active Directory to Yes and Mode to Enforced
5. You can add your custom banned list as well.

Microsoft Entra admin center

Home > Authentication methods

Authentication methods | Password protection

Manage

Policies

Password protection

Registration campaign

Authentication strengths (Preview)

Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: Yes

Egypt  
Mokhtar  
Dubai

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: Yes

Mode: Enforced

- Click Save at the top of the right pane.

# 7) Enable Conditional Access policies to block legacy authentication

To setup a conditional access policy to block legacy authentication, use the following steps:

1. Log in to <https://entra.microsoft.com/>
2. Select Protect & Secure, then select Conditional Access.
3. Create a new policy by selecting new policy.
4. Set the following conditions within the policy.
5. Under Assignments enable All users

**Block legacy authentication** ...

Conditional Access policy

 Delete

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

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. [Learn more](#)

**Name \*** Block legacy authentication

**Assignments**

Users ⓘ All users included and specific users excluded

Cloud apps or actions ⓘ All cloud apps

Conditions ⓘ 1 condition selected

Access controls

Grant ⓘ Block access

Session ⓘ 0 controls selected

What does this policy apply to? Users and groups

Include Exclude

None  All users  Select users and groups

**⚠️** Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

- Under Assignments and Users and groups set the Exclude any service account which required legacy authentication for example old legacy

SMTP application, you can exclude the emergency access admin accounts as well.

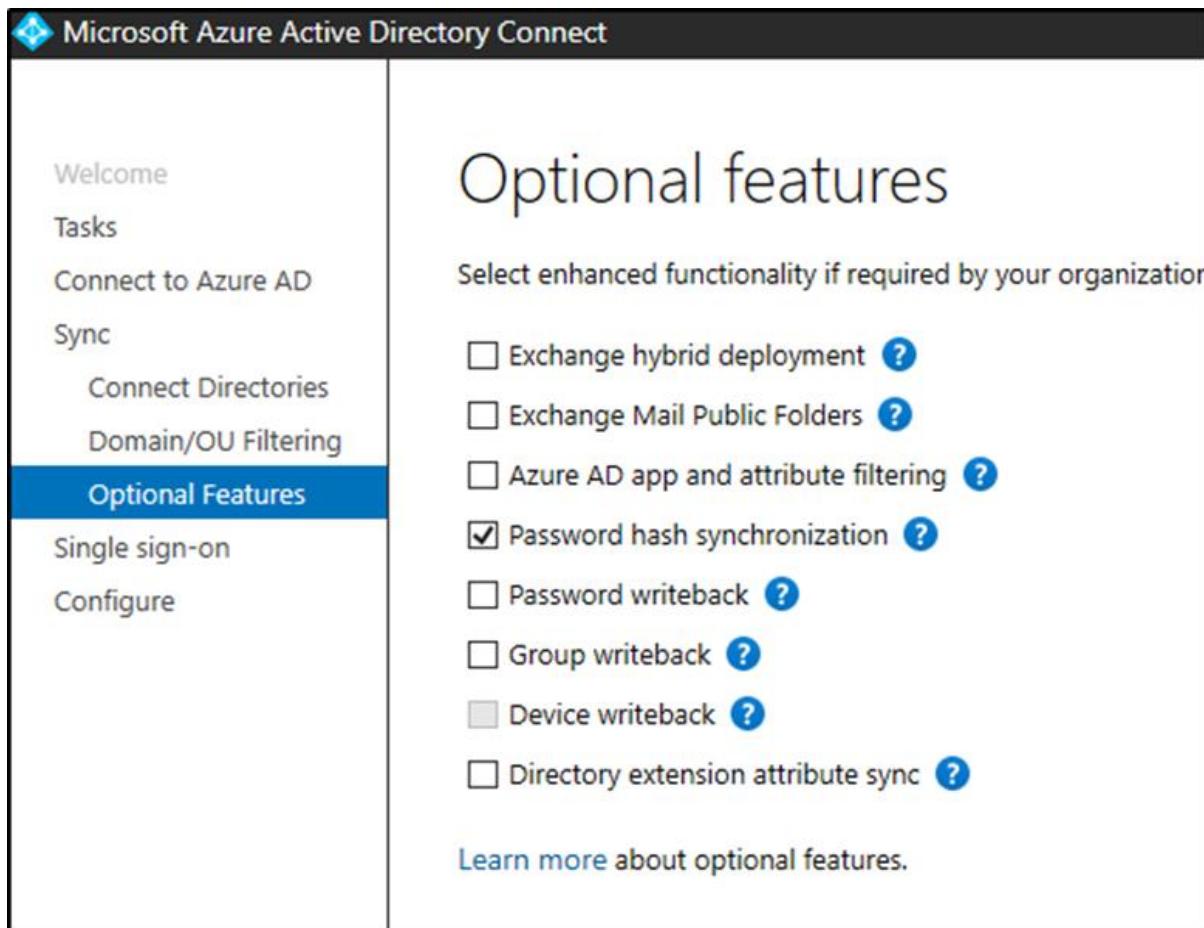
Select Conditions then Client apps, enable the settings for Exchange ActiveSync clients and other clients, select the grant action to be blocked

The screenshot shows the Microsoft Entra admin center interface for managing Conditional Access policies. A specific policy named "Block legacy authentication" is being edited. On the right side, under the "Client apps" section, there is a configuration panel with two main sections: "Modern authentication clients" and "Legacy authentication clients". Under "Modern authentication clients", the "Browser" and "Mobile apps and desktop" options are listed with checkboxes. Under "Legacy authentication clients", two checkboxes are checked: "Exchange ActiveSync client" and "Other clients". In the center of the screen, the "Access controls" section is highlighted with a yellow box, showing the "Grant" option selected. The "Block access" option is also visible. At the bottom of the page, there is a "Done" button.

## 8) Ensure that password hash sync is Enabled for hybrid deployments

To setup Password Hash Sync, use the following steps:

1. Log in to the server that hosts the Azure AD Connect tool
2. Double-click the Azure AD Connect icon that was created on the desktop
3. Click Configure.
4. On the Additional tasks page, select Customize synchronization options and click Next.
5. Enter the username and password for your global administrator.
6. On the Connect your directories screen, click Next.
7. On the Domain and OU filtering screen, click Next.
8. On the Optional features screen, check Password hash synchronization and click Next.



- On the Ready to configure screen click Configure.
- Once the configuration completes, click Exit.

# 9) Enable Azure AD Identity Protection sign-in risk policies

To configure a Sign-In risk policy, use the following steps:

1. Log in to <https://entra.microsoft.com/>
2. Select Protect & Secure.
3. Select Identity Protection
4. Select Sign-in risk policy
5. Set the following conditions within the policy.
  1. Under Users choose All users
  2. Under Sign-in risk Select Medium and above.
  3. Under Access Controls select Grant then in the right pane click Grant access then select Require multi-factor authentication.
6. Set the policy to on then Save

**Microsoft Entra admin center**

Home > Identity Protection

**Identity Protection | Sign-in risk policy**

We recommend migrating sign-in risk policy to Conditional Access

**Policy Name:** Sign-in risk remediation policy

**Assignments:** All users

**Sign-in risk:** Medium and above

**Controls:** Access (Require multifactor authentication)

**Enforce policy:** On

# 10) Enable Azure AD Identity Protection

## User risk policies

To configure a user risk policy, use the following steps:

1. Log in to <https://entra.microsoft.com/>
2. Select Security.
3. Select Identity Protection
4. Select Sign-in risk policy
5. Set the following conditions within the policy.
  1. Under Users choose All users
  2. Under Sign-in risk Select Medium and above.
  3. Under Access Controls select Grant then in the right pane click Grant access then select Require Password Change.
6. Set the policy to on then Save

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is titled 'Protect & secure' and includes 'Conditional Access', 'Identity Protection' (which is highlighted), 'Authentication methods', 'Password reset', 'Custom attributes', 'Risky activities', 'Identity Governance', and 'Learn & support'. The main content area is titled 'Identity Protection | User risk policy'. It features a search bar and a message about migrating user risk policy to Conditional Access. On the right, there are several sections: 'Policy Name' (User risk remediation policy), 'Assignments' (All users under User risk: Medium and above), 'Controls' (Access: Require password change), 'Report' (Risky users, Risky workload identities, Risky sign-ins, Risk detections), 'Notify' (Users at risk detected alerts, Weekly digest), 'Troubleshooting + Support' (Troubleshoot, New support request), and an 'Enforce policy' toggle switch set to 'On'. A 'Save' button is located at the bottom right.

# 11) Use Just in Time privileged access to Office 365 roles

we will deploy the below simple table using PIM

Role	Assignee	Justification	Approval	Person to Approve	Max Duration	Validity
Global Admin	Admin1	Required	Manual Approval	Mohamed Mokhtar	4 hours	1 year
Global Reader	Admin1	Required	Auto Approval	N/A	8 Hours	Permanent

**To configure Global Admin Role as per the above table**

- Sign-on to your Microsoft Entra admin center as global administrator by going to <https://entra.microsoft.com>
- Select Identity Governance Then Privileged Identity management.
- Under Manage click on Azure AD Roles.
- look for Global admin Roles and open it
- Click on settings then edit and configure it to match the above table or your required configurations

## Edit role setting - Global Administrator

Privileged Identity Management | Azure AD roles

Activation   Assignment   Notification

Activation maximum duration (hours)



On activation, require

None

Azure MFA

Require justification on activation

Require ticket information on activation

Require approval to activate

Select approver(s)

1 Member(s), 0 Group(s) selected

If no specific approvers are selected, privileged role administrators/global administrators will become the default approvers.

Selected approvers:

Update

Next: Assignment

<https://portal.azure.com/#home>

## Assign this role as eligible to admin1

Home > Privileged Identity Management | Azure AD roles > Mokhtar.Cloud | Roles > Global Administrator | Assignments

### Add assignments

Privileged Identity Management | Azure AD roles

**Info** You can also assign roles to groups now. [Learn more](#) X

**Resource**  
Mokhtar.Cloud

**Resource type**  
Directory

**Select role** ⓘ Global Administrator ▼

**Scope type** ⓘ Directory ▼

**Select member(s) \*** ⓘ  
1 Member(s) selected

**Selected member(s)** ⓘ

 admin admin@elshreef.net	Remove
---	--------

---

Next > Cancel

## Add assignments

Privileged Identity Management | Azure AD roles

[Membership](#) [Setting](#)
Assignment type [i](#)
 Eligible

 Active

Maximum allowed eligible duration is permanent.

 Permanently eligible
Assignment starts [\\*](#)
  
Assignment ends [\\*](#)
  

Home > Privileged Identity Management | Azure AD roles > Mokhtar.Cloud | Roles >

**Global Administrator | Assignments** [...](#)

Privileged Identity Management | Azure AD roles [X](#)

Manage																																							
<a href="#">Assignments</a>		<a href="#">Add assignments</a>	<a href="#">Settings</a>	<a href="#">Refresh</a>	<a href="#">Export</a>	<a href="#">Got feedback?</a>																																	
		<a href="#">Eligible assignments</a>	<a href="#">Active assignments</a>	<a href="#">Expired assignments</a>																																			
<input type="text"/> Search by member name or principal name																																							
<table border="1"> <thead> <tr> <th>Name</th> <th>Principal name</th> <th>Type</th> <th>Scope</th> <th>Membership</th> <th>Start time</th> <th>End time</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td colspan="8">Global Administrator</td> </tr> <tr> <td>admin</td> <td>admin@elshreef.net</td> <td>User</td> <td>Directory</td> <td>Direct</td> <td>5/29/2022, 4:51:49 PM</td> <td>Permanent</td> <td><a href="#">Remove</a>   <a href="#">Update</a></td> </tr> <tr> <td colspan="8">10/27/2022, 8:01:35 PM 10/27/2023, 8:00:06 PM <a href="#">Remove</a>   <a href="#">Update</a>   <a href="#">Ex</a></td> </tr> </tbody> </table>								Name	Principal name	Type	Scope	Membership	Start time	End time	Action	Global Administrator								admin	admin@elshreef.net	User	Directory	Direct	5/29/2022, 4:51:49 PM	Permanent	<a href="#">Remove</a>   <a href="#">Update</a>	10/27/2022, 8:01:35 PM 10/27/2023, 8:00:06 PM <a href="#">Remove</a>   <a href="#">Update</a>   <a href="#">Ex</a>							
Name	Principal name	Type	Scope	Membership	Start time	End time	Action																																
Global Administrator																																							
admin	admin@elshreef.net	User	Directory	Direct	5/29/2022, 4:51:49 PM	Permanent	<a href="#">Remove</a>   <a href="#">Update</a>																																
10/27/2022, 8:01:35 PM 10/27/2023, 8:00:06 PM <a href="#">Remove</a>   <a href="#">Update</a>   <a href="#">Ex</a>																																							

### To configure Global Reader Role as per the above table

- Sign-on to your Microsoft Entra admin center as global administrator by going to <https://entra.microsoft.com>
- Select Identity Governance Then Privileged Identity management.
- Under Manage click on Azure AD Roles.
- look for Global Reader Role and open it
- Click on settings, the default configuration will achieve our requirements

[Edit](#)

---

Activation	
Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	No
Approvers	None

---

Assign this role as eligible to admin

Click on add assignment

Home Privileged Identity Management | Azure AD roles > Mokhtar.Cloud | Roles >

## Global Reader | Assignments

Privileged Identity Management | Azure AD roles

Manage

+ Add assignments Settings Refresh Export Got feedback?

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

Name	Principal name	Type	Scope
No results			

Select Admin

Home > Privileged Identity Management | Azure AD roles > Mokhtar.Cloud | Roles > Global Re

## Add assignments

Privileged Identity Management | Azure AD roles

Membership    Setting

 You can also assign roles to groups now. [Learn more](#) X

Resource

Mokhtar.Cloud

Resource type

Directory

Select role (i)

Global Reader



Scope type (i)

Directory



Select member(s) \* (i)

1 Member(s) selected

Selected member(s) (i)



admin

admin@elshreef.net

[Remove](#)

As per our simple deployment we will select the below to match the above table

## Add assignments

Privileged Identity Management | Azure AD roles

Membership    **Setting**

Assignment type ⓘ

Eligible

Active

Maximum allowed eligible duration is permanent.

Permanently eligible

Assignment starts

10/28/2022



11:06:21 AM

Assignment ends

10/28/2023



11:06:21 AM

# 12) Ensure Security Defaults are disabled on Azure AD

Instead of Security Defaults its recommended to use Conditional Access to control and manage the MFA, To disable security defaults in your directory:

1. Log in to [Security defaults - Microsoft Azure](#)
2. Select Manage security defaults.
3. Set the Enable security defaults toggle to No.
4. Select Save.

The screenshot shows the 'Mo | Properties' page in the Azure Active Directory portal. On the left, there's a sidebar with various management options like Users, Groups, External Identities, etc. The main area displays 'Tenant properties' for tenant 'Mo'. A yellow box highlights the 'Enable security defaults' section, which contains a toggle switch set to 'No'. Below this, there's a note about security defaults being basic identity mechanisms recommended by Microsoft, and a 'Learn more' link. At the bottom of the page, another yellow box highlights the 'Manage security defaults' button.

## 13) Ensure that LinkedIn contact synchronization is disabled.

1. Log in to <https://entra.microsoft.com/>
2. Open Azure Active Directory then Users, then User Settings
  - Under LinkedIn account connections then click No.
  - Click Save at the top of the page.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is titled "Microsoft Entra admin center" and includes sections for Home, Favorites, Azure Active Directory, Overview, Users, User settings, and Groups. The "Users" and "User settings" items are highlighted with yellow boxes. The main content area is titled "Users | User settings" and shows a "LinkedIn account connections" section. This section contains a description: "Allow users to connect their work or school account with LinkedIn. Data sharing between Microsoft and LinkedIn is not enabled until you sign in to their LinkedIn account." Below this is a "Learn more about LinkedIn account connections" link. At the bottom of the section are three buttons: "Yes", "Selected group", and "No". The "No" button is highlighted with a red oval. Other buttons in the interface include "Save", "Discard", and "Got feedback?". A search bar and a "Restrict non-admin users from creating tenants (preview)" link are also visible.

## **14) Ensure Sign-in frequency is Enabled, and browser sessions are not persistent for Administrative Users.**

1. Log in to <https://entra.microsoft.com/>
2. Select Protect & Secure, then select Conditional Access.
3. Click New policy and provide the policy name
4. Go to Assignments > Users and groups > Include > Select users and groups > check Directory roles.
5. At a minimum, select the following roles: Billing admin, Conditional Access admin, Exchange admin, Global admin, Helpdesk admin, Security admin, SharePoint admin, and User admin (you can select any role with word admin).
6. exclude emergency access account
7. Go to Cloud apps or actions > Cloud apps > Include > select All cloud apps (and don't exclude any apps).
8. Under Access controls > Grant > select Grant access > check Require multifactor authentication.
9. Under Session check Sign-in frequency (Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.), we will configure it to 4 hours (You can select your preferred value)
10. Check Persistent browser session (A persistent browser session allows the end-user to remain signed in after closing and reopening their browser window) then select Never persistent in the dropdown menu.
11. Create.

**Require multifactor authentication for administrative roles** ...

Conditional Access policy

Delete

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

Name \*

Assignments

Users

Specific users included and specific users excluded

Cloud apps or actions  All cloud apps

Conditions  0 conditions selected

Access controls

Grant

1 control selected

Session  2 controls selected

SESSION

Control access based on session controls to enable limited experiences within specific cloud applications. [Learn more](#)

Use app enforced restrictions

This control only works with supported apps. Currently, Office 365, Exchange Online, and SharePoint Online are the only cloud apps that support app enforced restrictions. Click here to learn more.

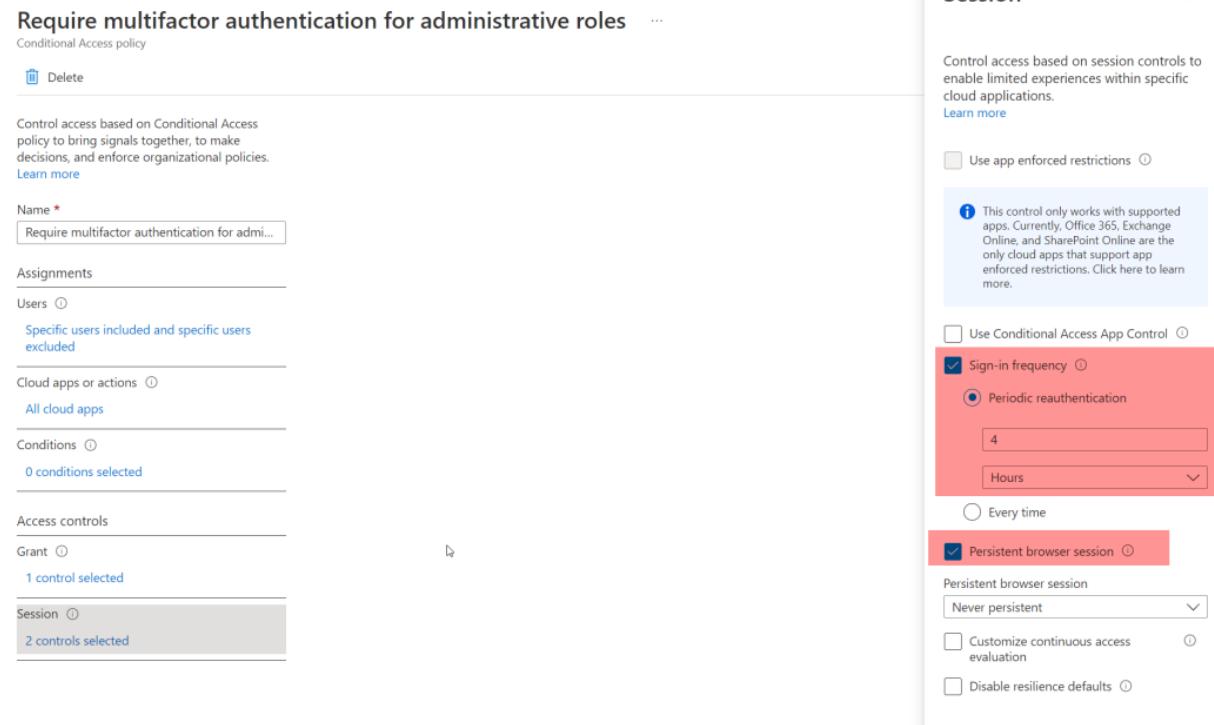
Use Conditional Access App Control

Sign-in frequency  Periodic reauthentication

Hours  Every time

Persistent browser session

Persistent browser session   Customize continuous access evaluation  Disable resilience defaults



# 15) Ensure the option to remain signed in is hidden

1. Log in to <https://portal.azure.com>
2. Click on Azure Active Directory
3. Under Manage select Company branding followed by the appropriate Locale policy.
4. If no policy exists, you will need to click Configure to create one
5. Scroll to the bottom of the newly opened pane and ensure Show option to remain signed in is not checked.
6. Click Save.

The screenshot shows the 'Configure company branding' page in the Azure portal. On the left, there's a sidebar with navigation links like Dashboard, All services, Favorites, Azure Active Directory, Users (which is selected), Enterprise applications, Manage, and Monitoring. In the main area, there's a title 'Configure company branding' and a sub-section 'Azure Active Directory'. Below this, there are several input fields for sign-in page background image, banner logo, username hint, and sign-in page text. Under 'Advanced settings', there are fields for sign-in page background color and square logo image. At the bottom, there's a section titled 'Show option to remain signed in' which contains a checkbox. This checkbox is currently unchecked. A yellow callout box highlights this section with the text: 'Important: some features of SharePoint Online and Office 2010 have a dependency on users remaining signed in. If you hide this option, users may get additional and unexpected sign in prompts.'

# 16) Do not expire passwords

To set Office 365 Passwords to Expire, use the Microsoft 365 Admin Center:

1. Login to <https://admin.microsoft.com/>
2. Expand Settings then select the Org Settings subcategory.
3. Click on Security & privacy.
4. Select Password expiration policy.
5. If the Set passwords to never expire (recommended) box is unchecked, check it.
6. Click Save.

The screenshot shows the Microsoft 365 Admin Center interface. On the left, there's a navigation sidebar with various categories like Home, Users, Teams & groups, Roles, Resources, Billing, Support, and Settings. Under Settings, 'Org settings' is selected. The main content area is titled 'Org settings' and shows the 'Security & privacy' tab is active. On the right, there's a yellow callout box titled 'Password expiration policy' with the following text:  
The policy you choose here applies to everyone in your organization.  
Learn why passwords that never expire are more secure  
 Set passwords to never expire (recommended)

## 17) Ensure Administrative accounts are separate and cloud-only

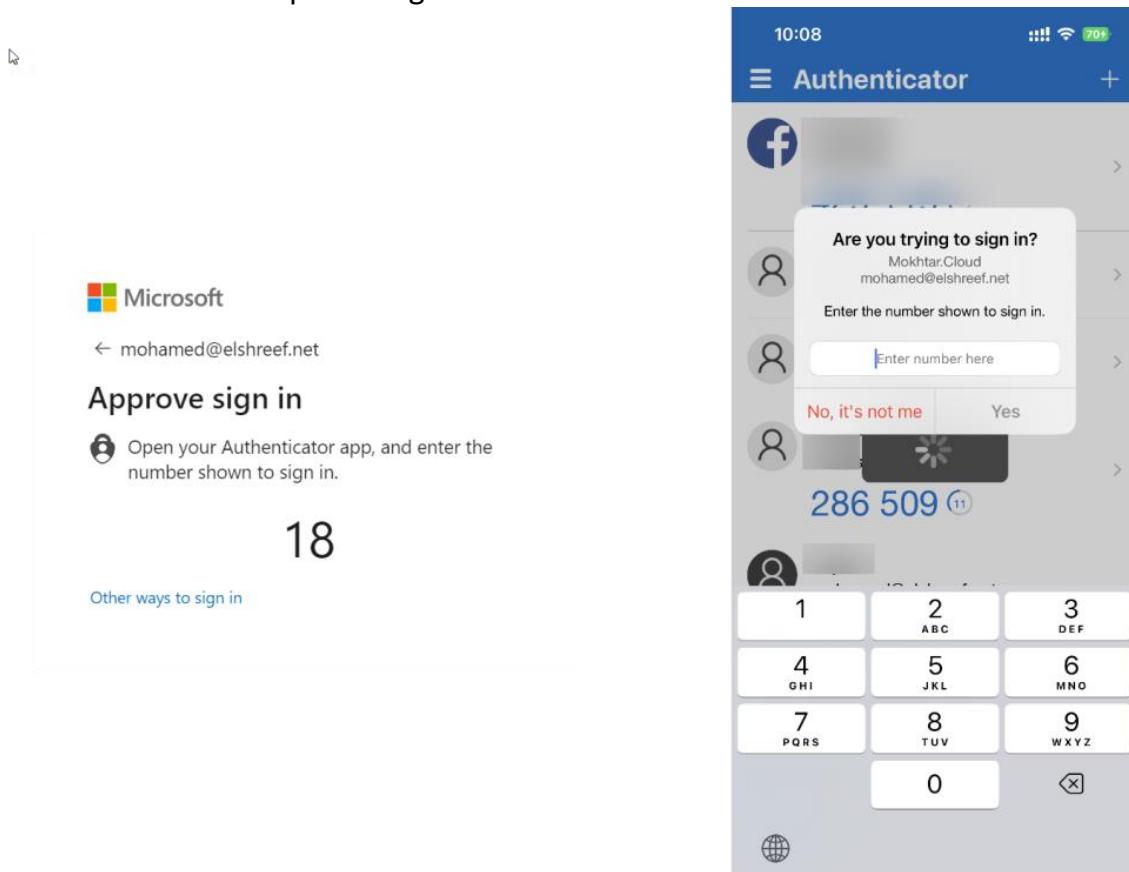
- Be sure to create separate accounts for users to do Global Administrator tasks.
- Make sure that your Global Administrators don't accidentally open emails or run programs with their administrator accounts.
- Be sure those accounts have their email forwarded to a working mailbox.
- Global Administrator (and other privileged groups) accounts should be cloud-only accounts with no ties to on-premises Active Directory.

## 18) Passwordless sign-in with the Microsoft Authenticator app

The Microsoft Authenticator app can be used to sign into any Azure AD account without using a password. Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a device, where the device uses a PIN or biometric.

Users register themselves for the Passwordless authentication method of Azure AD by using the following steps:

1. Browse to <https://aka.ms/mysecurityinfo>.
2. Sign in, then add the Authenticator app by selecting **Add method > Authenticator app**, then **Add**.
3. Follow the instructions to install and configure the Microsoft Authenticator app on your device.
4. Select **Done** to complete Authenticator configuration.
5. In **Microsoft Authenticator**, choose **Enable phone sign-in** from the drop-down menu for the account registered.
6. Follow the instructions in the app to finish registering the account for Passwordless phone sign-in.



## 19) Passwordless: Windows Hello for Business

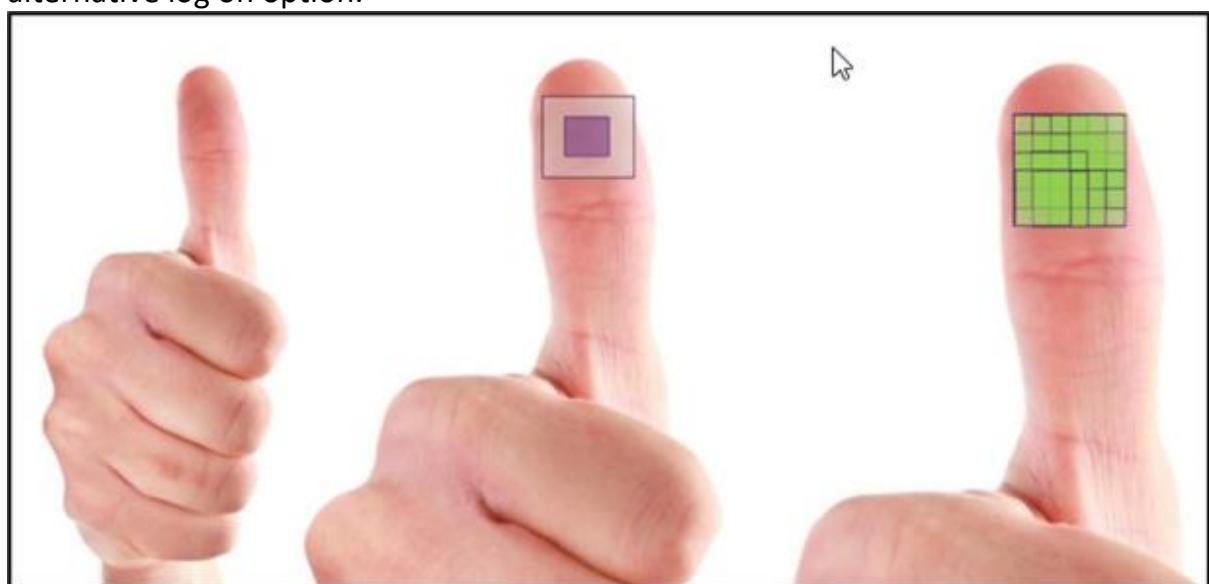
In Windows 10&11, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

Windows Hello provides reliable, fully integrated biometric authentication based on facial recognition or fingerprint matching.

**Facial recognition** sensors use special cameras that see in IR light, letting them tell the difference between a photo and a living person while scanning an employee's facial features.



**Fingerprint sensors**, or sensors that use an employee's unique fingerprint as an alternative log on option.



Windows Hello for Business has a different deployment model (On-premises, Hybrid and Cloud Only) on this lab we will cover the configuration of Cloud Only using Microsoft Endpoint Manager

Enable Windows Hello for Business using Microsoft Endpoint Manager for all users (Alternative you can create a configuration profile rule if you want to apply WHfB for specific group)

## Windows Hello for Business

X

Windows enrollment

### ^ Essentials

Last modified	: 08/31/22, 10:05 AM
Assigned to	: <a href="#">All users.</a>

---

Windows Hello for Business settings lets users access their devices using a gesture, such as biometric authentication, or a PIN. [Learn more.](#)

Learn about integrating Windows Hello for Business with Microsoft Intune

Name

All users and all devices

Description

This is the default Windows Hello for Business configuration applied with the lowest priority to all users regardless of group membership.

Configure Windows Hello for Business: ⓘ Enabled

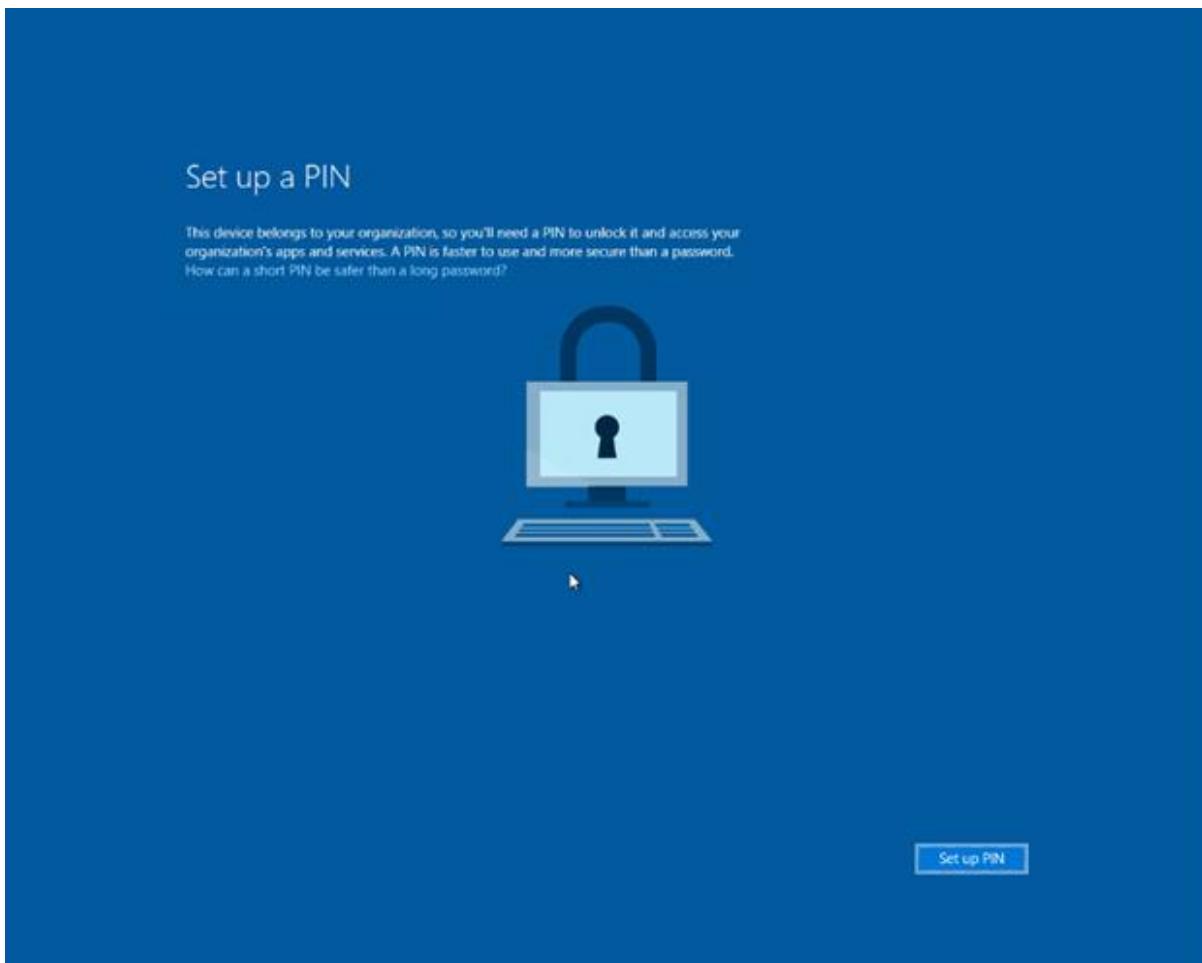
Use a Trusted Platform Module (TPM): ⓘ Required Preferred

Minimum PIN length: ⓘ 6

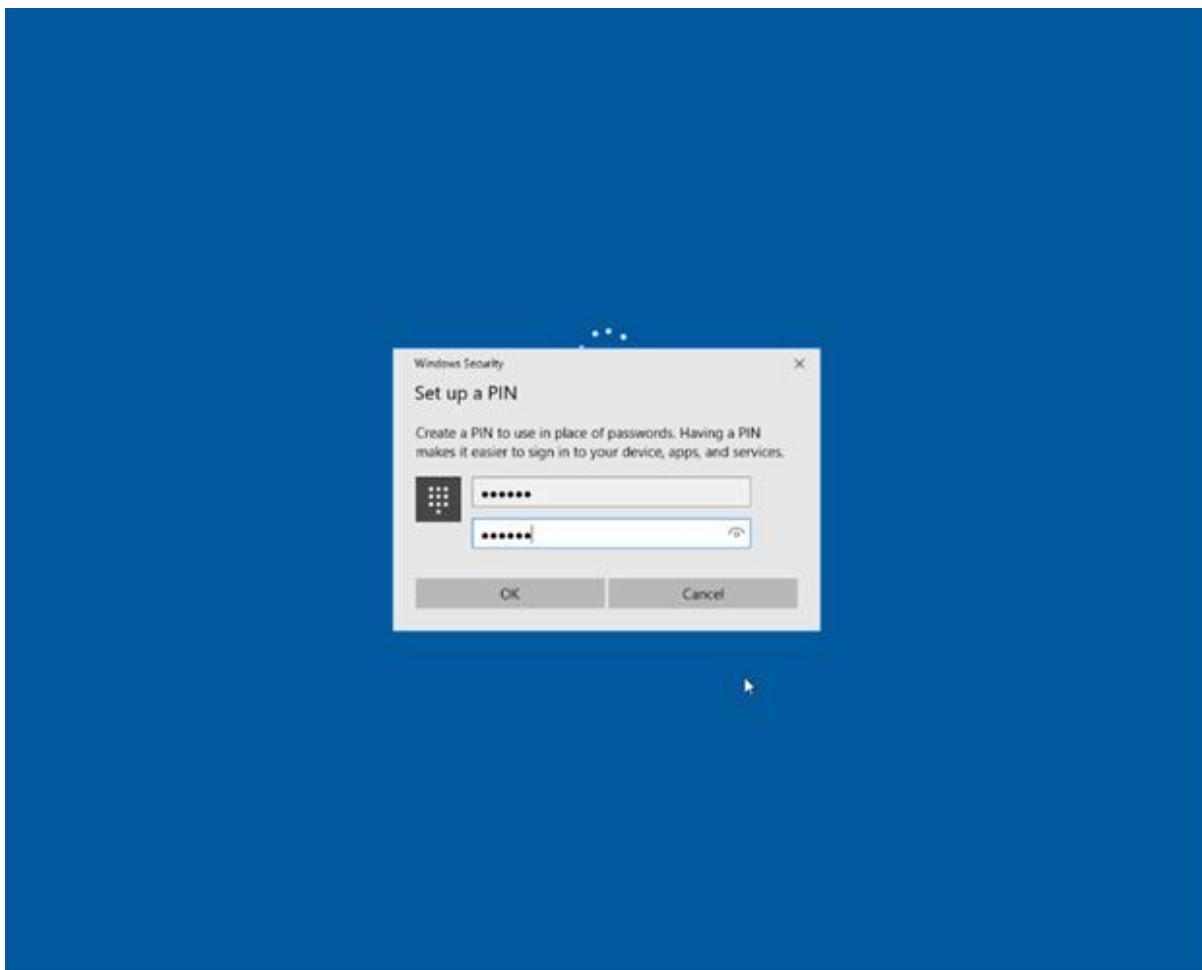
Configure Windows Hello for Business:	<input type="button" value="Enabled"/> 
Use a Trusted Platform Module (TPM):	<input type="button" value="Required"/> <input type="button" value="Preferred"/> 
Minimum PIN length:	<input type="text" value="6"/> 
Maximum PIN length:	<input type="text" value="127"/> 
Lowercase letters in PIN:	<input type="button" value="Not allowed"/> 
Uppercase letters in PIN:	<input type="button" value="Not allowed"/> 
Special characters in PIN:	<input type="button" value="Not allowed"/> 
PIN expiration (days):	<input type="button" value="Never"/> 
Remember PIN history:	<input type="button" value="No"/> 
Allow biometric authentication:	<input type="button" value="Yes"/> <input type="button" value="No"/> 
Use enhanced anti-spoofing, when available:	<input type="button" value="Not configured"/> 
Allow phone sign-in:	<input type="button" value="Yes"/> <input type="button" value="No"/> 
Use security keys for sign-in:	<input type="button" value="Not configured"/> 

## Registration

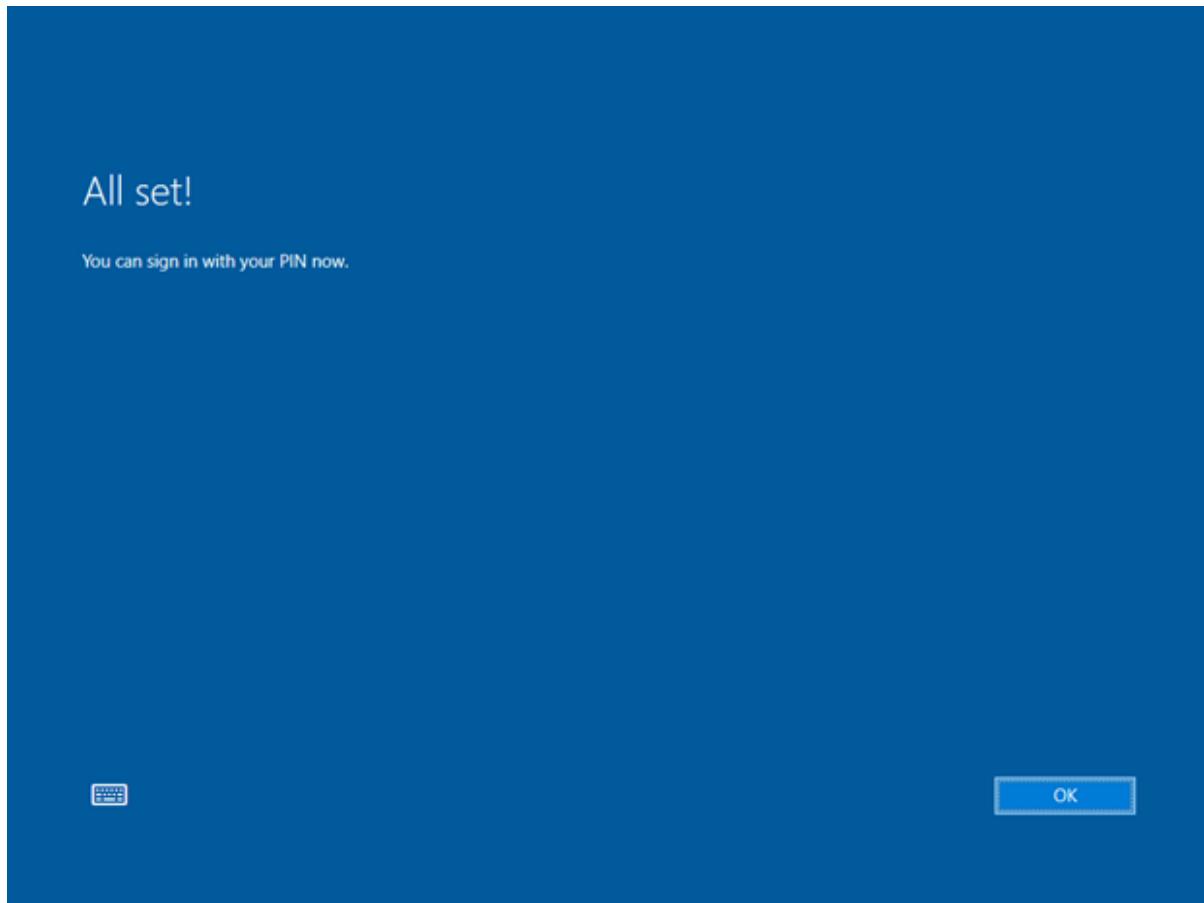
Windows Hello for Business provisioning begins with a full screen page with the title **Setup a PIN** and button with the same name. The user clicks **Setup a PIN**.



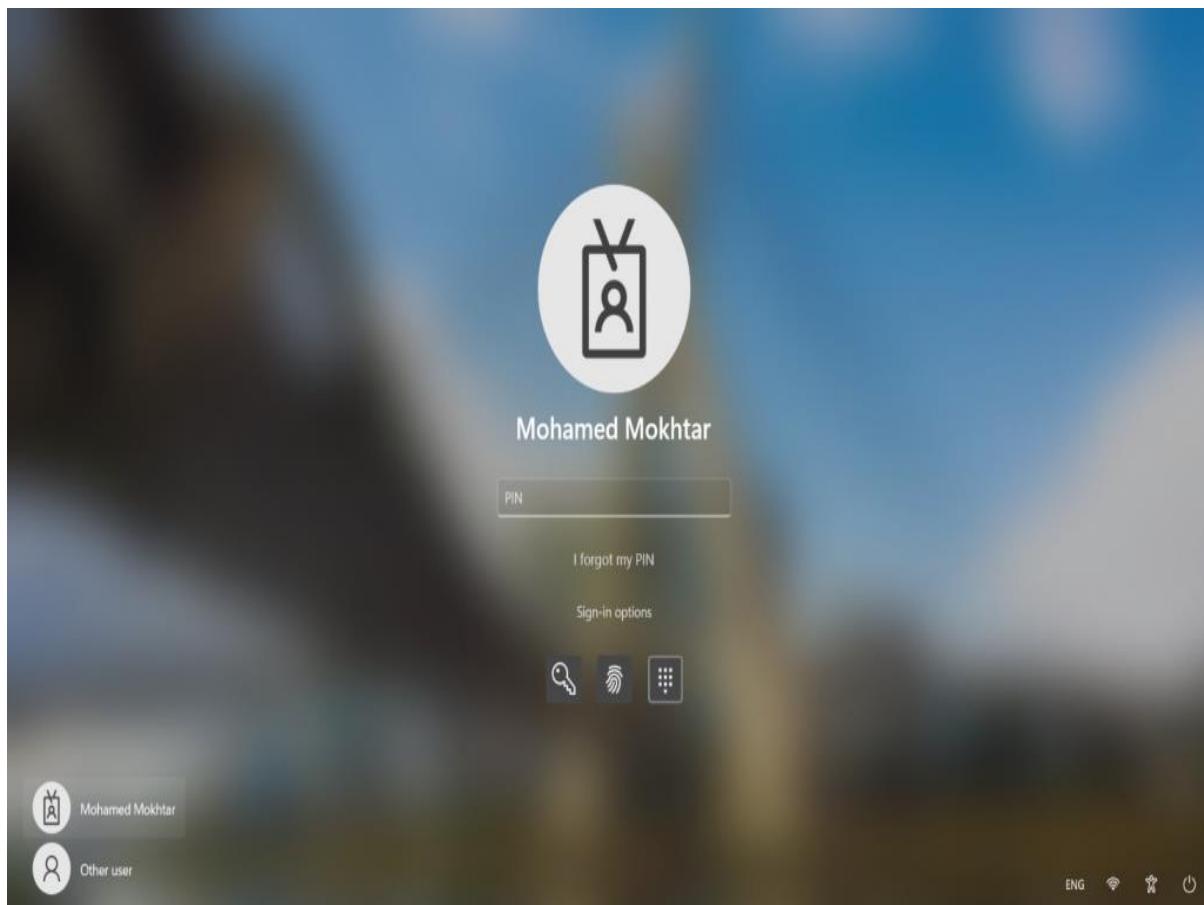
After a successful MFA, the provisioning flow asks the user to create and validate a PIN. This PIN must observe any PIN complexity requirements that you deployed to the environment.



All set!



The last thing to do is to check if everything works fine



# 20) New feature: Azure AD Authentication Strengths (Preview)

Authentication Strength enable the IT admin to force the combination of authentication methods that can be used with the conditional access.

Authentication strength	Type	Authentication methods	Conditional access policies
Multifactor authentication	Built-in	Windows Hello For Business and 16 more	Not configured in any policy yet
Passwordless MFA	Built-in	Windows Hello For Business and 3 more	Force Passwordless for Microsoft Teams
Phishing-resistant MFA	Built-in	Windows Hello For Business and 2 more	Not configured in any policy yet

The following screenshot shows the properties of one of the built-in pre-created authentication strength

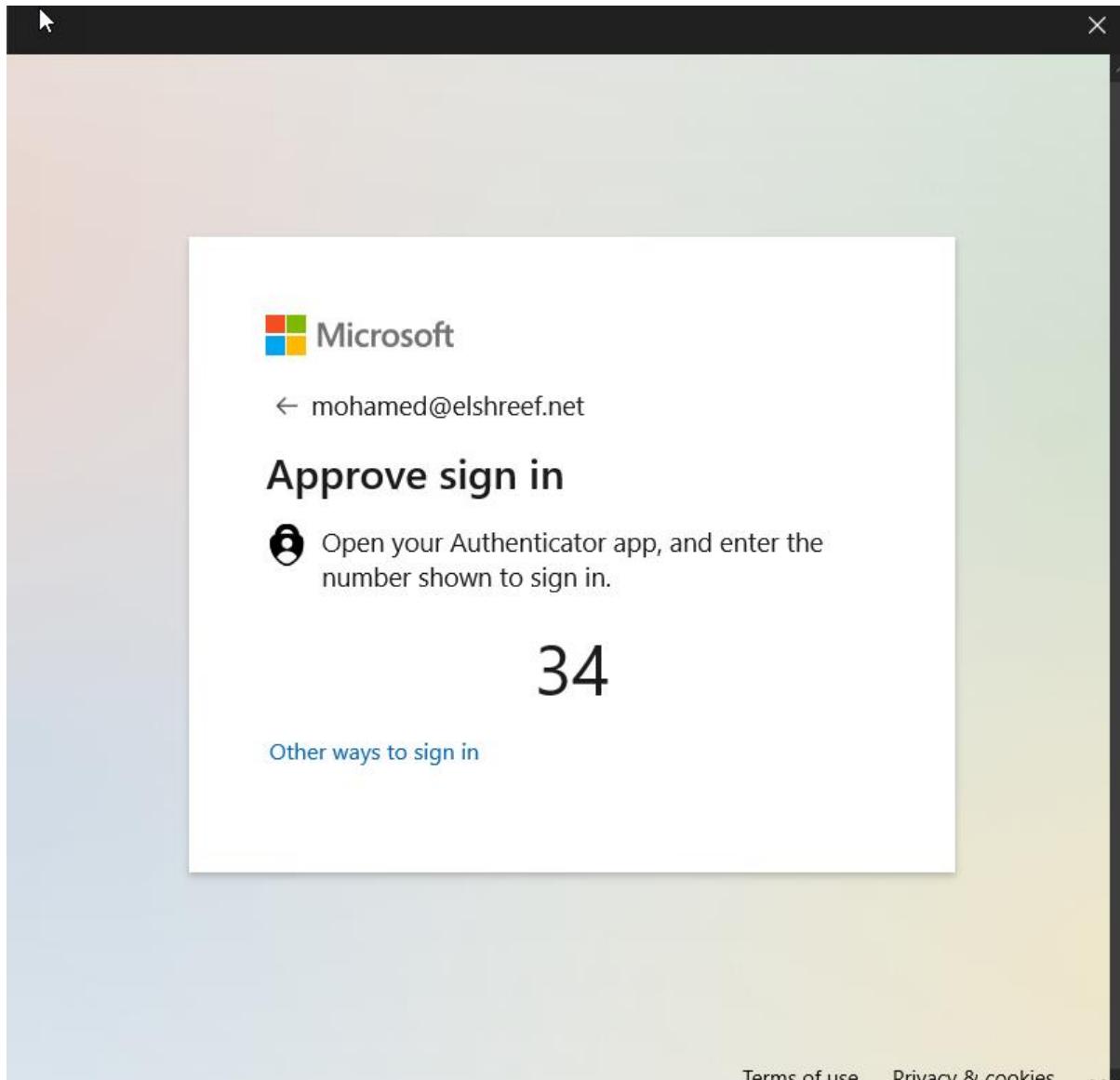
## View Authentication Strength

Name	Passwordless
Type	Built-in
Description	High assurance authentication strength that includes methods with Cryptographic keys, for example FIDO2 security key
Authentication Flows	Windows Hello For Business
<b>OR</b>	
FIDO2 Security Key	
<b>OR</b>	
Certificate Based Authentication (Multi-Factor)	
<b>OR</b>	
Microsoft Authenticator (Phone Sign-in)	

I created a conditional access policy to force passwordless while login to Microsoft teams as per the below

The screenshot shows the Microsoft Entra admin center interface. On the left, there's a sidebar with icons for Home, Conditional Access policies, Assignments, Users, Cloud apps or actions, Conditions, Access controls, Session, and Enable policy. The main area displays a policy titled "Force Passwordless for Microsoft Teams". The "Grant" tab is selected. In the "Grant" section, there are two options: "Block access" (radio button) and "Grant access" (radio button, which is selected). Below these are two checkboxes: "Require multifactor authentication" (unchecked) and "Require authentication strength (Preview)" (checked). A yellow warning box states: "'Require authentication strength' cannot be used with 'Require multifactor authentication'." A blue info box provides instructions: "To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Azure AD tenants for external users. Authentication strengths will only configure second factor authentication for external users." At the bottom right of the "Grant" section is a "Select" button.

Testing



Validation

## Activity Details: Sign-ins

[Basic info](#) [Location](#) [Device info](#) [Authentication Details](#) [Conditional Access](#) [Report-only](#) [Additional Details](#) Search

Policy Name ↑↓	Grant Controls ↑↓	Session Controls ↑↓	Result ↑↓	...
[SharePoint admin center]Use ...		Use app-enforced restrictions	Not Applied	...
Block Legacy Authentication	Block		Not Applied	...
Block legacy authentication	Block		Not Applied	...
Block native App	Require approved app		Not Applied	...
Force Passwordless for Micros...	Require authentication strength		Success	...

### Authentication Policies Applied

Per-user multifactor authentication

Conditional Access

Authentication Strength(s)

Date	Authentication met...	Authenticat...	Succeeded	Result detail	Requirement
10/6/2022, 12:27:50 AM	Passwordless phone si...		true	User approved	Passwordless MFA
10/6/2022, 12:27:50 AM	Previously satisfied		true	MFA requirement satis...	Passwordless MFA

# 21) Regularly Check identity secure score

Identity Secure Score provides organizations with increased visibility and control over their security posture by discovering opportunities that will help to improve security across your organization.

1. Log in to <https://entra.microsoft.com/>
2. Select Azure Active Directory Then Protect & Secure then Identity Secure Score

**Secure Score for Identity**

**Comparison**

Organization	Score
Mokhtar.Cloud	70.49%
Typical 1-100 person company	56.83%

**Improvement actions**

Name ↑	Score Impact ↑↓	User Impact ↑↓
Use least privileged administrative accounts	1.64%	Low
Protect all users with a user risk policy	11.48%	Moderate
Designate more than one global administrator	1.64%	Low
Enable policy to block legacy authentication methods	13.11%	Moderate
Ensure all users can complete multi-factor authentication	11.70%	High

## 22) Require trusted location for MFA and SSPR registration

Log in to <https://entra.microsoft.com/>

Select Protect & Secure, then select Conditional Access.

Click New policy and provide the policy name

on assignment, assign this policy for all users and exclude emergency admin and other services accounts.

The screenshot shows the 'Conditional Access policy' creation interface. The title is 'Allow Security registration from trusted location'. The 'Name' field contains 'Allow Security registration from trusted loc...'. Under 'Assignments', 'Users or workload identities' is selected, showing 'All users included and specific users excluded'. Under 'Conditions', '1 condition selected' is shown. Under 'Access controls', 'Enable policy' is set to 'On'. A warning message at the bottom right says: '⚠️ Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.'

Home >

## Allow Security registration from trusted location

Conditional Access policy

Delete

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

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. [Learn more](#)

Name \*

Allow Security registration from trusted loc...

Assignments

Users or workload identities ⓘ

All users included and specific users excluded

Cloud apps or actions ⓘ

1 user action included

Conditions ⓘ

1 condition selected

Access controls

Enable policy

Report-only  On  Off

⚠️ Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

on cloud application, select user actions then register security information

Home >

## Allow Security registration from trusted location

Conditional Access policy

 Delete

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name \*

Allow Security registration from trusted loc...

Assignments

Users or workload identities ⓘ

[All users included and specific users excluded](#)

Cloud apps or actions ⓘ

[1 user action included](#)

Conditions ⓘ

[1 condition selected](#)

Access controls

Enable policy

Report-only    On    Off

[Save](#)

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

User actions



Select the action this policy will apply to

Register security information

Register or join devices

on conditions select locations include any location and exclude your trusted locations/IPs/Countries

Home >

## Allow Security registration from trusted location

Conditional Access policy

Delete

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

Name \*

Allow Security registration from trusted loc...

Assignments

Users or workload identities ⓘ

All users included and specific users excluded

Cloud apps or actions ⓘ

1 user action included

Conditions ⓘ

1 condition selected

Access controls

Enable policy

Report-only  On  Off

Save

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

User risk ⓘ

Not configured

Sign-in risk ⓘ

Not configured

Device platforms ⓘ

Not configured

Locations ⓘ

Any location and all trusted locations excluded

Client apps ⓘ

Not configured

Filter for devices ⓘ

Control user access based on their physical location. [Learn more](#)

Configure ⓘ

Yes  No

Include  Exclude

Any location

All trusted locations

Selected locations

## set the grant action to block

Home >

## Allow Security registration from trusted location

Conditional Access policy

Delete

Assignments

Users or workload identities ⓘ

All users included and specific users excluded

Cloud apps or actions ⓘ

1 user action included

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

Block access

Session ⓘ

0 controls selected

Enable policy

Report-only  On  Off

Save

## Grant

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

Block access  Grant access

- Require multifactor authentication
- Require authentication strength (Preview)
- 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

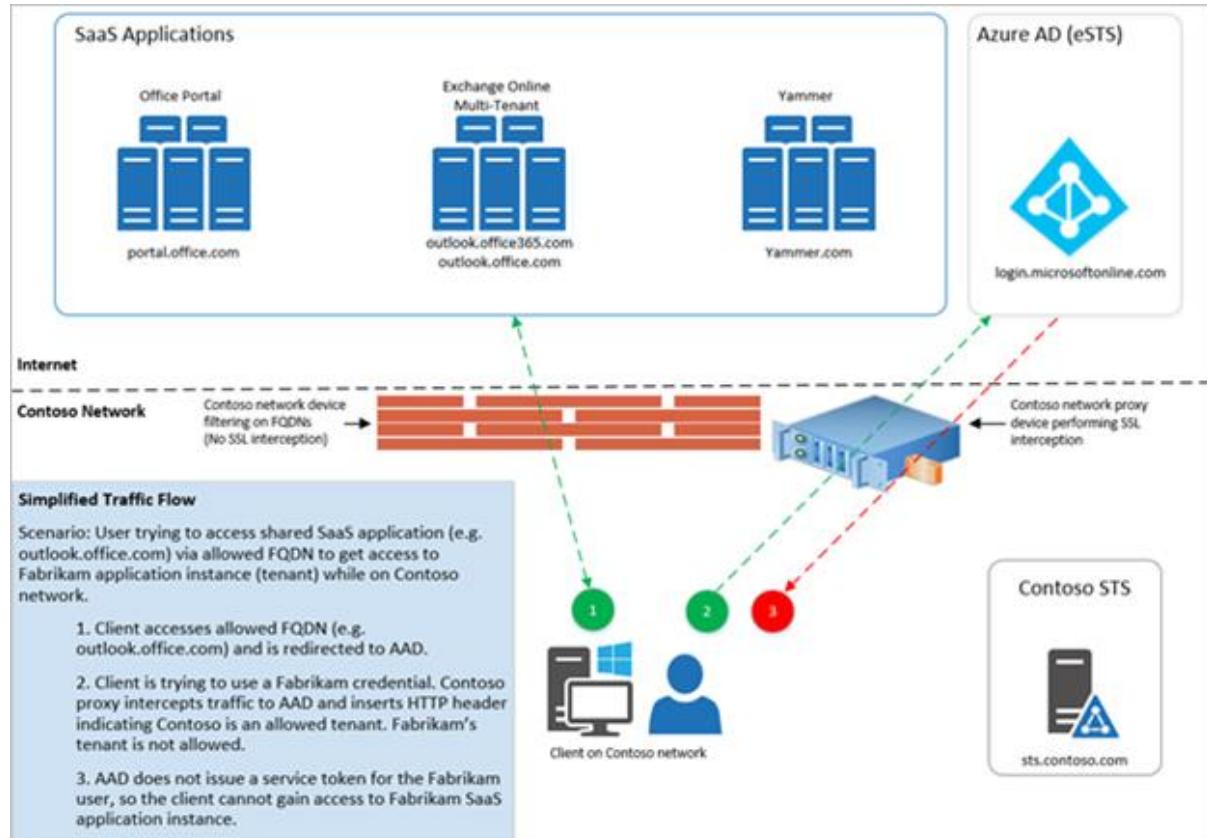
For multiple controls

Select

## 23) Tenant restrictions

The use case for tenant restriction is to allow access to Company Microsoft 365 resources and Azure tenant while blocking access to personal/non-company Microsoft/Azure 365 resources.

The below diagram from Microsoft illustrates how the traffic flow will happen when enabling tenant restrictions



To set up tenant restrictions you will need to configure your proxy infrastructure as per the above diagram.

### Prerequisites

- The proxy must be able to perform TLS interception, HTTP header insertion, and filter destinations using FQDNs/URLs.
- Clients must trust the certificate chain presented by the proxy for TLS communications. For example, if certificates from an internal public key infrastructure (PKI) are used, the internal issuing root certificate authority certificate must be trusted.
- Azure AD Premium 1 licenses are required for use of Tenant Restrictions.

### Proxy Configuration

For each outgoing request to login.microsoftonline.com, login.microsoft.com, and login.windows.net, insert two HTTP headers: *Restrict-Access-To-Tenants* and *Restrict-Access-Context*.

For *Restrict-Access-To-Tenants*

Restrict-Access-To-Tenants: contoso.com,fabrikam.onmicrosoft.com,72f988bf-86f1-41af-91ab-2d7cd011db47

For *Restrict-Access-Context*

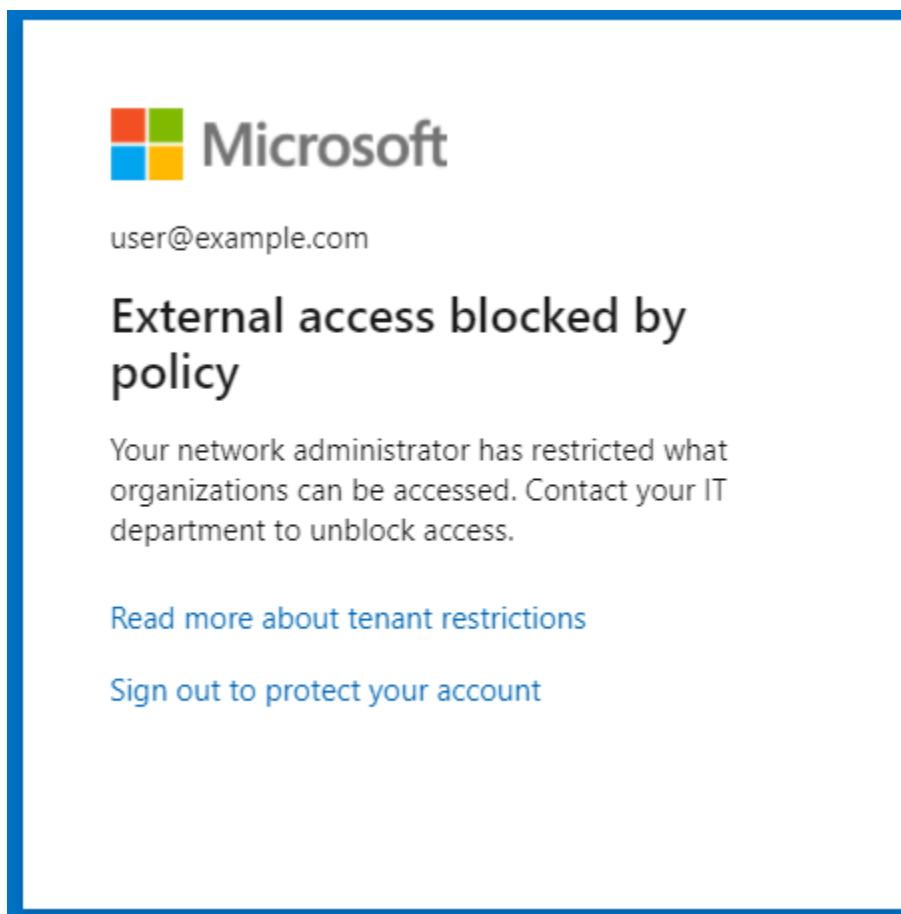
Restrict-Access-Context: 456ff232-3512-5h23-b3b3-3236w0826f3d

\* Tenant Domain names

\* Tenant ID

\* Directory ID

End User experience, user tried to log in to another M365 tenant or personal tenant



Admin logs

Under Azure Active Directory then tenant restrictions from the overview tab, you will see all sign-ins blocked because of the tenant restrictions policy

## 24) Conditional Access filters for apps

A new setting recently released in conditional access called filter for apps, using filter for apps will enable you to create conditional access rules targeting specific application based on custom security attributes.

We will create a conditional access policy to block accessing confidential App from untrusted networks , you will find here that we used the new feature App filter to filter the confidential app using the custom security attribute CA\_AppClassification

**Edit filter (Preview)**

Conditional Access policy

Name \* Block Accessing confidential A

Configure ⓘ Yes No

Using custom security attributes you can use the rule builder or rule syntax text box to create or edit the filter rules. In the preview type Integer or Boolean will not be shown. [Learn more](#)

And/Or	Attribute	Operator	Value
	CA_AppClassification	Equals	Confidential

+ Add expression

Rule syntax ⓘ

```
CustomSecurityAttribute.CA_AppClassification -eq "Confidential"
```

Contr apps

Select Cloud

Incl

Cloud apps or actions ⓘ Configured

Conditions ⓘ 1 condition selected

Access controls

Grant ⓘ Block access

Session ⓘ

Enable policy

Report-only On Off

Save Done

You will need your customized security attributes before creating the conditional access policy, as per the below

The screenshot shows the Microsoft Entra admin center interface. On the left, the navigation menu includes 'Enterprise applications', 'Conditional Access', and 'Identity Protection'. The main content area displays the 'Salesforce | Custom security attributes (preview)' page for an 'Enterprise Application'. The 'Manage' section is selected, showing options like 'Properties', 'Single sign-on', and 'Custom security attributes (preview)'. The 'Custom security attributes (preview)' section lists an attribute named 'CA' with the value 'AppClassification' and type 'String'. The 'Assigned values' column shows 'Confidential'.

## Validation "Rule Applied when access from untrusted location"

The screenshot shows the 'What If' policy test tool. It allows testing the impact of Conditional Access policies under various conditions. The 'Cloud apps' section is selected, and the 'Select' dropdown shows 'Salesforce'. Other sections include 'User or Workload identity', 'Cloud apps, actions, or authentication context', 'IP address', 'Device platform', 'Client apps', 'Device state (deprecated)', 'Sign-in risk', 'User risk', 'Service principal risk (Preview)', and 'Filter for devices'. At the bottom, there are tabs for 'Evaluation result' (warning: 'Classic policies are not evaluated by this tool'), 'Policies that will apply' (selected), and 'Policies that will not apply'. A table at the bottom lists a single policy: 'Block Accessing confidential Apps from Non-trusted IP' with 'Grant controls' set to 'Block access', 'Session controls' to 'On', and 'Has filter' to 'Yes'.

## Validation2: "Rule Skipped when access from trusted location"

# The Comprehensive Guide to Secure Azure AD & User Identities

## What If ...

Policies

[Info](#) | [Got feedback?](#)

Test the impact of Conditional Access on a user when signing in under certain conditions. [Learn more](#)

User or Workload identity

user2

Cloud apps, actions, or authentication context

1 app selected

IP address

Country

2001:8f8:1161:b8ab:44dd:48

United Arab Emirates

Select what this policy applies to

Cloud apps

Any cloud app

Select apps

Select

Salesforce

Device platform

Select device platform...

Client apps

Select a client app...

Device state (deprecated)

Select device state...

Sign-in risk

Select sign-in risk...

User risk

Select user risk...

Service principal risk (Preview)

Select service principal risk...

Filter for devices

Property Value

<Pick a property and operator fir...

**What If**

**Reset**

Evaluation result

⚠ Classic policies are not evaluated by this tool.

[Policies that will apply](#) [\*\*Policies that will not apply\*\*](#)

[Search](#)

Policy Name ↑↓	Reasons why this policy will not apply ↑↓	State ↑↓	Has filter <input type="radio"/> ↑↓
[SharePoint admin center]Block access from apps on unmanaged devices - 2022/05/10	Cloud apps	Report-only	No
[SharePoint admin center]Use app-enforced Restrictions for browser access - 2022/05/10	Cloud apps	On	No
Block Accessing confidential Apps from Non-trusted IP	Location	On	Yes

# 25) Prevent Users from creating Azure AD tenant

Users can create tenants in the Azure AD and Entra administration portal under Manage tenant. The creation of a tenant is recorded in the Audit log as category Directory Management and activity Create Company. Anyone who creates a tenant becomes the Global Administrator of that tenant. The newly created tenant doesn't inherit any settings or configurations.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar is titled "Azure Active Directory" and includes options for "Overview", "Users", "All users", "Deleted users", "User settings" (which is selected and highlighted), "Groups", and "Devices". The main content area is titled "Users | User settings" and contains a "Search" bar, "Save" and "Discard" buttons, and a "Got feedback?" link. A yellow box highlights the "Tenant creation" section, which says "Restrict non-admin users from creating tenants (preview)" with "Learn more" and "Yes" and "No" buttons. Below this are sections for "Manage" (with "Deleted users (preview)", "Password reset", "User settings" which is selected and highlighted, and "Bulk operation results"), "LinkedIn account connections" (with "Allow users to connect their work or school account with LinkedIn" and "Learn more about LinkedIn account connections"), and "Show keep user signed in".