



The Comprehensive Guide to Secure Azure AD & User Identities

By: Mohamed Mokhtar
<https://mokhtar.cloud>
version: 1.1

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.....	27
11) Use Just in Time privileged access to Office 365 roles	29
12) Ensure Security Defaults are disabled on Azure AD.....	36
13) Ensure that LinkedIn contact synchronization is disabled.	37
14) Ensure Sign-in frequency is Enabled, and browser sessions are not persistent for Administrative Users.	38
15) Ensure the option to remain signed in is hidden.....	40
16) Do not expire passwords.....	41
17) Ensure Administrative accounts are separate and cloud-only	42
18) Passwordless sign-in with the Microsoft Authenticator app	43
19) Passwordless: Windows Hello for Business.....	44
20) New feature: Azure AD Authentication Strengths (Preview).....	52
21) Regularly Check identity secure score	56
22) Require trusted location for MFA and SSPR registration	57
23) Tenant restrictions	60

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.

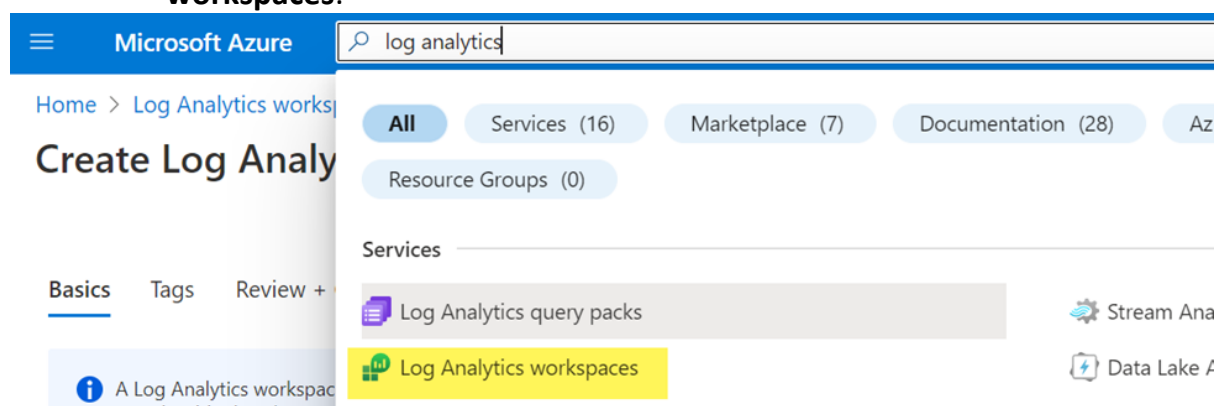
These accounts should be cloud-only accounts that use the *.onmicrosoft.com domain and that are not federated or synchronized from an on-premises environment

1. Log in to <https://aad.portal.azure.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**.



Microsoft Azure Search resources, services, and docs (G+)

Home > Log Analytics workspaces >

Create Log Analytics workspace

Basics Tags Review + Create

i 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](#)

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

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

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Name * ⓘ ✓

Region * ⓘ

- Azure Log Analytics workspace created
- Then go to **Azure Active Directory > 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

Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name AzureADLogs

Logs

Categories

- ☒ AuditLogs
- ☒ SignInLogs
- ☐ NonInteractiveUserSignInLogs
- ☐ ServicePrincipalSignInLogs
- ☐ ManagedIdentitySignInLogs
- ☐ ProvisioningLogs
- ☐ ADFSSignInLogs
- ☐ RiskyUsers
- ☐ UserRiskEvents
- ☐ NetworkAccessTrafficLogs
- ☐ RiskyServicePrincipals
- ☐ ServicePrincipalRiskEvents

Destination details

- ☒ Send to Log Analytics workspace
- Subscription
 -
- Log Analytics workspace
 - LogAnalytics (northeurope)
- ☐ Archive to a storage account
- ☐ Stream to an event hub
- ☐ Send to partner solution

i In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, [start a free trial](#).

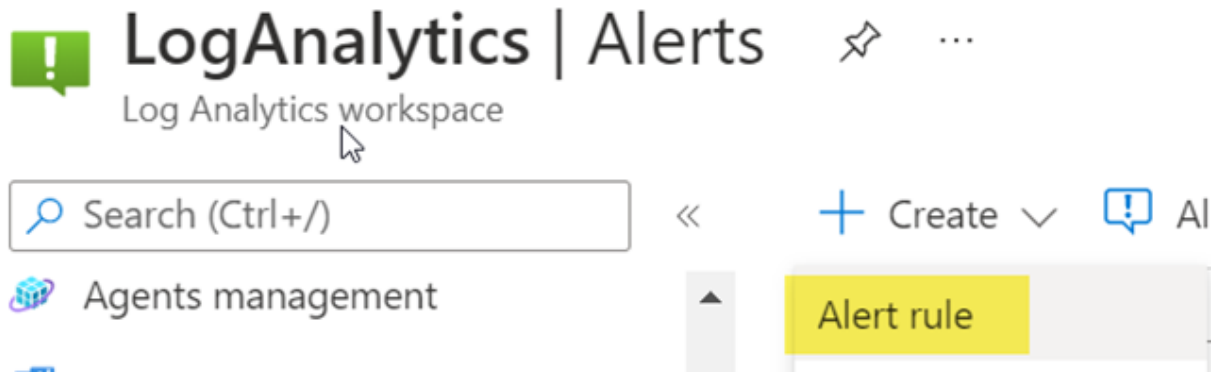
Obtain Object IDs of the break glass accounts

1. Sign in to the [Azure portal](#) or [Azure AD admin center](#) with an account assigned to the User Administrator role.
2. Select **Azure Active Directory > 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.

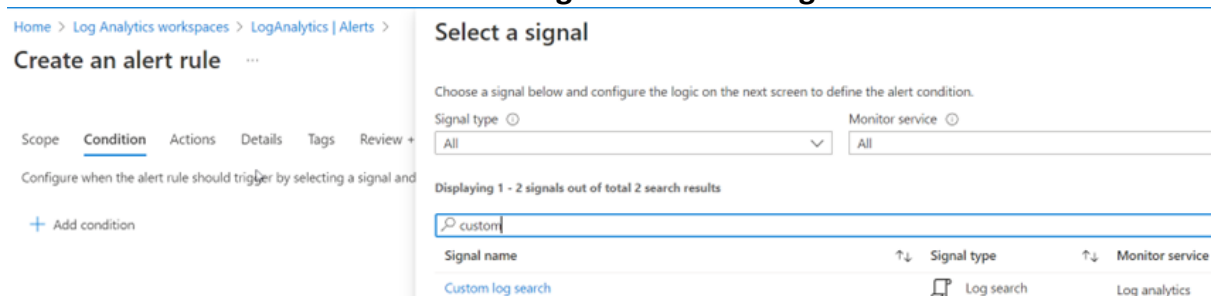
User principal name	 @elshreef.net 
Object ID	da8eb00b-5649-426f-992a-d9771d98465e 
Created date time	May 30, 2022, 6:16 PM
User type	Member

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**.



- 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**.



- 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”



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 == "da8eb0b-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	☐

Alert logic

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 ▼		

Email/SMS message/Push/Voice ×

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

☒ Email

Email * ⓘ <outlook.com> ✓

☒ SMS (Carrier charges may apply)

Country code * 971 ✓

Phone number * 5431C ✓

☐ Azure mobile app notification

Azure account email ⓘ

☐ Voice

Country code ⓘ 1

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 * ⓘ [Create new](#)

Alert rule details

Severity * ⓘ

Alert rule name * ⓘ

Alert rule description ⓘ

Region * ⓘ

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

Table rows

Aggregation type

Count

Aggregation granularity

5 minutes

Advanced options

Resource ID column

dontSplit

Alert logic

Operator

GreaterThan

Threshold value

Frequency of evaluation

5 minutes

Advanced options

Number of violations

1 violations

Evaluation period

5 minutes (1 aggregated points)

Actions

Action group name

Contain actions

Break-Glass-AG

1 Email, 1 SMS message ⓘ

Details

Project details

Subscription

VPN MSDN Platforms

Resource group

RG-BG-01

Region

northeurope

Alert rule details

Severity

 0 - Critical

Alert rule name

Emergency Access

Alert rule description

Advanced options

Enable upon creation

☒

Automatically resolve alerts (preview)

☐

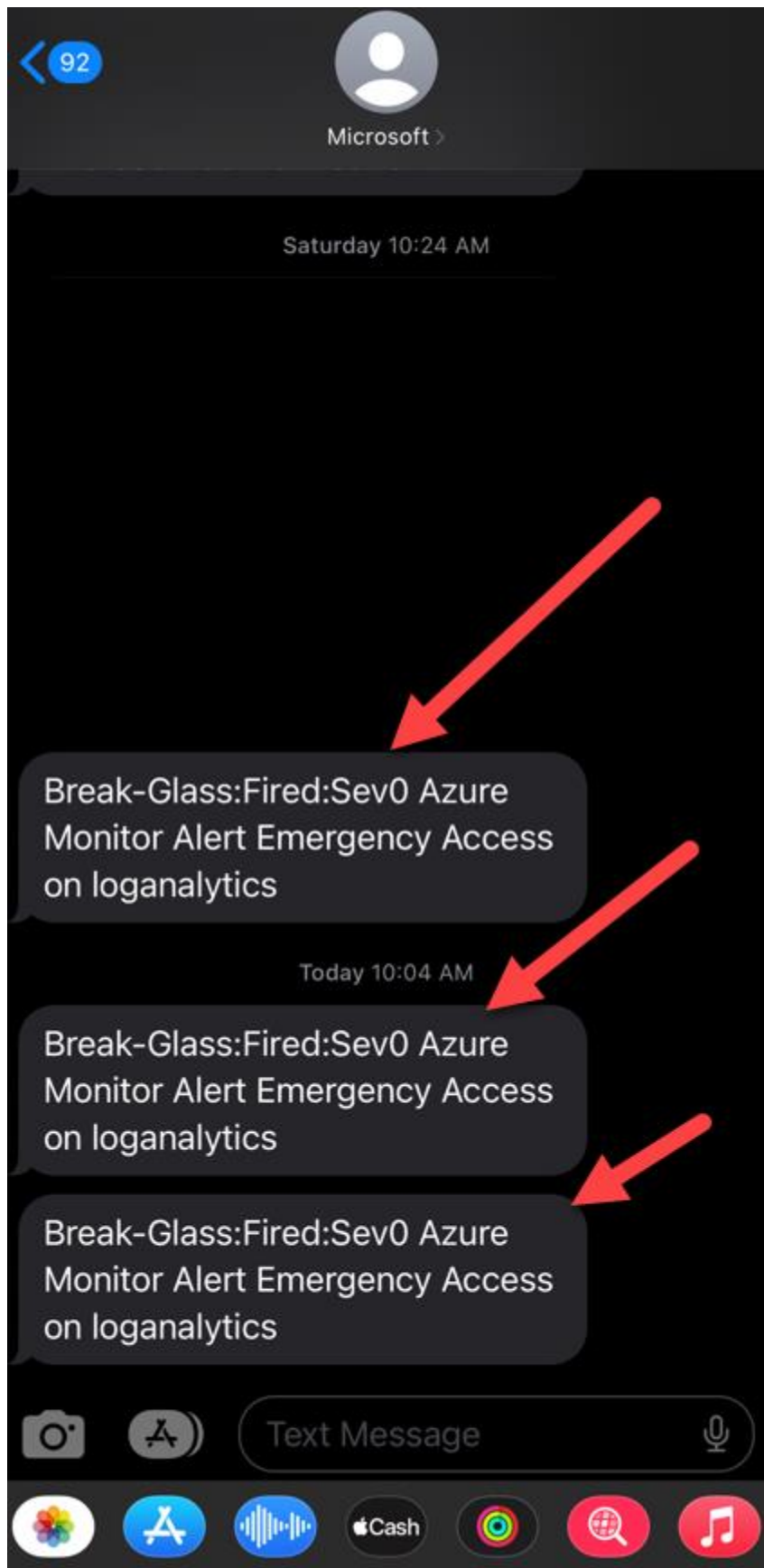
Require a workspace linked storage

☐

Create

Previous

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



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

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

Summary

Alert name	Emergency Access
Severity	Sev0
Monitor condition	Fired
Affected resource	loganalytics

2) Require multifactor authentication for administrative roles

1. Log in to <https://aad.portal.azure.com/>
2. Select Security, 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., 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](#)

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

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... ✓

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

[Learn more](#)

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://aad.portal.azure.com/>
2. Select Security, then select Conditional Access.
3. Create a policy which require MFA authentication from all users

Home > Mokhtar.Cloud | Security > Security | Conditional Access > Conditional Access | Policies >

Require MFA for all users

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 *

Require MFA for all users

Assignments

Users ⓘ

[All 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](#)

Grant

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

☐ Block access

☒ Grant access

☒ Require multifactor authentication ⓘ

Consider testing the new "Require authentication strength" public preview

☐ Require authentication strength (Preview) ⓘ

"Require authentication strength" cannot be used with "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 ⓘ

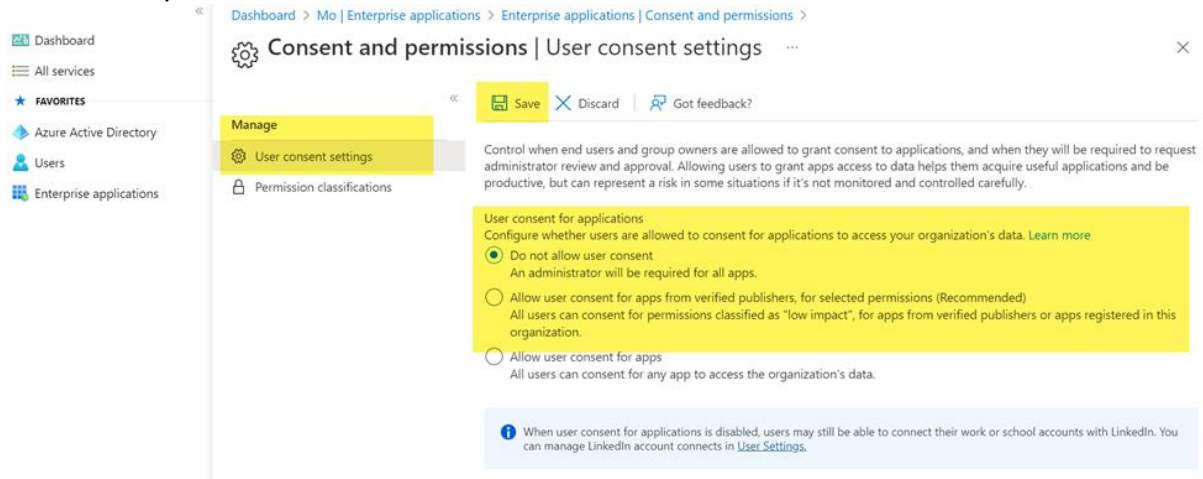
For multiple controls

☐ Require all the selected controls

☒ Require one of the selected controls

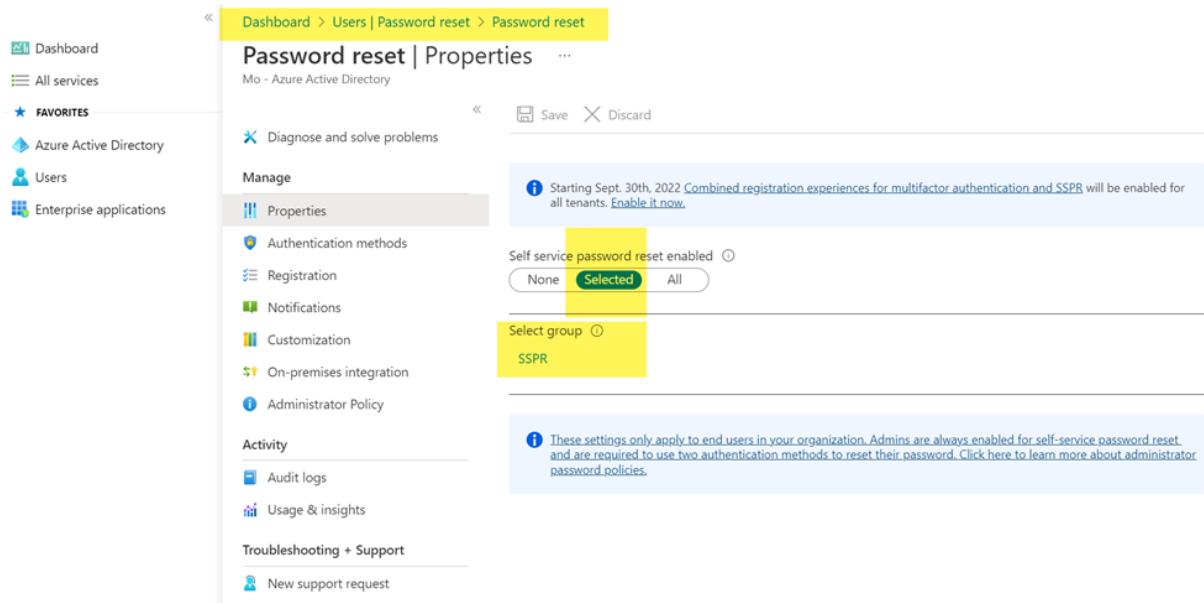
4) Do not allow Users to grant consent to unreliable applications

1. Log in to <https://aad.portal.azure.com/>
2. Go to Azure Active Directory > Enterprise applications > Consent and permissions



5) Enable Self-Service Password Reset

1. Create a Group called SSPR or any other name
2. Log in to <https://aad.portal.azure.com/>
3. Choose Users from the left-hand navigation.
4. Choose Password reset.
5. On the Properties page, select the SSPR group which you created at step1
6. Select Save.



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://aad.portal.azure.com/>
3. Select Security on the left side navigation followed by 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.

Home > Mokhtar.Cloud | Security > Security | Authentication methods > Authentication methods

Authentication methods | Password protection 🔑 ...

Mokhtar.Cloud - Azure AD Security

Search « Save Discard

Manage

- Policies
- Password protection**
- Registration campaign
- Authentication strengths (Preview)

Monitoring

- Activity
- User registration details
- Registration and reset events
- Bulk operation results

Custom smart lockout

Lockout threshold ⓘ

Lockout duration in seconds ⓘ

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

Egypt

Mokhtar

✓

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

- 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://aad.portal.azure.com/>
2. Select Security.
3. Select Conditional Access.
4. Create a new policy by selecting new policy.
5. Set the following conditions within the policy.
6. 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](#)

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

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

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

Dashboard > Mo | Security > Security | Conditional Access > Conditional Access | Policies >

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](#)

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

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

User risk level

Not configured

Sign-in risk level

Not configured

Device platforms

Not configured

Locations

Not configured

Client apps

2 included

Filter for devices

Not configured

Client apps

Control user access to target specific client applications not using modern authentication. [Learn more](#)

Configure

Yes No

Select the client apps this policy will apply to

Modern authentication clients

☐ Browser

☐ Mobile apps and desktop clients

Legacy authentication clients

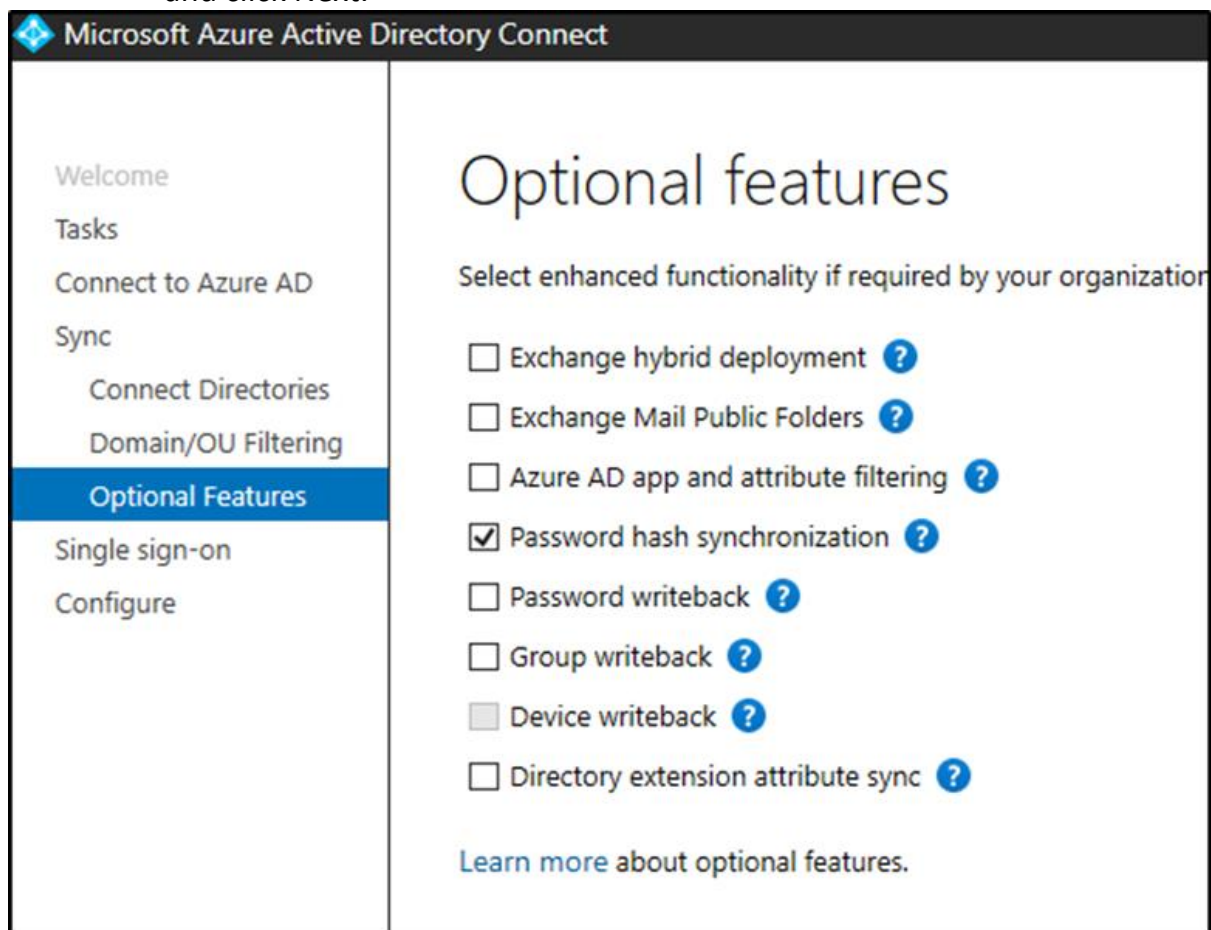
☒ Exchange ActiveSync clients

☒ Other clients

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://aad.portal.azure.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 multi-factor authentication.
6. Set the policy to on then Save

Dashboard > Mo | Security > Security | Identity Protection > Identity Protection

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

Overview

Diagnose and solve problems

Protect

User risk policy

Sign-in risk policy

Multifactor authentication registration policy

Report

Risky users

Risky workload identities (preview)

Risky sign-ins

Risk detections

Notify

Users at risk detected alerts

Weekly digest

Troubleshooting + Support

Virtual assistant (Preview)

Troubleshoot

New support request

Policy Name

Sign-in risk remediation policy

Assignments

Users

All users

Sign-in risk ⓘ

Medium and above

Controls

Access ⓘ

Require multifactor authentication

Enforce policy

On

Off

Save

Access ×

Sign-in risk remediation policy

Control access enforcement to block or grant access.

Select the controls to be enforced.

☐ Block access

☒ Allow access

☒ Require multifactor authentication

Done

10) Enable Azure AD Identity Protection

User risk policies

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

1. Log in to <https://aad.portal.azure.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

Dashboard > Mo | Security > Security | Identity Protection > Identity Protection

Identity Protection | User risk policy ...

Search (Ctrl+J)

Overview

Diagnose and solve problems

Protect

User risk policy

Sign-in risk policy

Multifactor authentication registration policy

Report

Risky users

Risky workload identities (preview)

Risky sign-ins

Risk detections

Notify

Users at risk detected alerts

Weekly digest

Troubleshooting + Support

Virtual assistant (Preview)

Troubleshoot

New support request

Policy Name

User risk remediation policy

Assignments

Users

All users

User risk

Medium and above

Controls

Access

Require password change

Enforce policy

On

Off

Save

Access

User risk remediation policy

Control access enforcement to block or grant access.

Select the controls to be enforced.

☐ Block access

☒ Allow access

☒ Require password change

Done

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 Azure portal as global administrator by going to <https://portal.azure.com>
- In the Azure portal, click Services and search for and click on Azure AD
- 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

[Home](#) > [Privileged Identity Management | Azure AD roles](#) > [Mokhtar.Cloud | Roles](#) > [Global Administrator | Assignments](#)

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

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

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](#)

[Home](#) > [Privileged Identity Management | Azure AD roles](#) > [Mokhtar.Cloud | Roles](#) > [Global /](#)

Add assignments

Privileged Identity Management | Azure AD roles

Membership **Setting**

Assignment type ⓘ

☒ Eligible

☐ Active

Maximum allowed eligible duration is permanent.

☐ Permanently eligible

Assignment starts *

10/27/2022



8:00:06 PM

Assignment ends *

10/27/2023



8:00:06 PM

[Home](#) > [Privileged Identity Management | Azure AD roles](#) > [Mokhtar.Cloud | Roles](#) >

Global Administrator | Assignments

Privileged Identity Management | Azure AD roles

Manage

Assignments

Description

Role settings

« + 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	Membership	Start time	End time	Action
Global Administrator							
admin	admin@elshreef.net	User	Directory	Direct	10/27/2022, 8:01:35 PM	10/27/2023, 8:00:06 PM	Remove Update Ex

To configure Global Reader Role as per the above table

- Sign-on to your Azure portal as global administrator by going to <https://portal.azure.com>
- In the Azure portal, click Services and search for and click on Azure AD
- 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

[«](#) [+ Add assignments](#) [Settings](#) [Refresh](#) [Export](#) | [Got feedback?](#)

Manage

[Assignments](#)

[Description](#)

[Role settings](#)

Eligible assignments **Active assignments** **Expired assignments**

Name	Principal name	Type	Scope
No results			

Select Admin

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

Add assignments

Privileged Identity Management | Azure AD roles

Membership

Setting

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

Resource

Mokhtar.Cloud

Resource type

Directory

Select role 

Global Reader

Scope type 

Directory

Select member(s) * 

1 Member(s) selected

Selected member(s) 



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

To disable security defaults in your directory:

1. Log in to <https://aad.portal.azure.com/>
2. Browse to Azure Active Directory > Properties.
3. Select Manage security defaults.
4. Set the Enable security defaults toggle to No.
5. Select Save.

The screenshot shows the Azure Active Directory (Mo) Properties page. On the left is a navigation pane with sections like Overview, Preview features, and Manage. The 'Manage' section is expanded, showing options like Users, Groups, and External Identities. The main content area displays 'Tenant properties' with fields for Name (Mo), Location (EU Model Clause compliant datacenters), Notification language (English), Tenant ID (0c916b26-5cf7-4f3d-8f73-dada221b4efc), Technical contact (mohamed@elshreef.net), Global privacy contact, and Privacy statement URL. Below these is the 'Access management for Azure resources' section, which includes a toggle for 'Mohamed Mo groups in this tenant' set to 'No'. At the bottom of the main content area is a yellow button labeled 'Manage security defaults'. A modal dialog titled 'Enable security defaults' is open on the right, showing a description of security defaults and a toggle set to 'No'.

Dashboard > Mo

Mo | Properties
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
Identity Governance
Application proxy
Custom security attributes (Preview)
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding

Save Discard Got feedback?

Tenant properties

Name *
Mo

Location
EU Model Clause compliant datacenters

Notification language
English

Tenant ID
0c916b26-5cf7-4f3d-8f73-dada221b4efc

Technical contact
mohamed@elshreef.net

Global privacy contact

Privacy statement URL

Access management for Azure resources

Mohamed Mo groups in this tenant. [Learn more](#)
Yes No

Manage security defaults

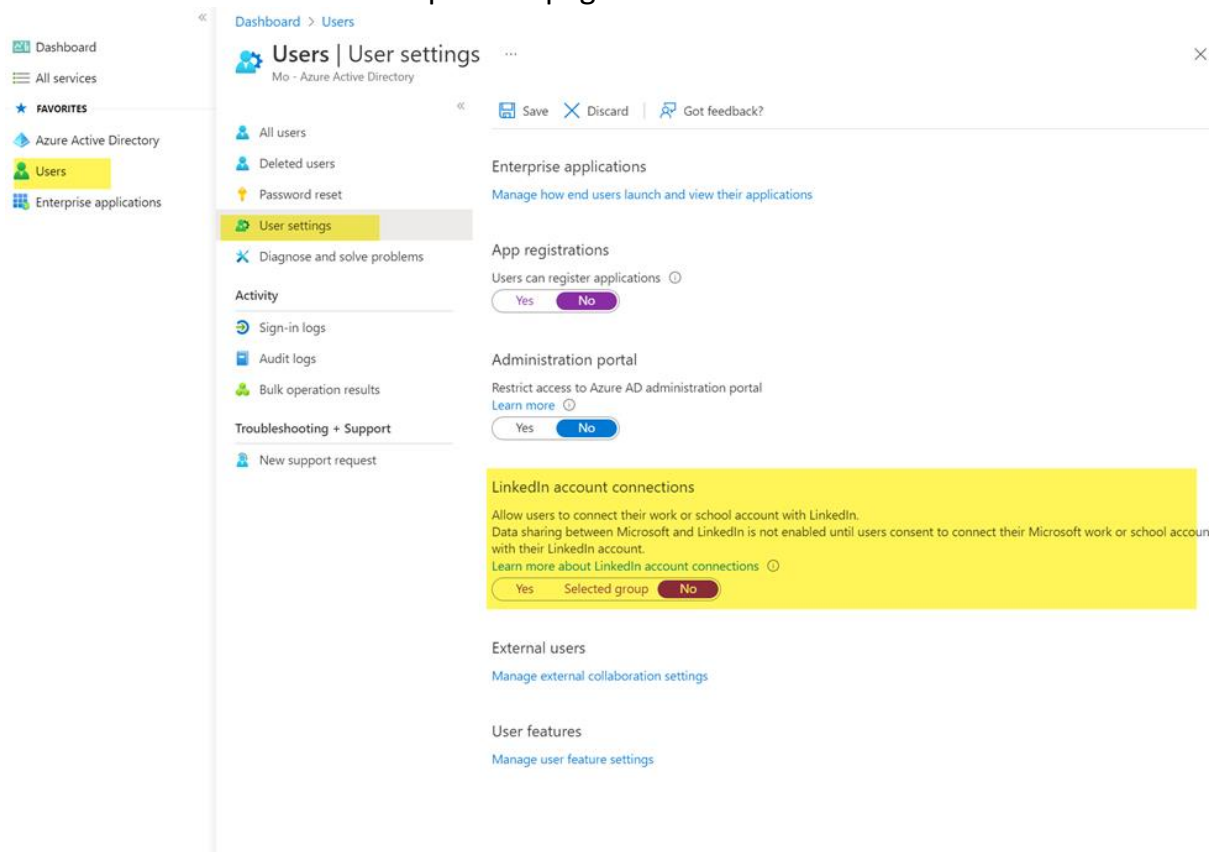
Enable security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be better protected from common identity-related attacks. [Learn more](#)

Enable security defaults
Yes No

13) Ensure that LinkedIn contact synchronization is disabled.

1. Log in to <https://aad.portal.azure.com/>
 2. Once the Azure AD Admin center is open select Users followed by User Settings then User settings.
- Under LinkedIn account connections then click No.
 - Click Save at the top of the page.



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

1. Log in to <https://aad.portal.azure.com/>
2. Select Security, 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.

Home > Mokhtar.Cloud | Security > Security | Conditional Access > Conditional Access | Policies >

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 *

Require multifactor authentication for admini...

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

i 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

4

Hours

☐ Every time

☒ Persistent browser session

Persistent browser session

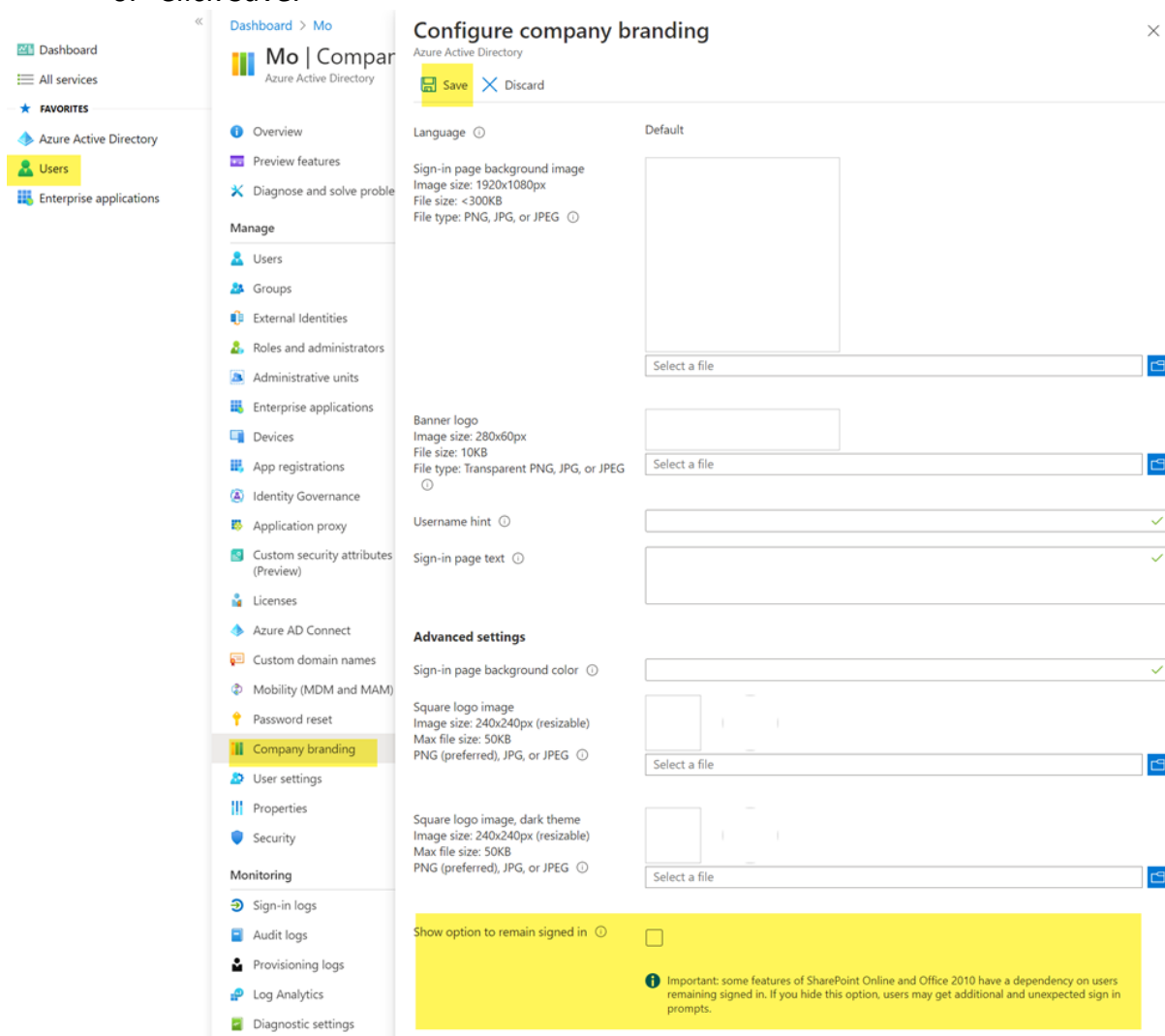
Never persistent

☐ Customize continuous access evaluation

☐ Disable resilience defaults

15) Ensure the option to remain signed in is hidden

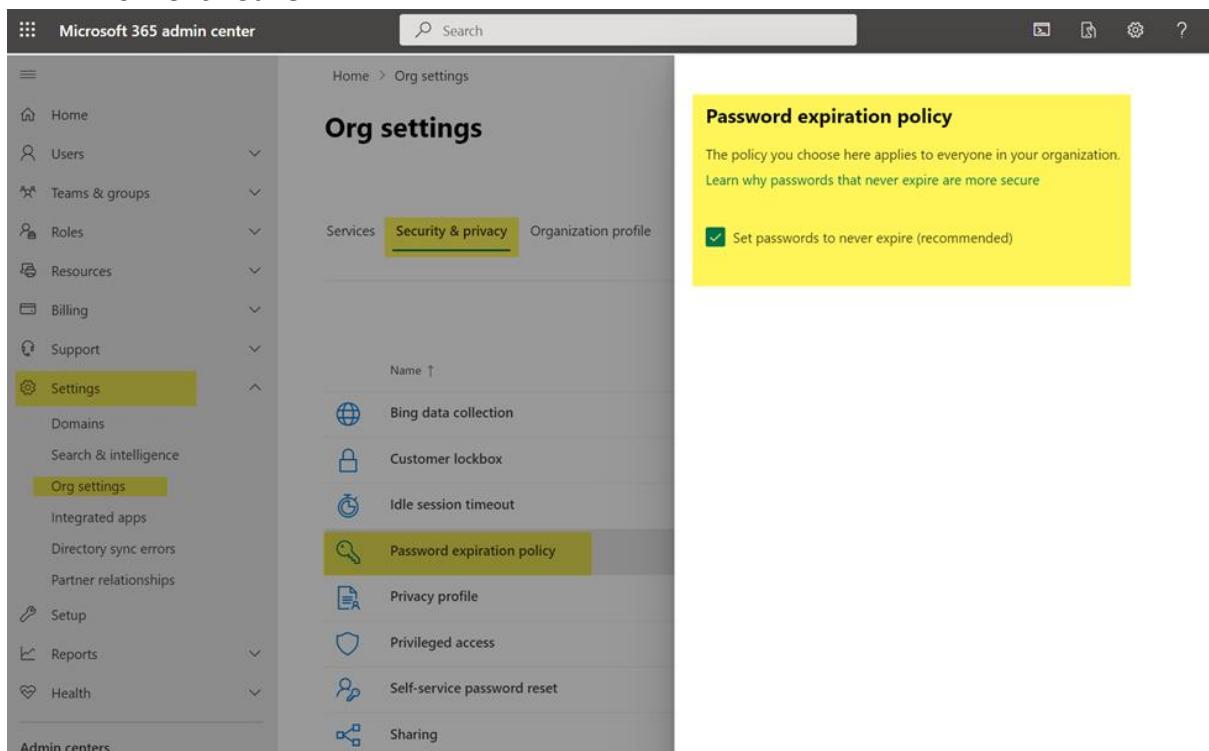
1. Log in to <https://aad.portal.azure.com/>
2. Click on Azure Active Directory
3. Under Manage select Company branding followed by the appropriate Locale policy.
4. If no policy exists, you will need to click Configure to create one
5. Scroll to the bottom of the newly opened pane and ensure Show option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



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.



17) Ensure Administrative accounts are separate and cloud-only

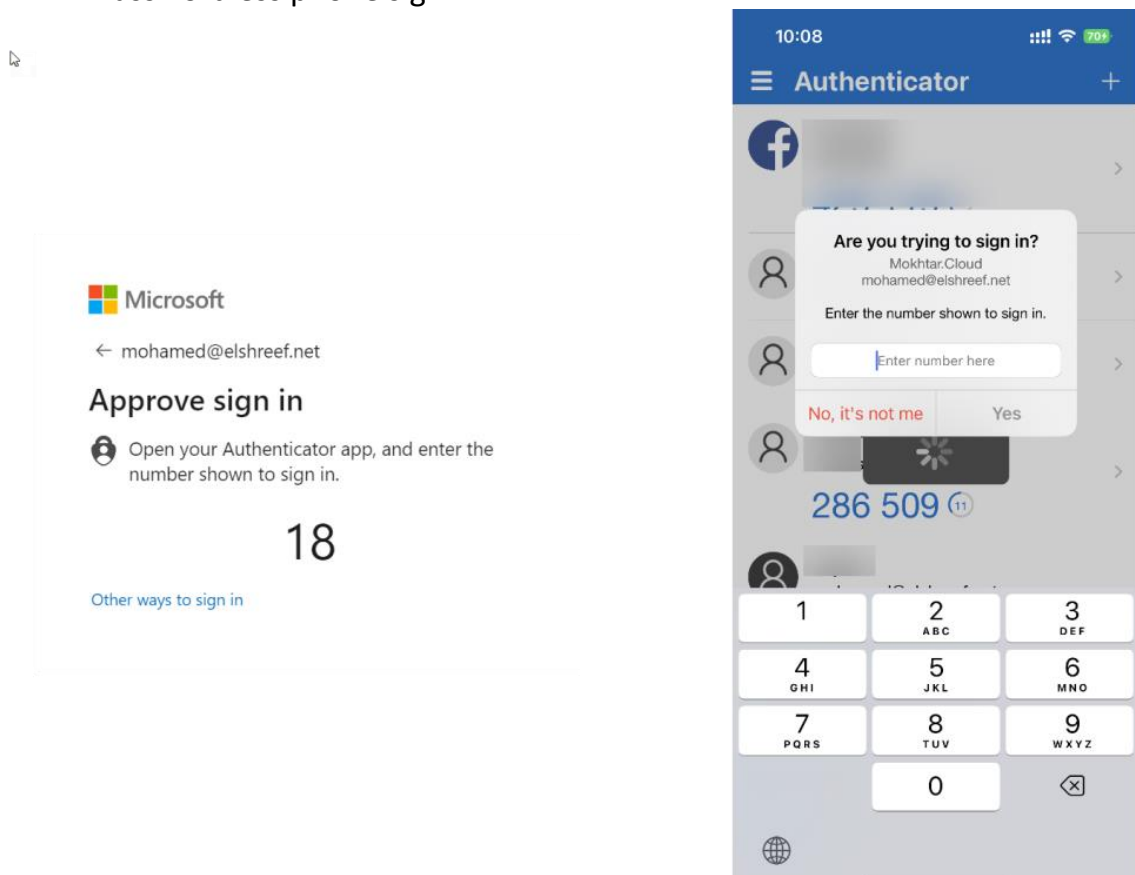
- Be sure to create separate accounts for users to do Global Administrator tasks.
- Make sure that your Global Administrators don't accidentally open emails or run programs with their administrator accounts.
- Be sure those accounts have their email forwarded to a working mailbox.
- Global Administrator (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

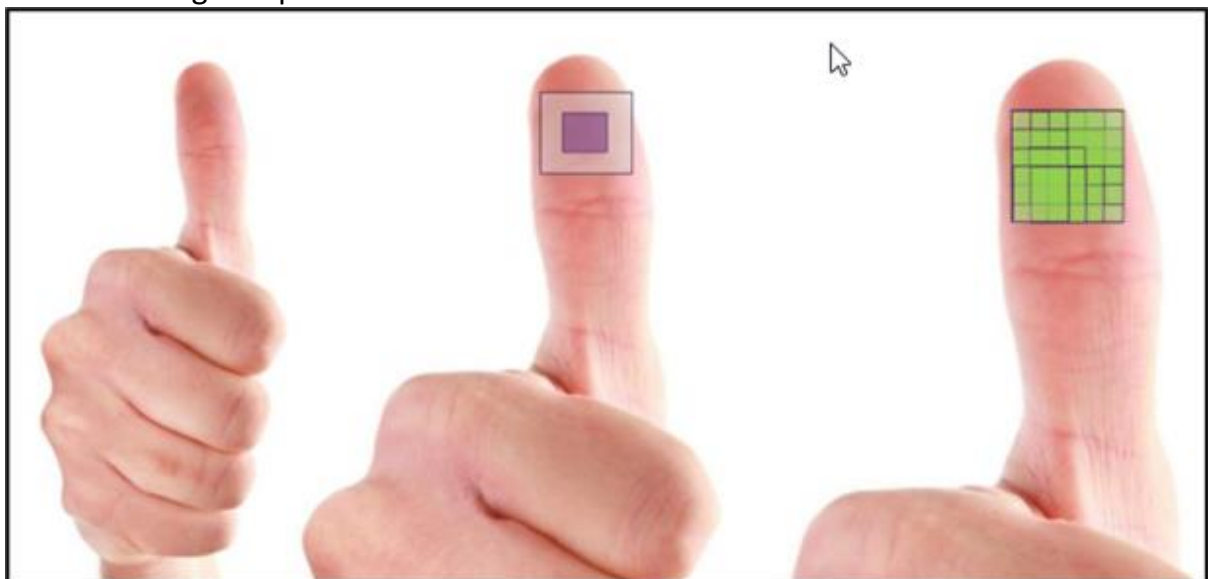
In Windows 10&11, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

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



Windows enrollment

^ Essentials

Last modified : 08/31/22, 10:05 AM

Assigned to : [All users.](#)

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

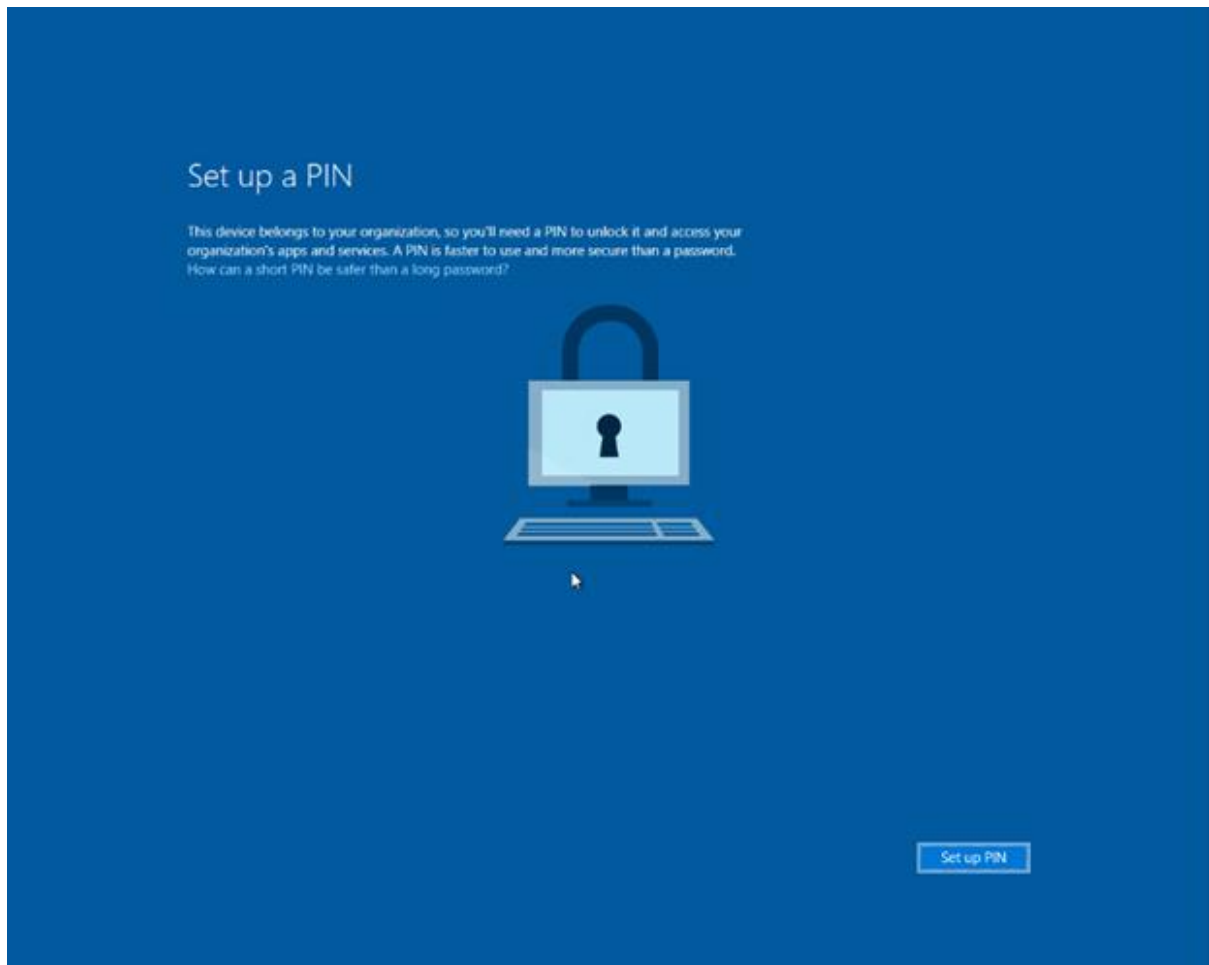
Use a Trusted Platform Module (TPM): ⓘ Required Preferred

Minimum PIN length: ⓘ 6 ✓

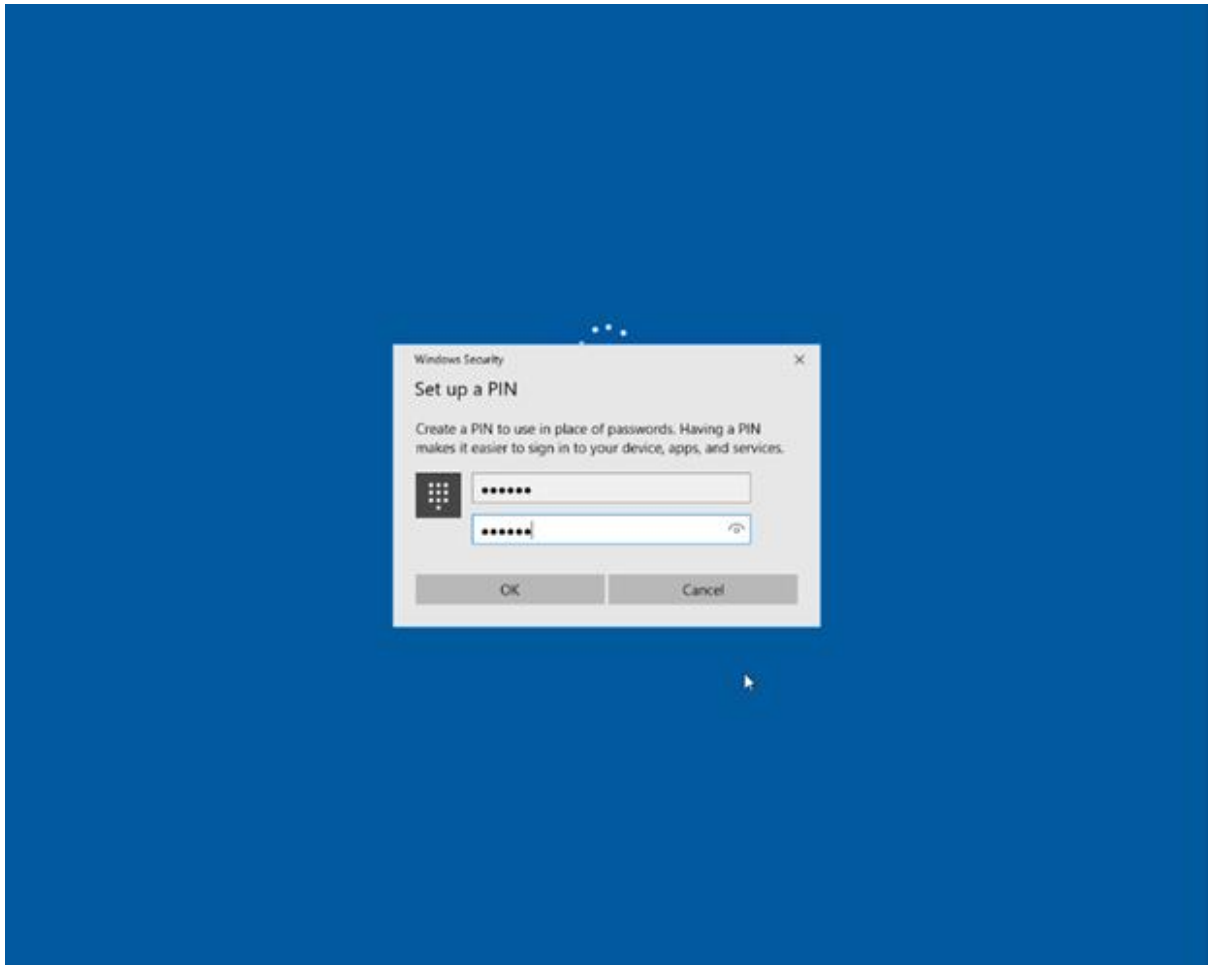
Configure Windows Hello for Business: ⓘ	Enabled	▼
Use a Trusted Platform Module (TPM): ⓘ	Required	Preferred
Minimum PIN length: ⓘ	6	✓
Maximum PIN length: ⓘ	127	✓
Lowercase letters in PIN: ⓘ	Not allowed	▼
Uppercase letters in PIN: ⓘ	Not allowed	▼
Special characters in PIN: ⓘ	Not allowed	▼
PIN expiration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

Registration

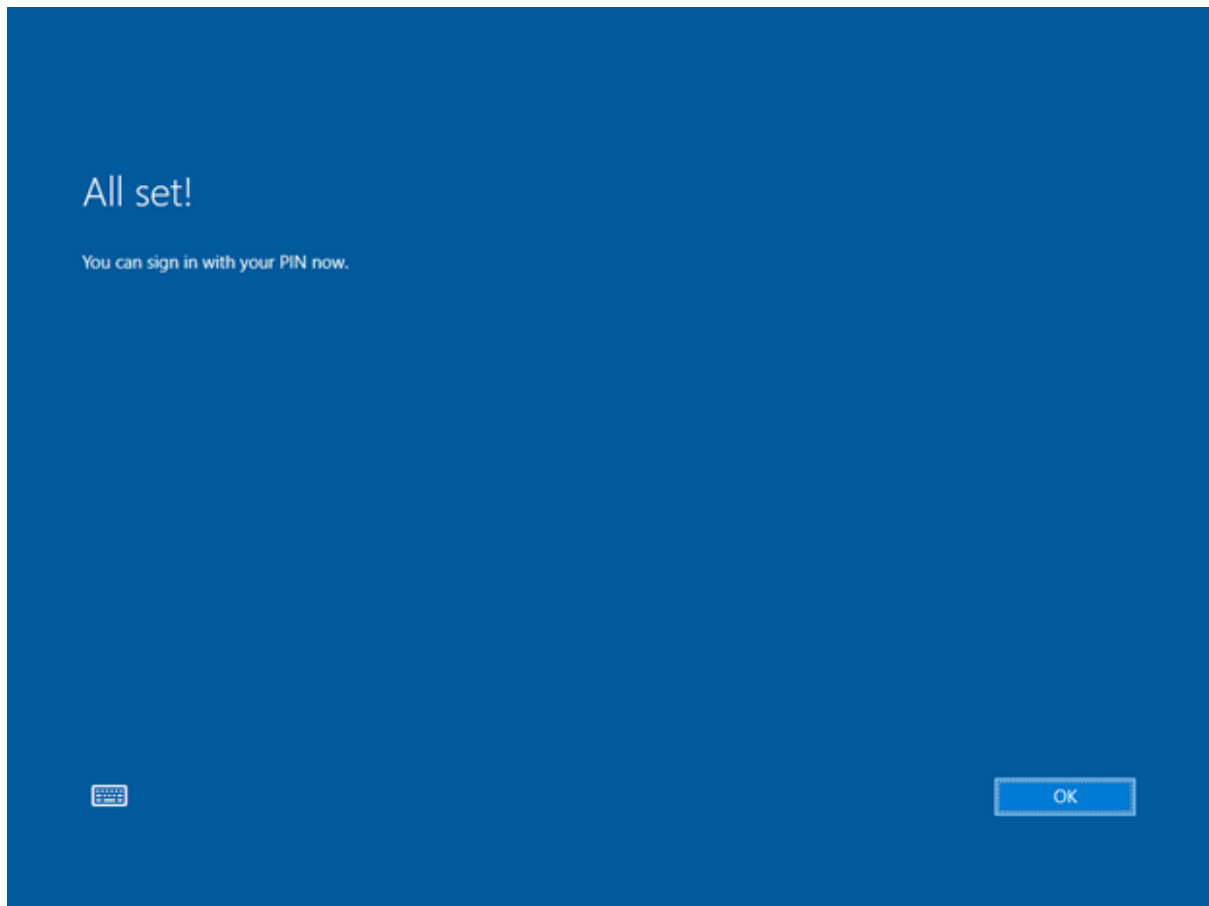
Windows Hello for Business provisioning begins with a full screen page with the title **Setup a PIN** and button with the same name. The user clicks **Setup a PIN**.



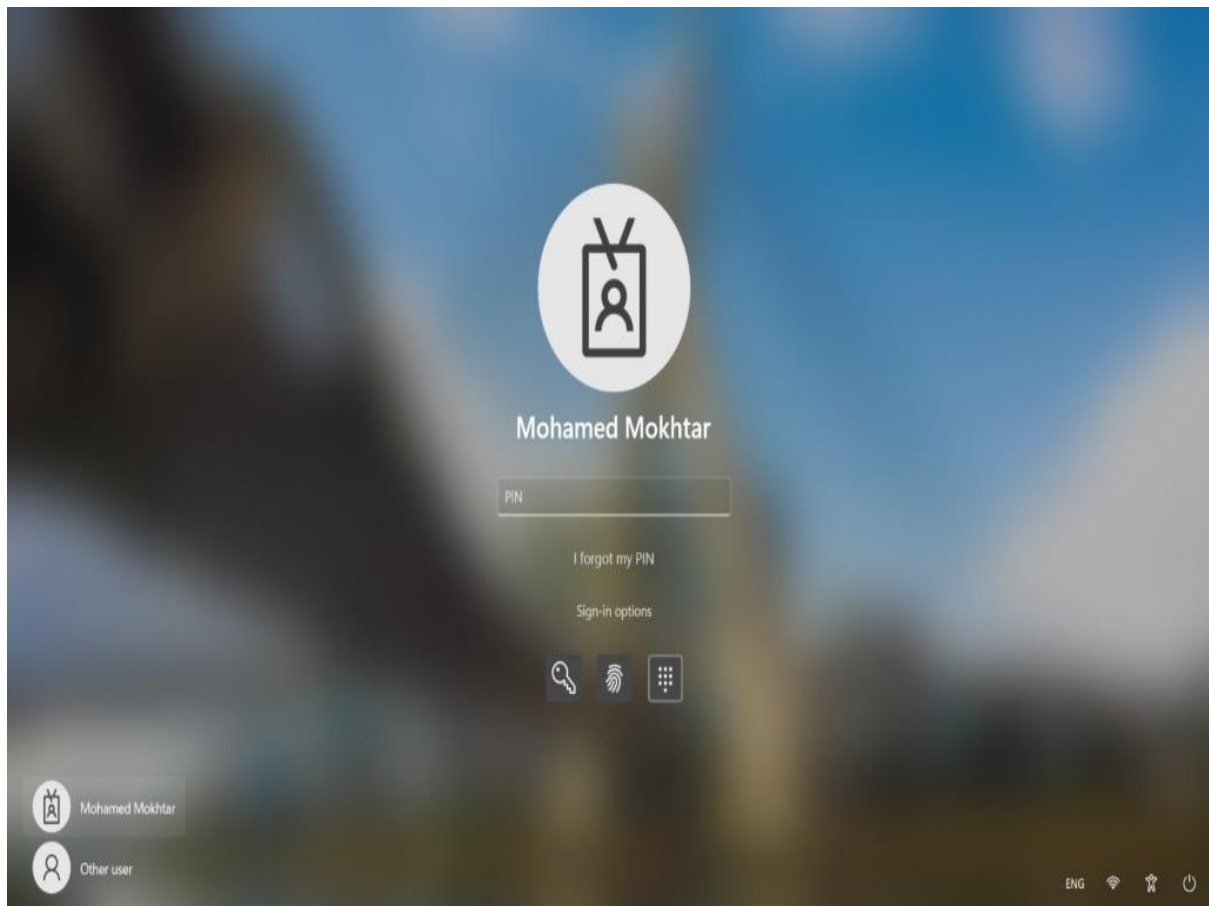
After a successful MFA, the provisioning flow asks the user to create and validate a PIN. This PIN must observe any PIN complexity requirements that you deployed to the environment.



All set!



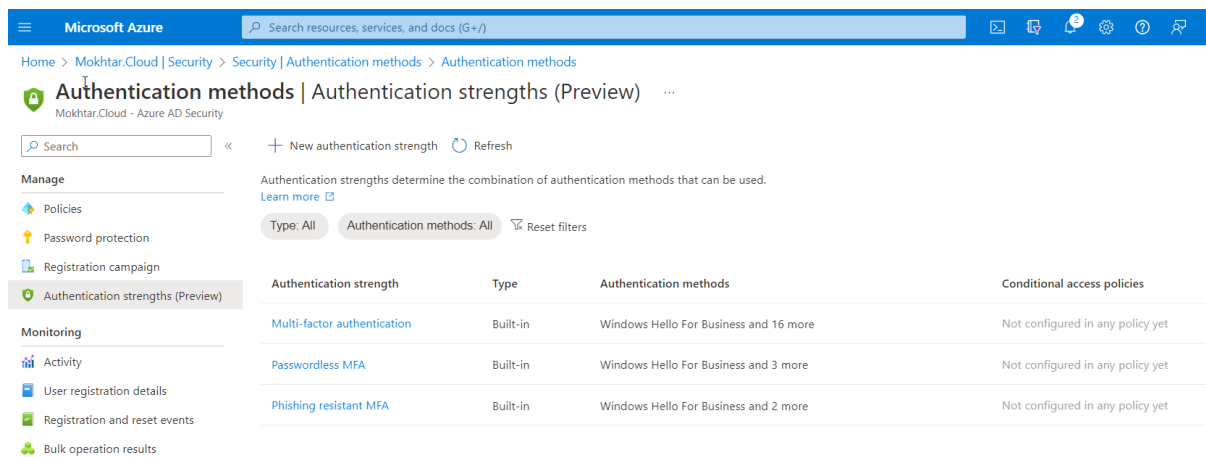
The last thing to do is to check if everything works fine



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

Microsoft has released a new feature called Authentication Strength, the new feature will enable the IT admin to force the combination of authentication methods that can be used with the conditional access.

The following screenshot shows the new feature



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the path: Home > Mokhtar.Cloud | Security > Security | Authentication methods > Authentication methods. The main heading is 'Authentication methods | Authentication strengths (Preview)'. Below this, there's a search bar and a '+ New authentication strength' button. The left sidebar shows the 'Manage' section with options like Policies, Password protection, Registration campaign, and Authentication strengths (Preview). The main content area shows a table of authentication strengths.

Authentication strength	Type	Authentication methods	Conditional access policies
Multi-factor 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	Not configured in any policy yet
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 OR FIDO2 Security Key OR Certificate Based Authentication (Multi-Factor) OR Microsoft Authenticator (Phone Sign-in)

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

Home > Mokhtar.Cloud | 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](#)

Name *
Force Passwordless for Microsoft Teams ✓

Assignments

Users or workload identities ⓘ

All users

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

0 controls selected

Enable policy

Report-only On Off

Create

Grant

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

☐ Block access
☒ Grant access

☐ Require multifactor authentication ⓘ

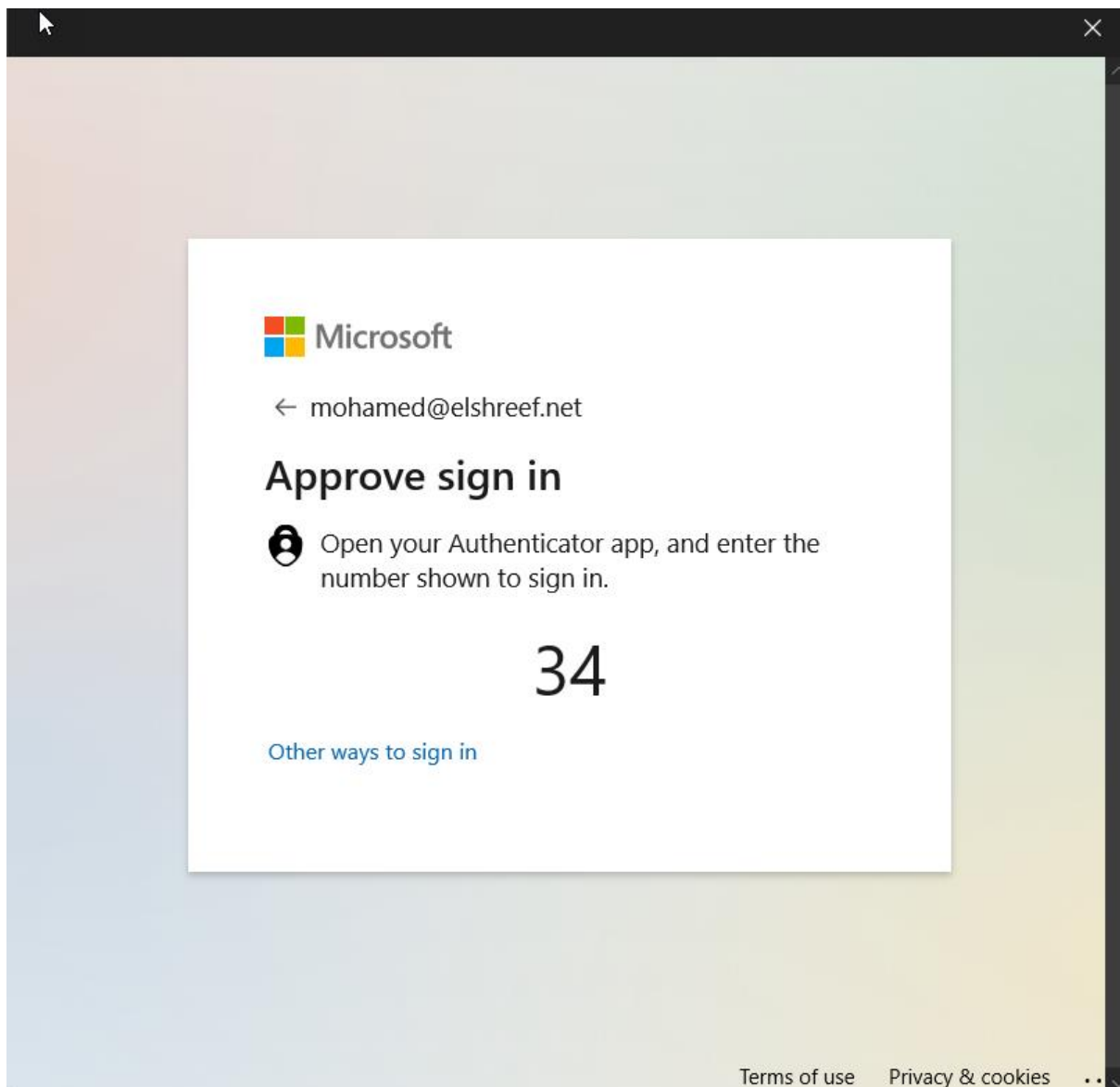
☒ Require authentication strength (Preview) ⓘ
Passwordless MFA

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication"

ℹ 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.

Select

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

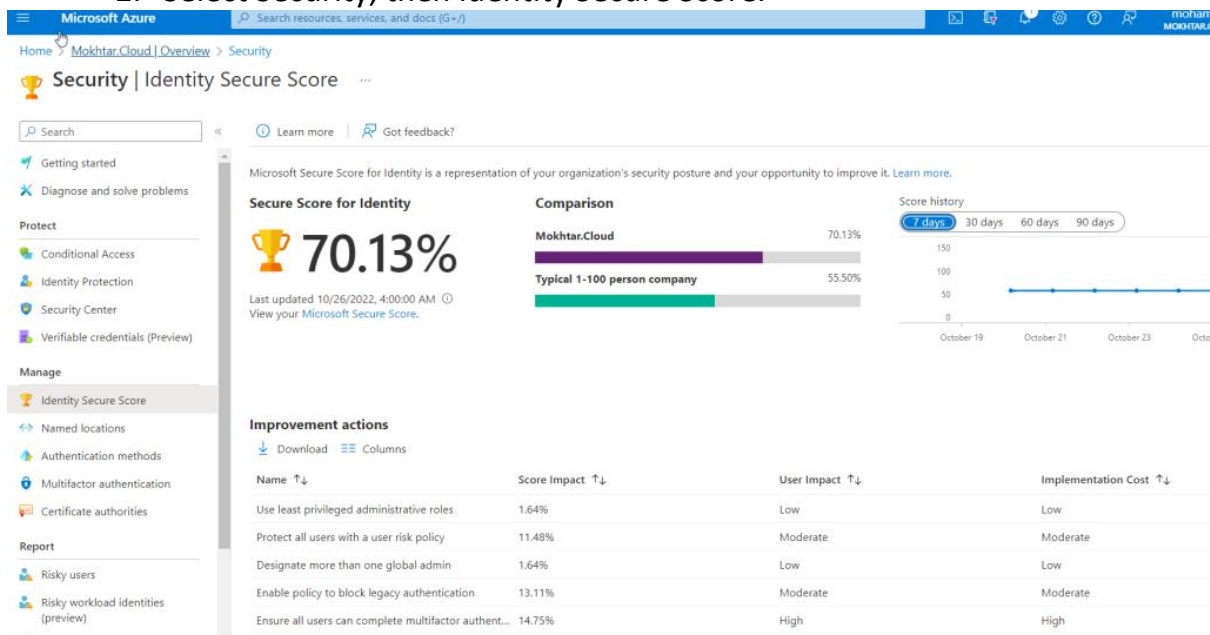
Authentication Strength(s)

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://aad.portal.azure.com/>
2. Select Security, then Identity Secure Score.



22) Require trusted location for MFA and SSPR registration

Log in to <https://aad.portal.azure.com/>
Select Security, 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.

[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...

What does this policy apply to?

Users and groups

Assignments

Users or workload identities ⓘ

All users included and specific users excluded

Include

Exclude

☐

None

☒

All users

☐

Select users and groups

Cloud apps or actions ⓘ

1 user action included

Conditions ⓘ

1 condition selected

Access controls



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.

Enable policy

Report-only

On

Off

Save

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

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

Enable policy

Report-only

On

Off

Save

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

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

Enable policy

Report-only ☒ On ☐ Off

Save

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 ⓘ

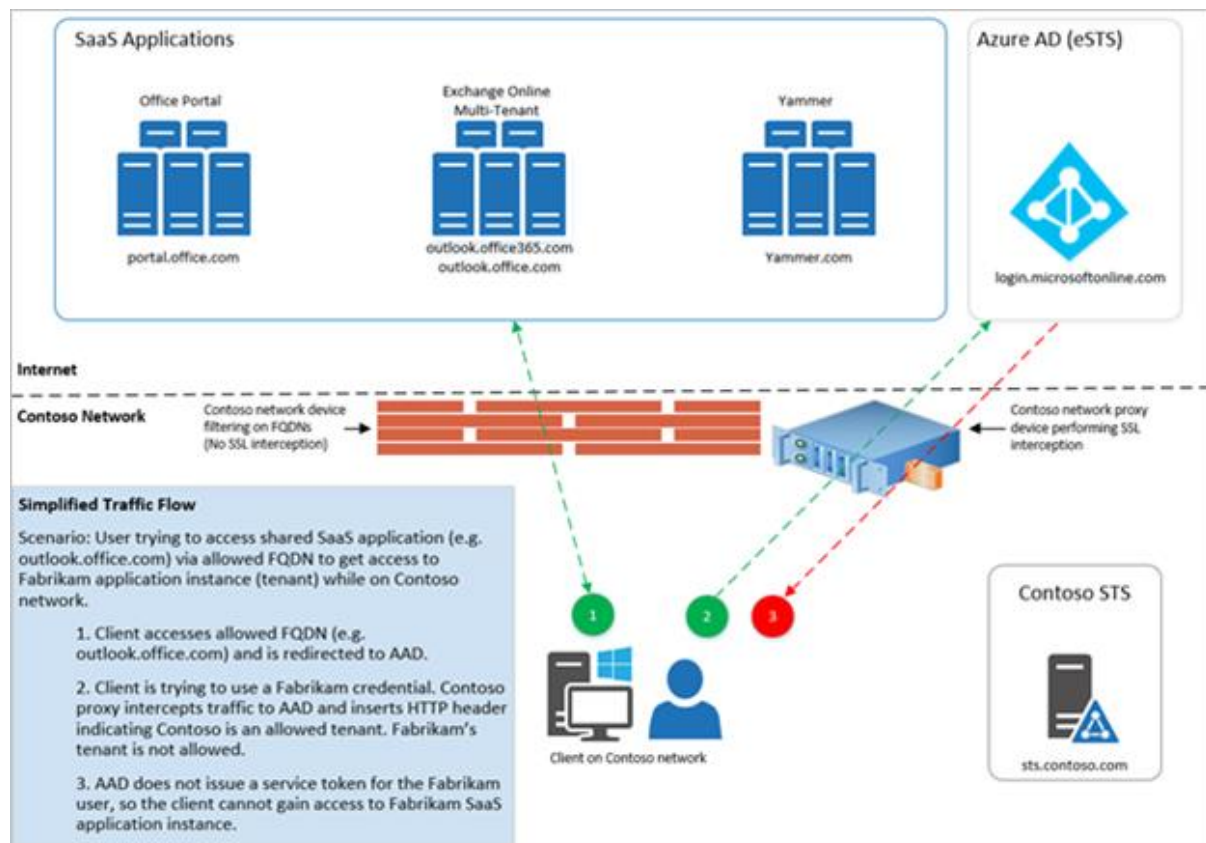
For multiple controls

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*

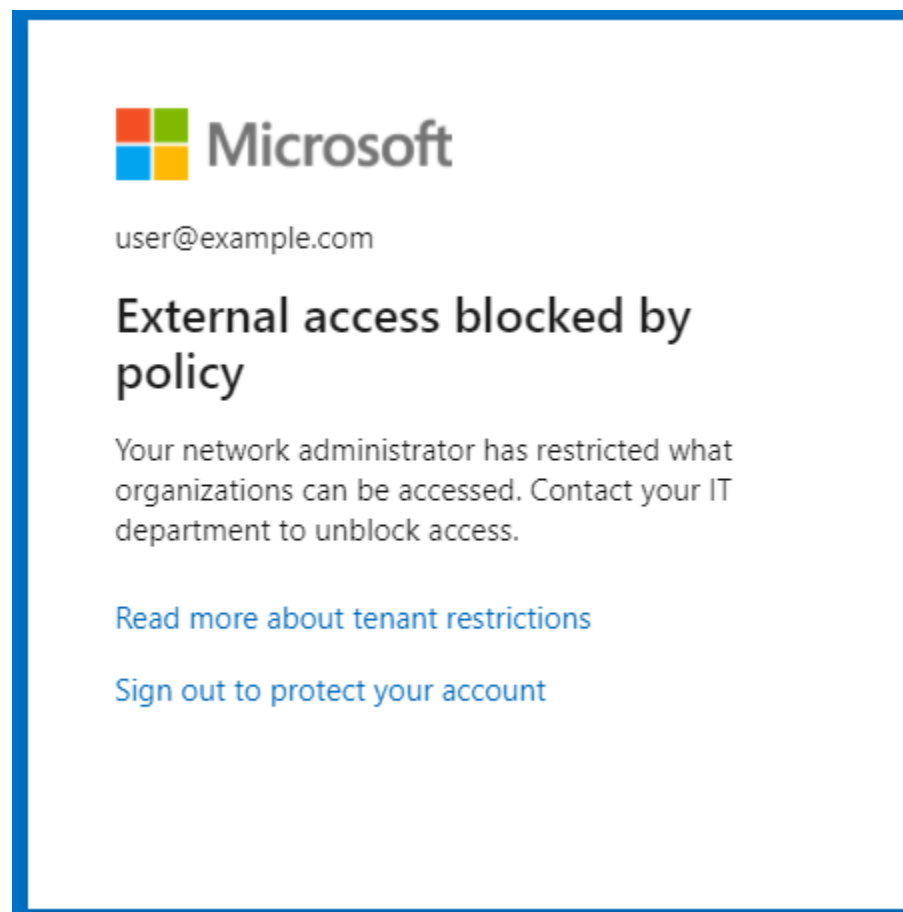
Restrict-Access-Context: 456ff232-3512-5h23-b3b3-3236w0826f3d

* 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