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

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.

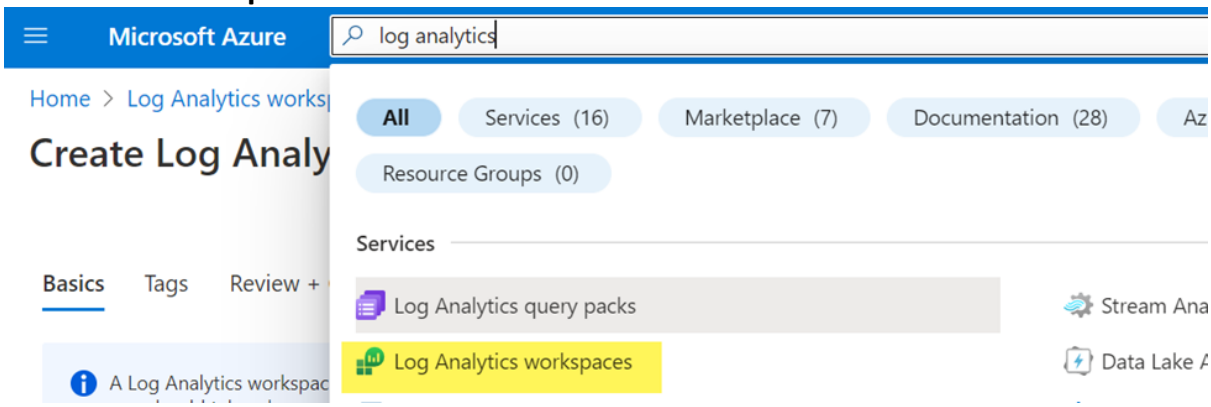
Create two or more emergency access accounts.
These accounts should be cloud-only accounts that use the *.onmicrosoft.com domain and that are not federated or synchronized from an on-premises environment

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.

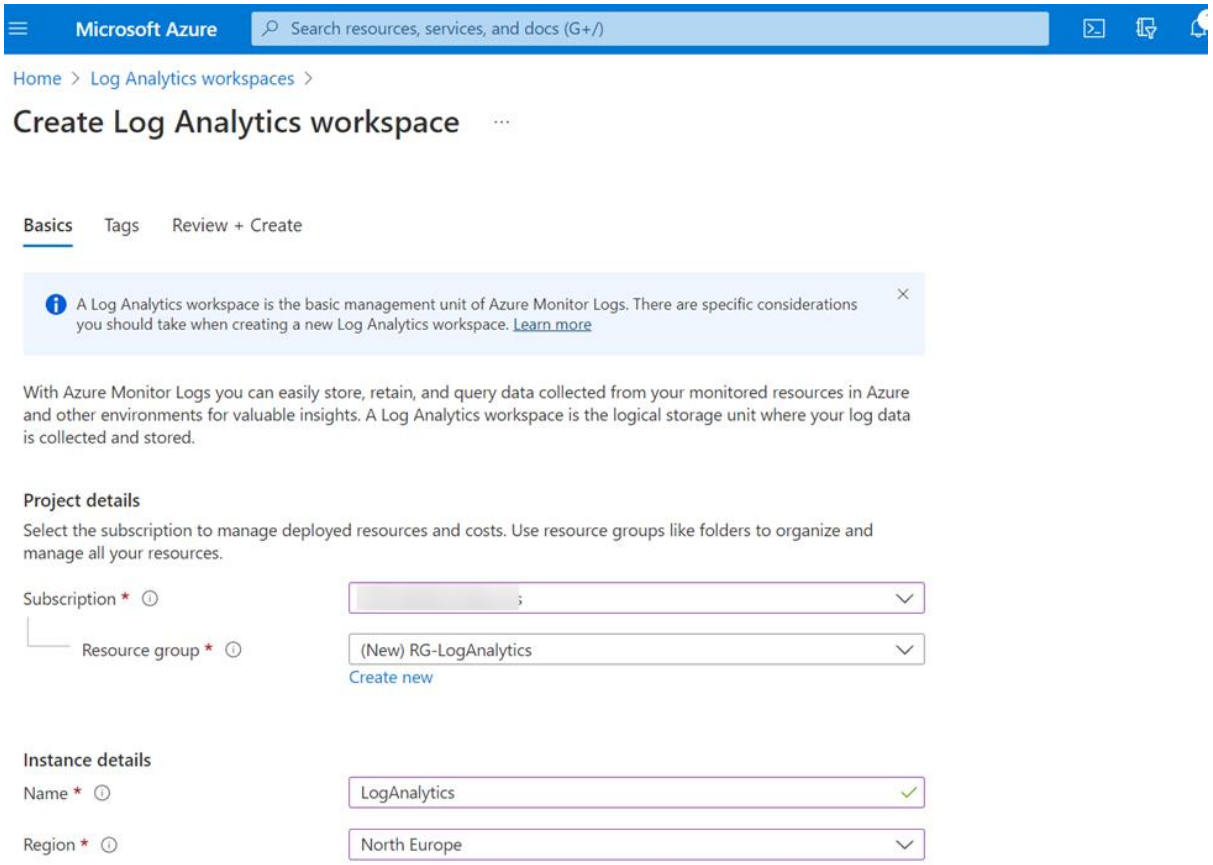
You should monitor sign-in activity from the emergency account, by following the below we will use Azure Log Analytics to monitor the sign-in log from the emergency account and it will trigger email and SMS to admin people whenever break glass account sign-in.

Send Azure AD Sign-in Logs to Azure Monitor

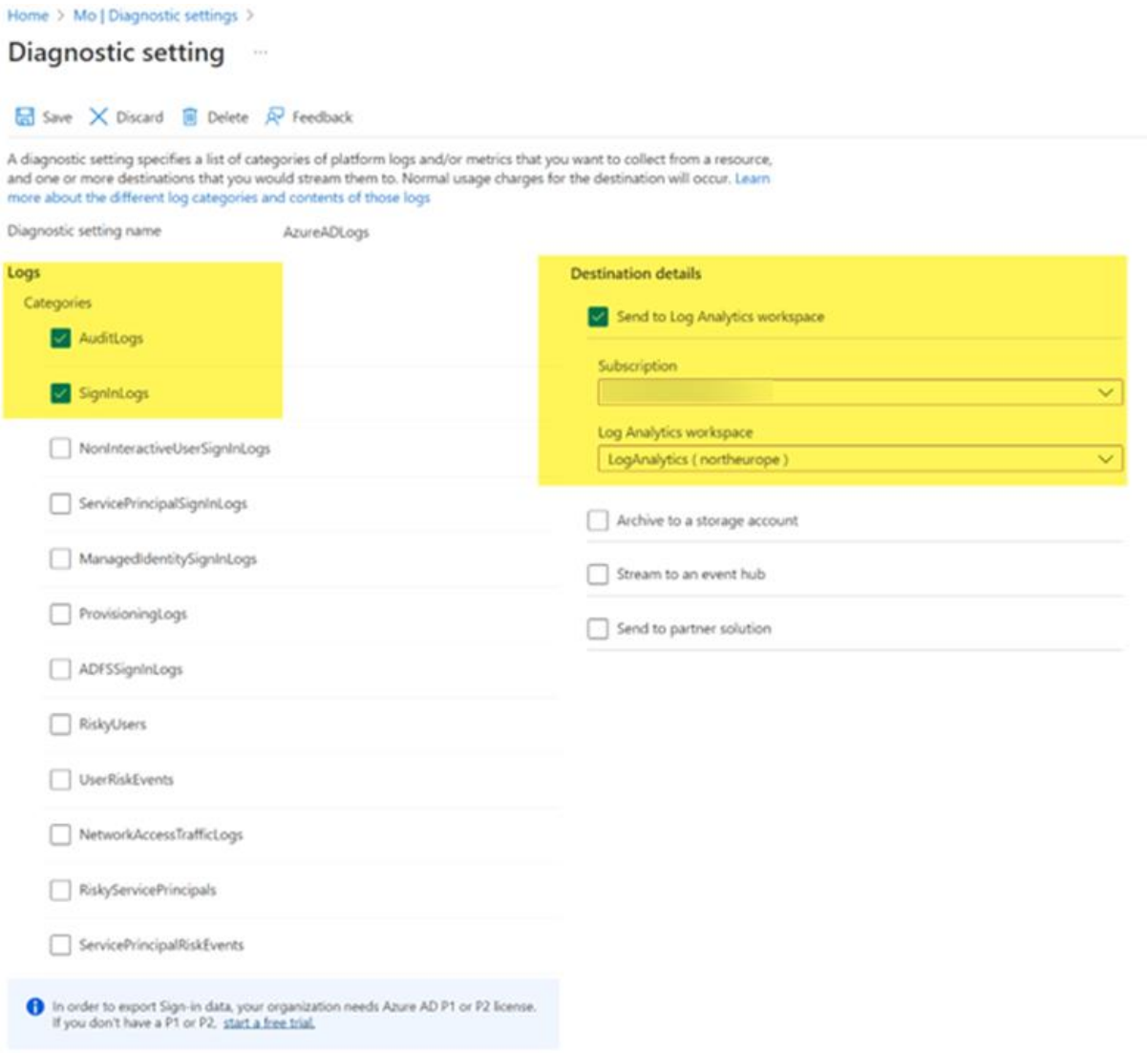
1. Create a **Log Analytics workspace**
2. In the Azure portal, enter **Log Analytics** in the search box. As you begin typing, the list filters based on your input. Select **Log Analytics workspaces**.



Click Create

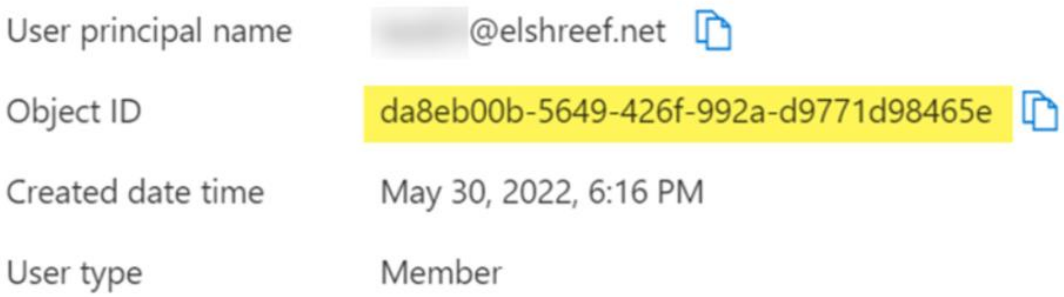


- Azure Log Analytics workspace created.
- Then from the Entra Admin Centre go to **Azure Active Directory** > **Monitoring & Health** > **Diagnostic settings** -> **Add diagnostic setting**. You can also select **Export Settings** from the **Audit Logs** or **Sign-ins** page to get to the diagnostic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



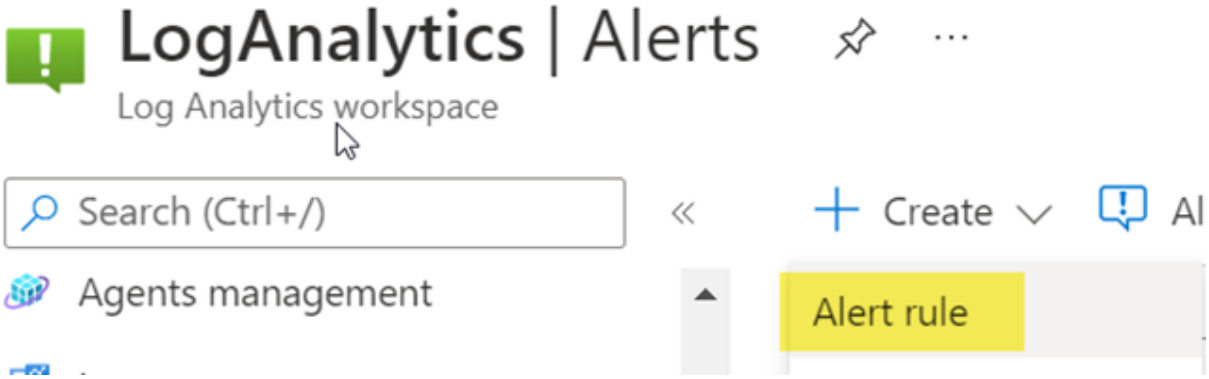
Obtain Object IDs of the break glass accounts

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.

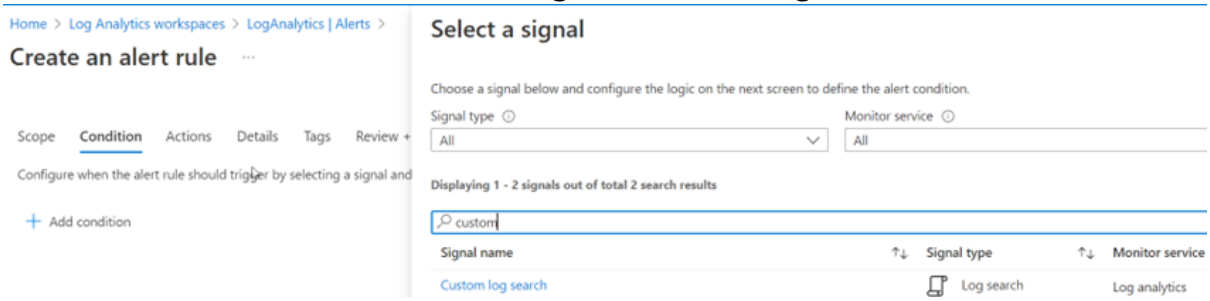


Create an alert rule

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**.



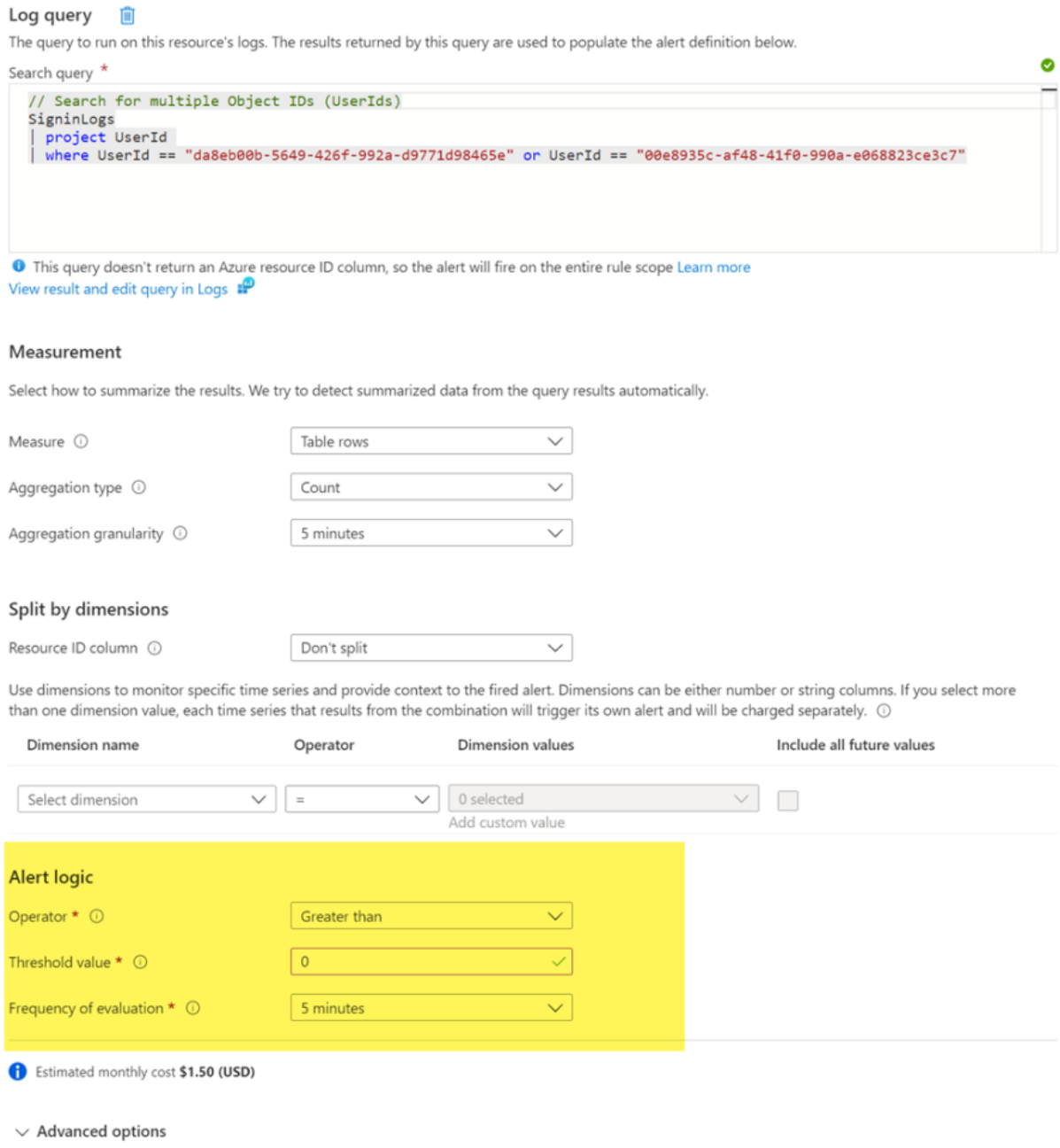
- Under **Search query**, enter the following query, inserting the object IDs of the two break glass accounts.

```
// 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:

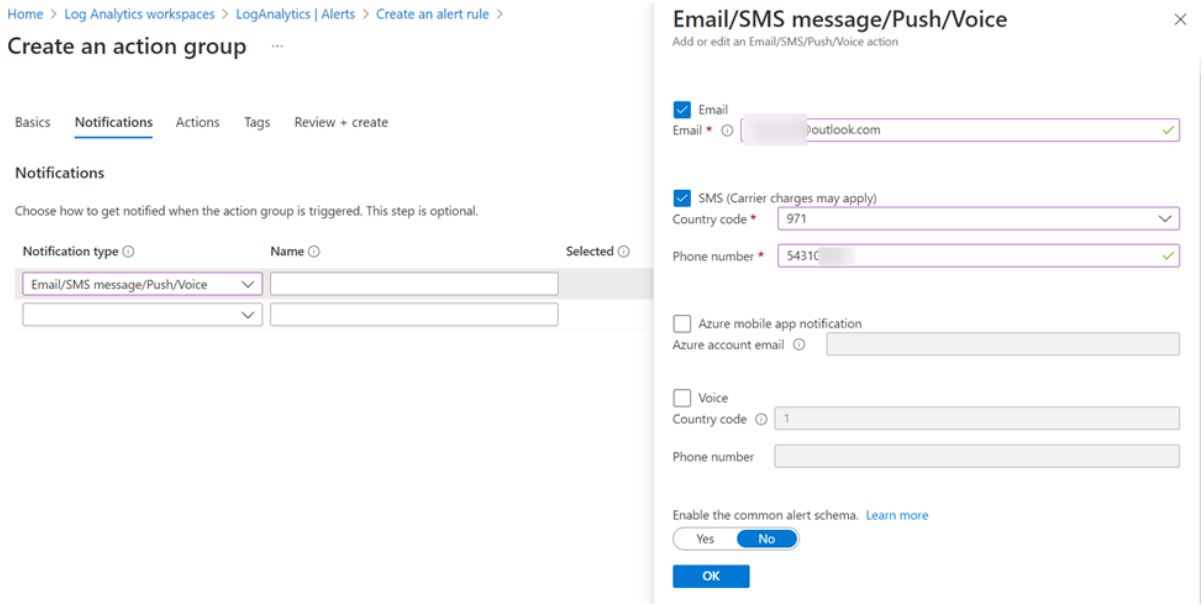
- Based on: Number of results
- Operator: Greater than
- Threshold value: 0



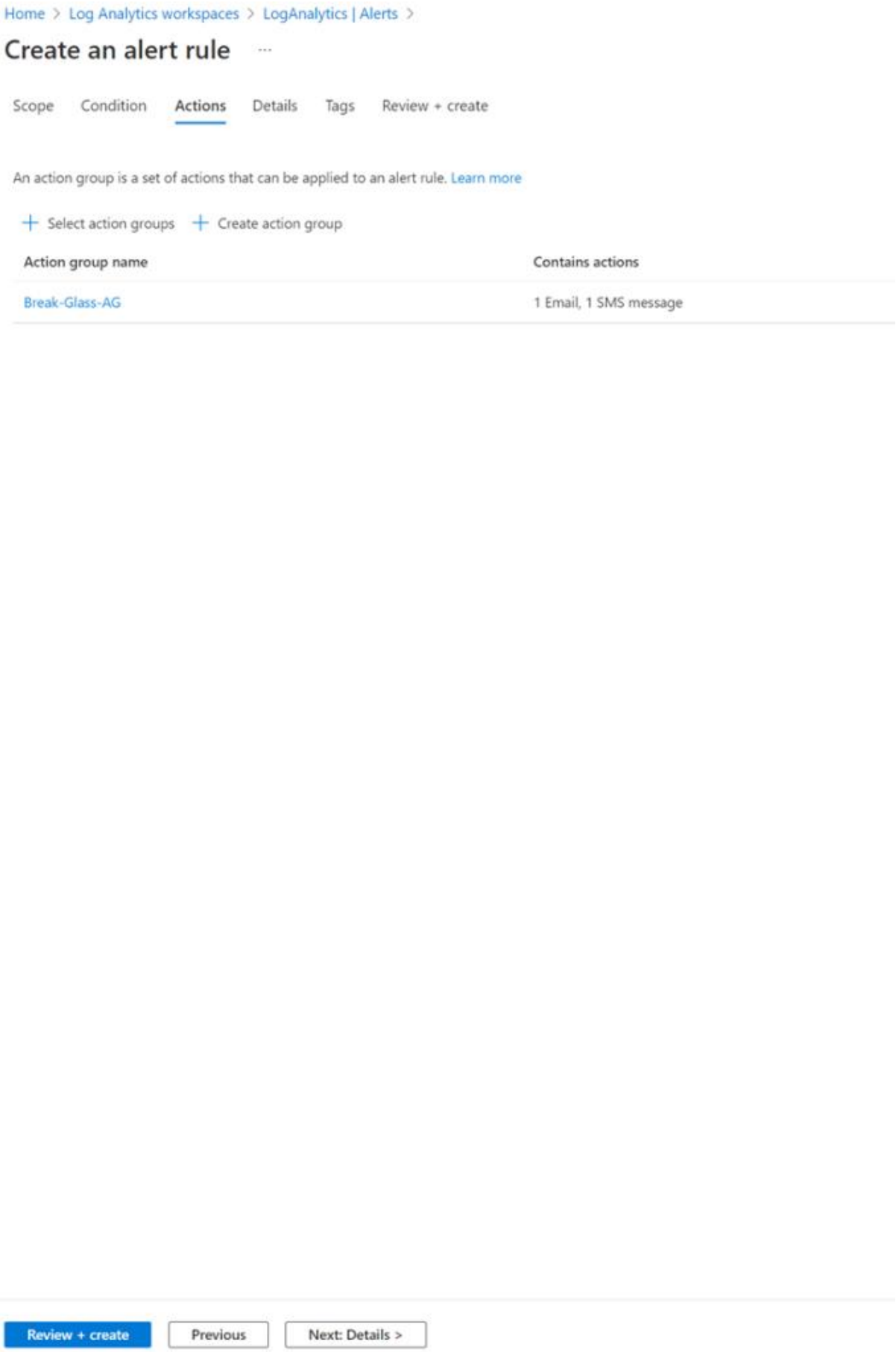
Then select Done

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**.

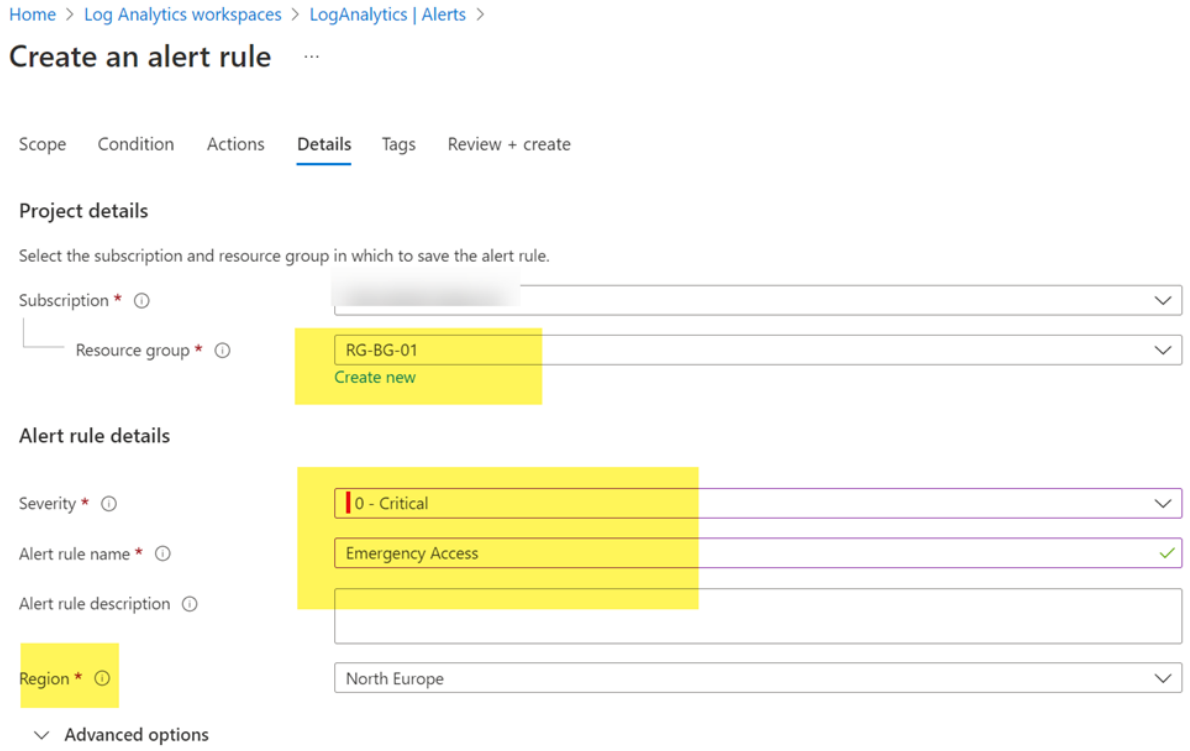
6. Select the **Action Type** as **Email/SMS/Push/Voice**.
7. Select **Edit details** to select the notification methods you want to configure and enter the required contact information, and then select **Ok** to save the details.
8. Add any additional actions you want to trigger.
9. Select **OK**.



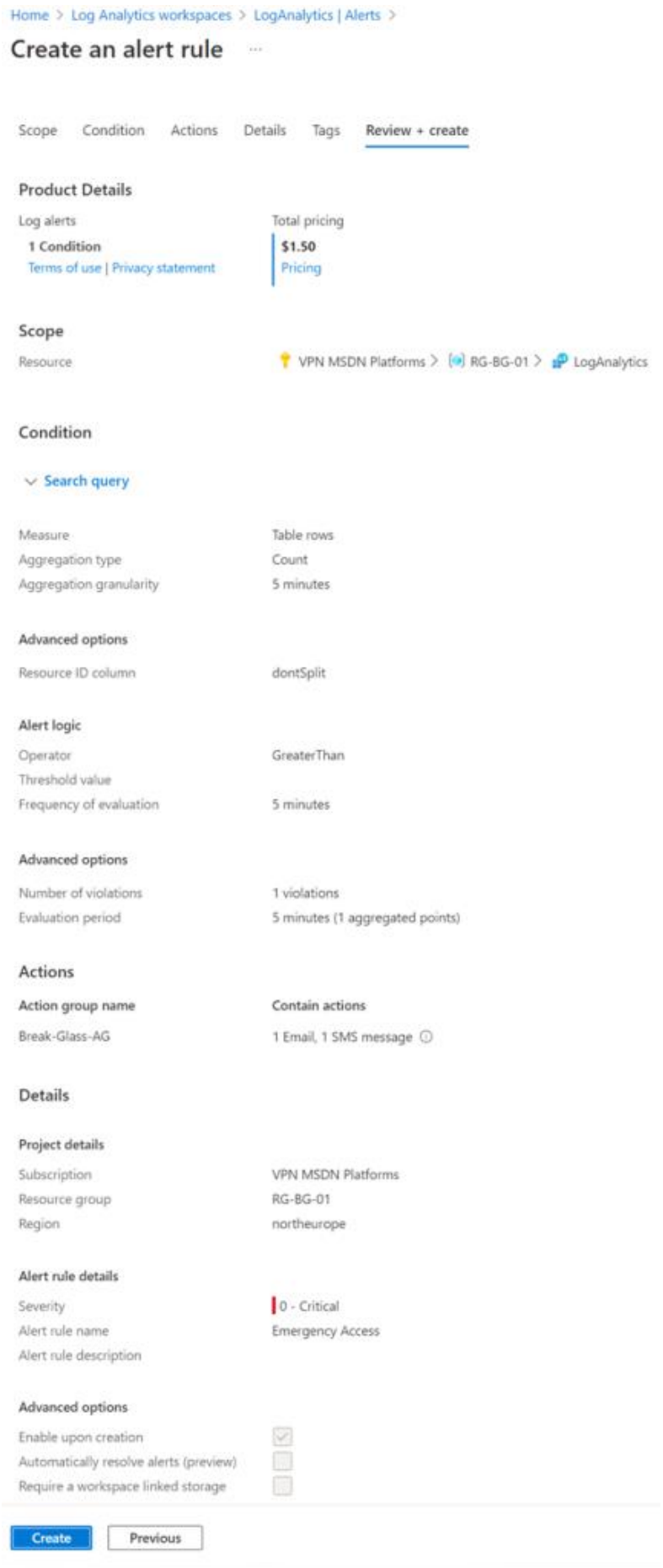
Then review and create


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 >

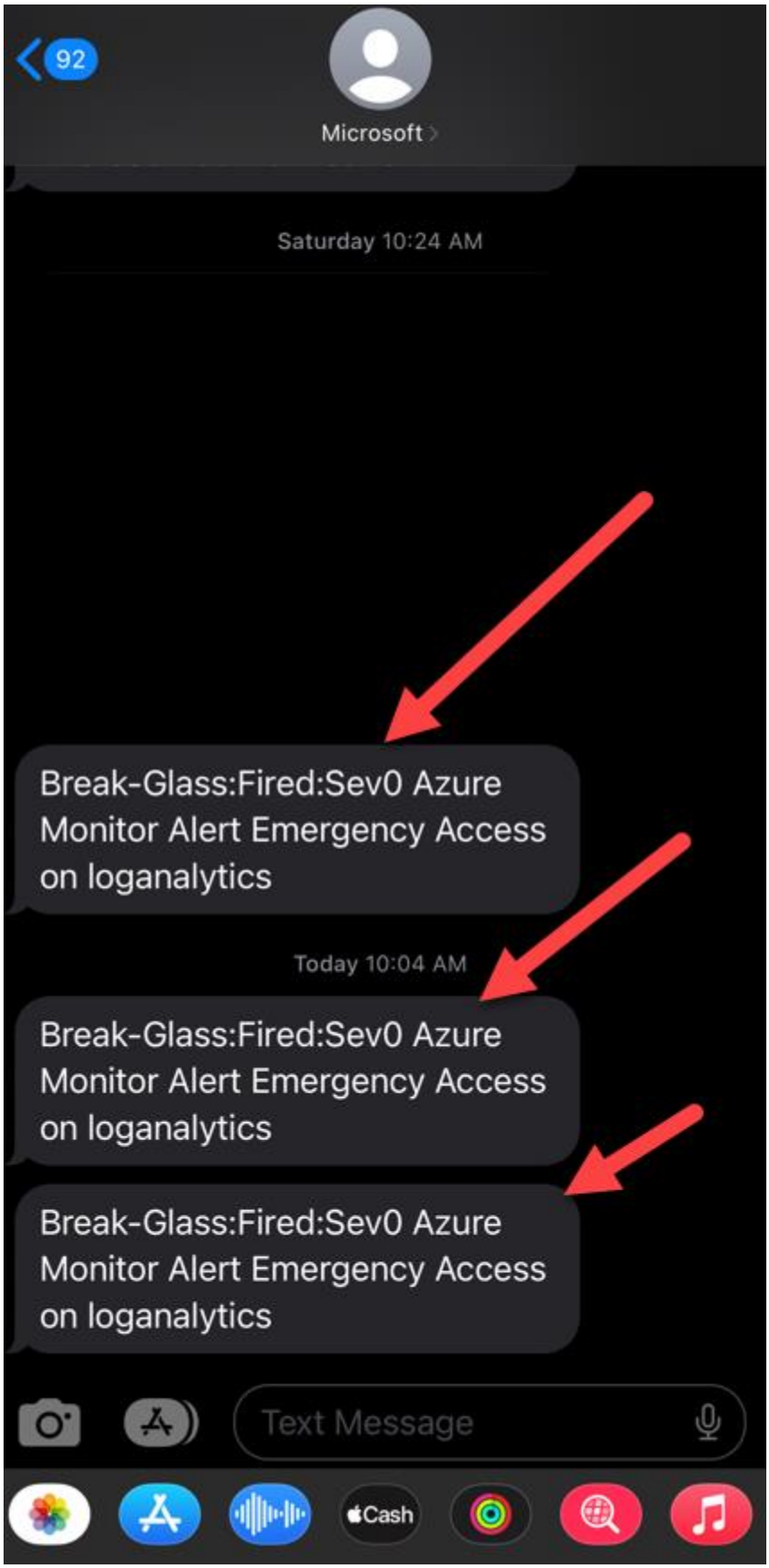
- To customize the email notification sent to the members of the action group, select actions under **Customize Actions**.
- Under **Alert Details**, specify the alert rule name and add an optional description.
- Set the **Severity level** of the event. We recommend that you set it to **Critical(Sev 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**.

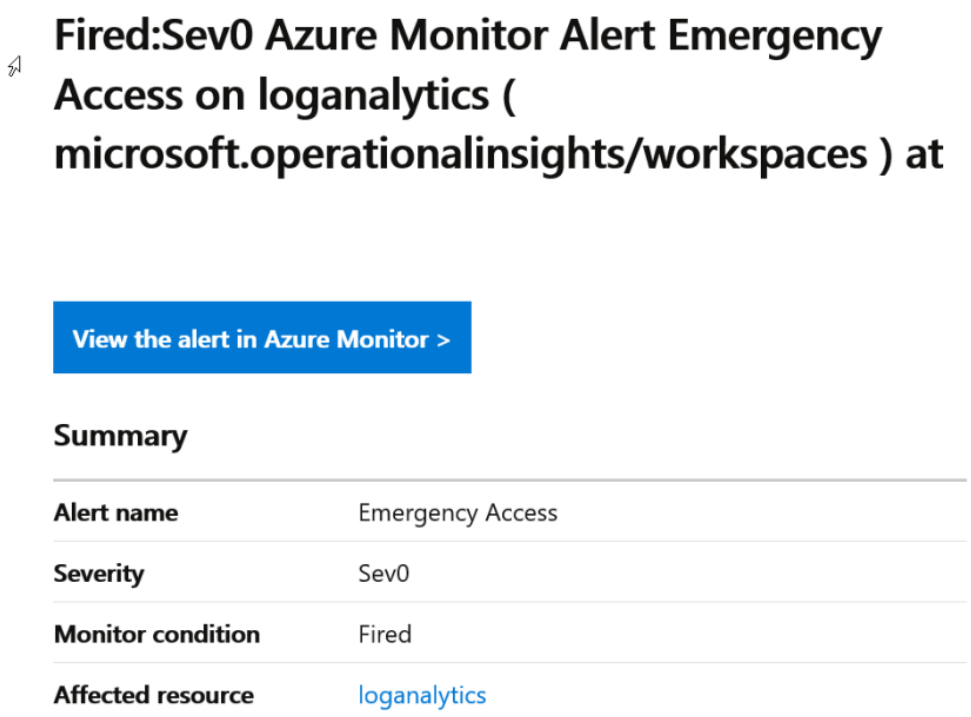


Then select Review and Create


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

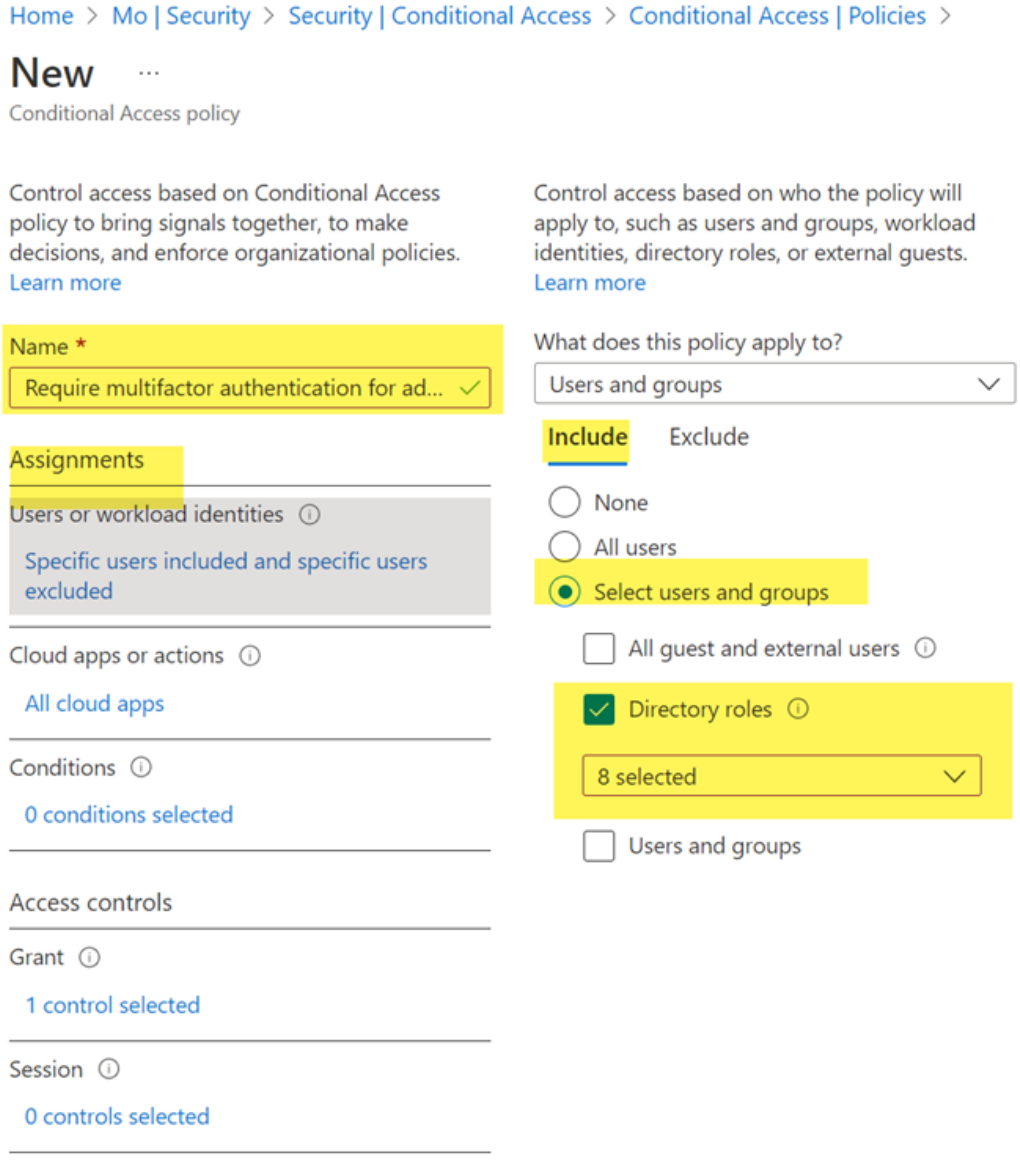
When anyone attempts to login using the emergency admin account, you will receive a SMS and Email as per the below



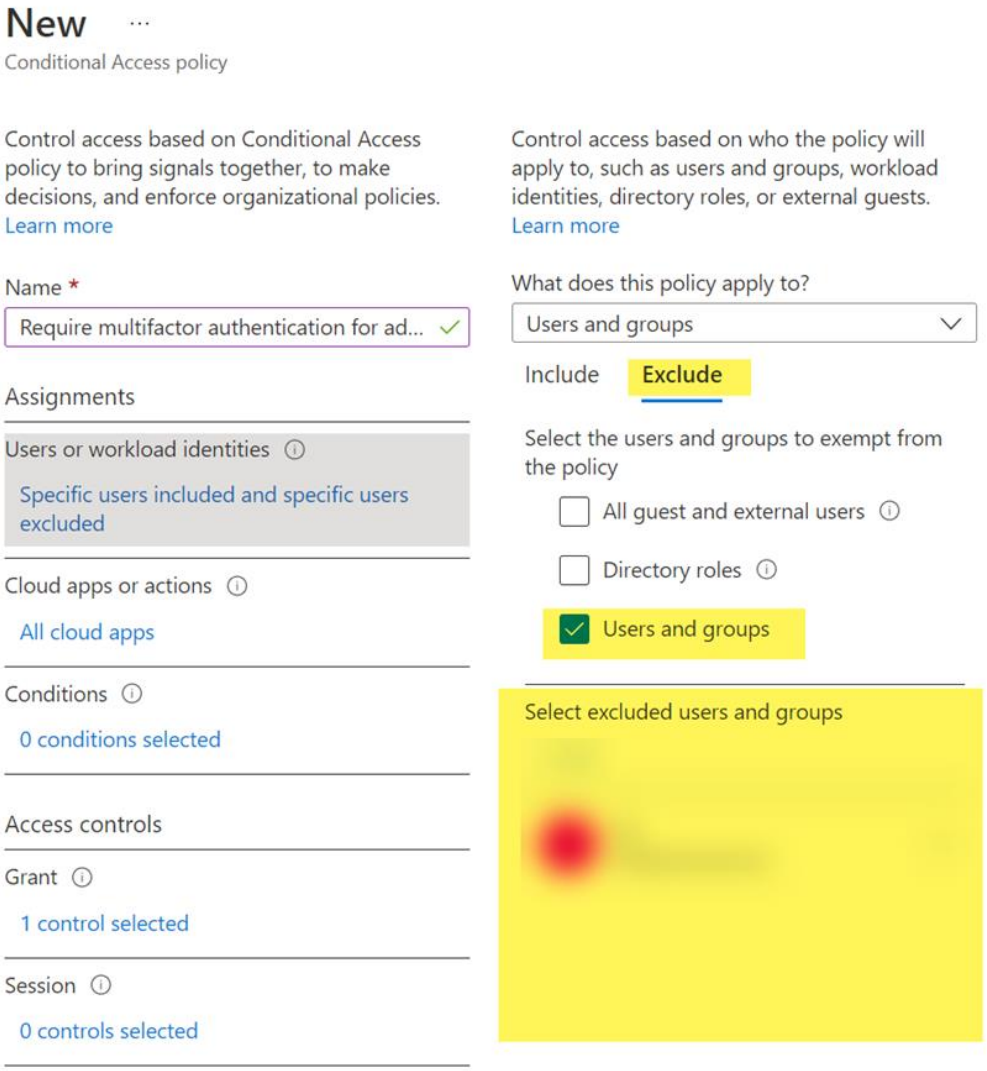

Fired:Sev0 Azure Monitor Alert Emergency Access on loganalytics (microsoft.operationalinsights/workspaces) at
View the alert in Azure Monitor >
Summary
Alert name
Emergency Access
Severity
Sev0
Monitor condition
Fired
Affected resource
loganalytics

2) Require multifactor authentication for administrative roles

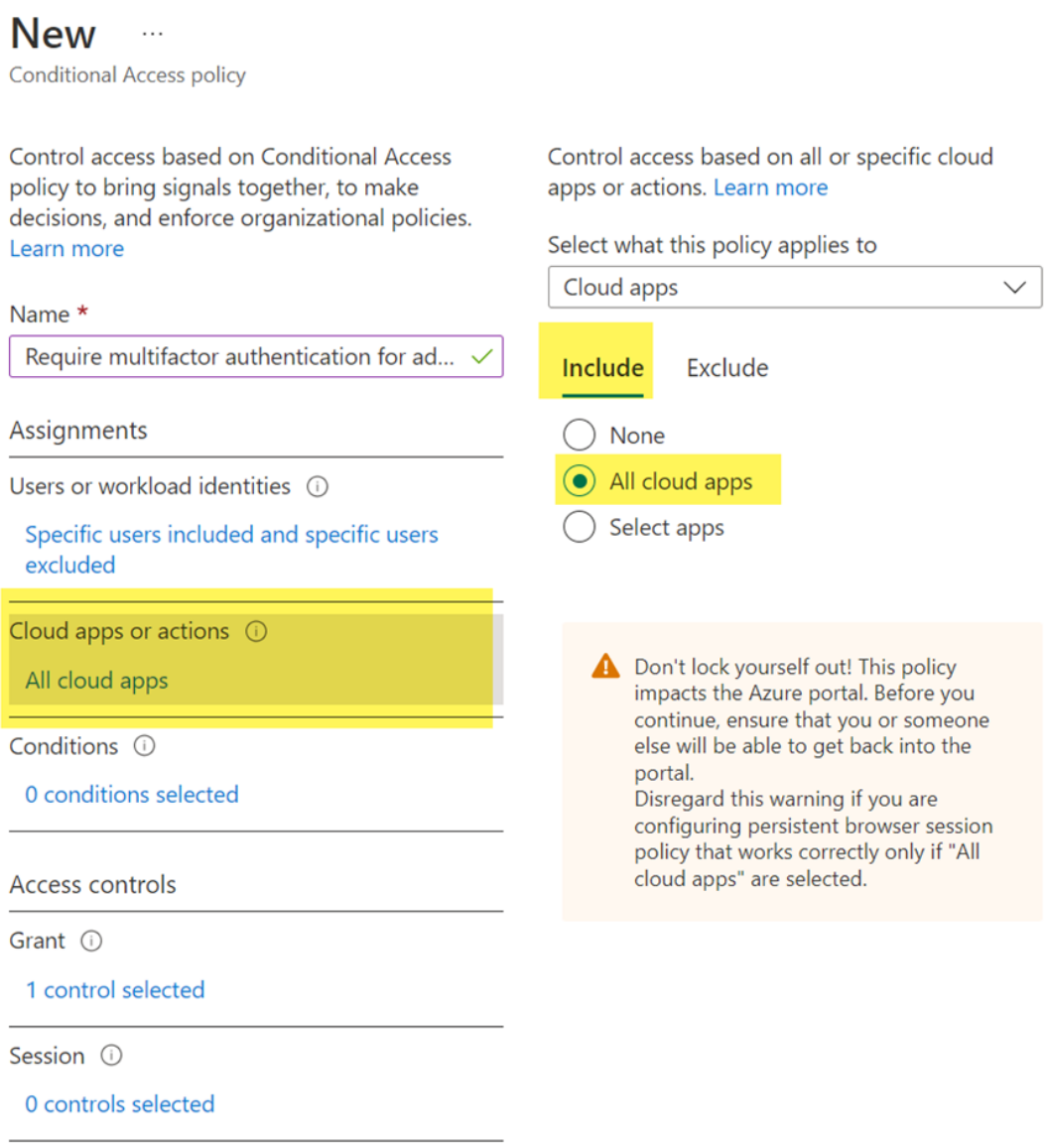
1. Log in to https://entra.microsoft.com/
2. Expand Azure Active Directory
3. Select Protect & Secure, then select Conditional Access.
4. Click New policy and provide the policy name
5. Go to Assignments > Users and groups > Include > Select users and groups > check Directory roles., At a minimum, select 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).



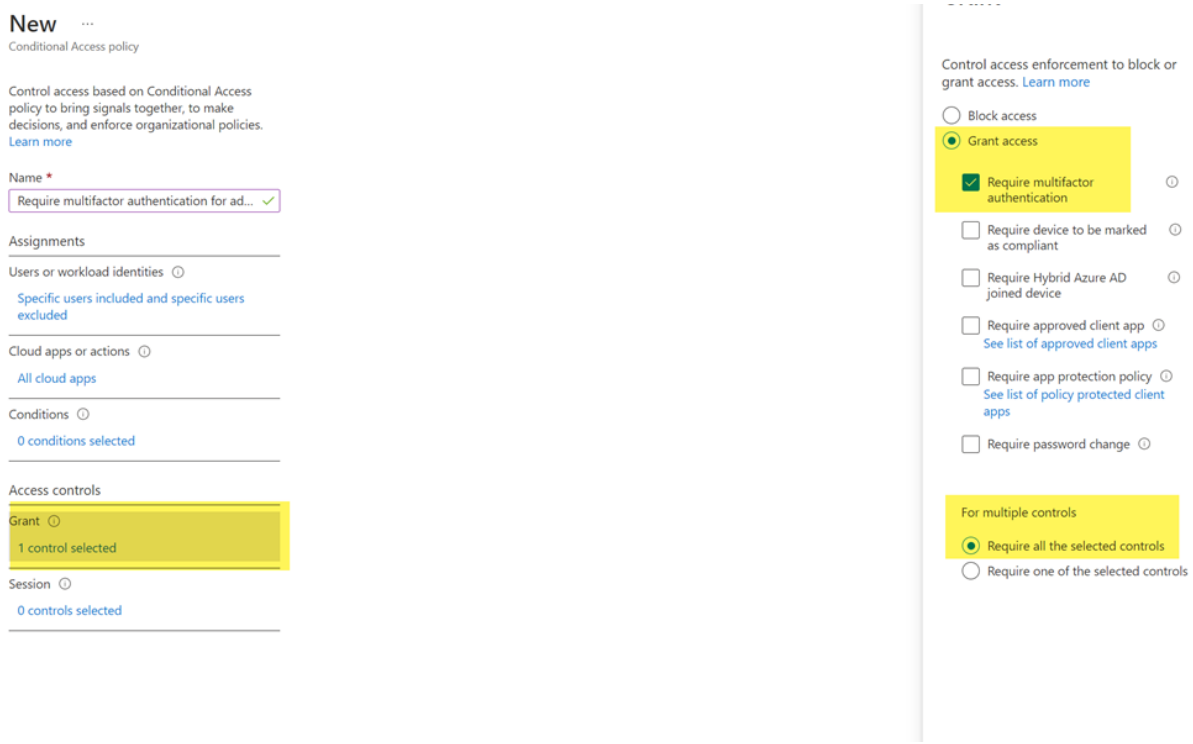
- Exclude Emergency access accounts from MFA



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

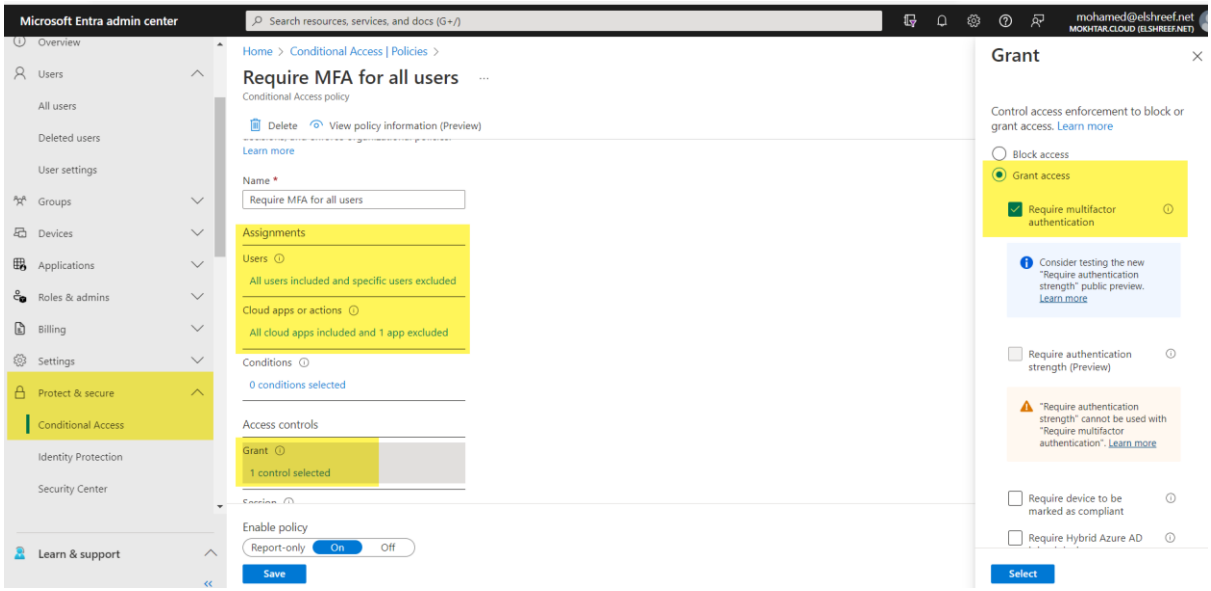


- Under Access controls > Grant > select Grant access > check Require multifactor authentication (and nothing else).
- Create.


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

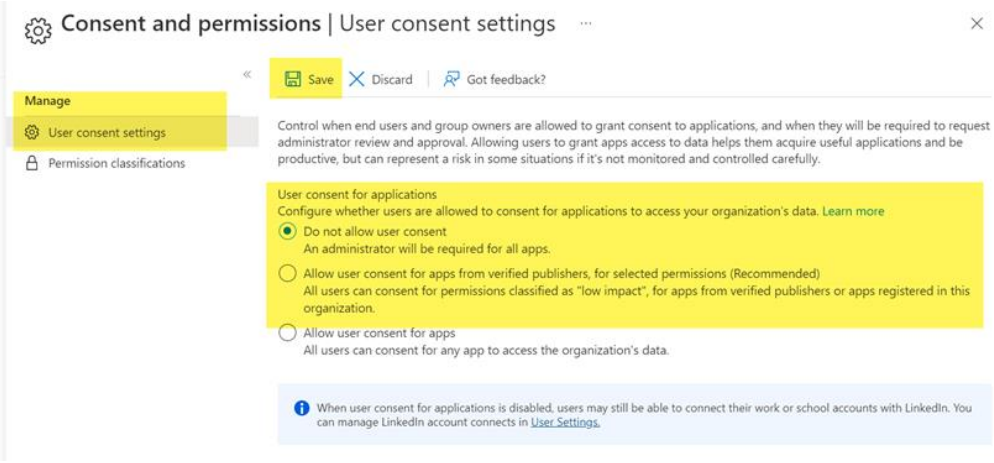
3) Ensure all Users can complete multifactor authentication

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



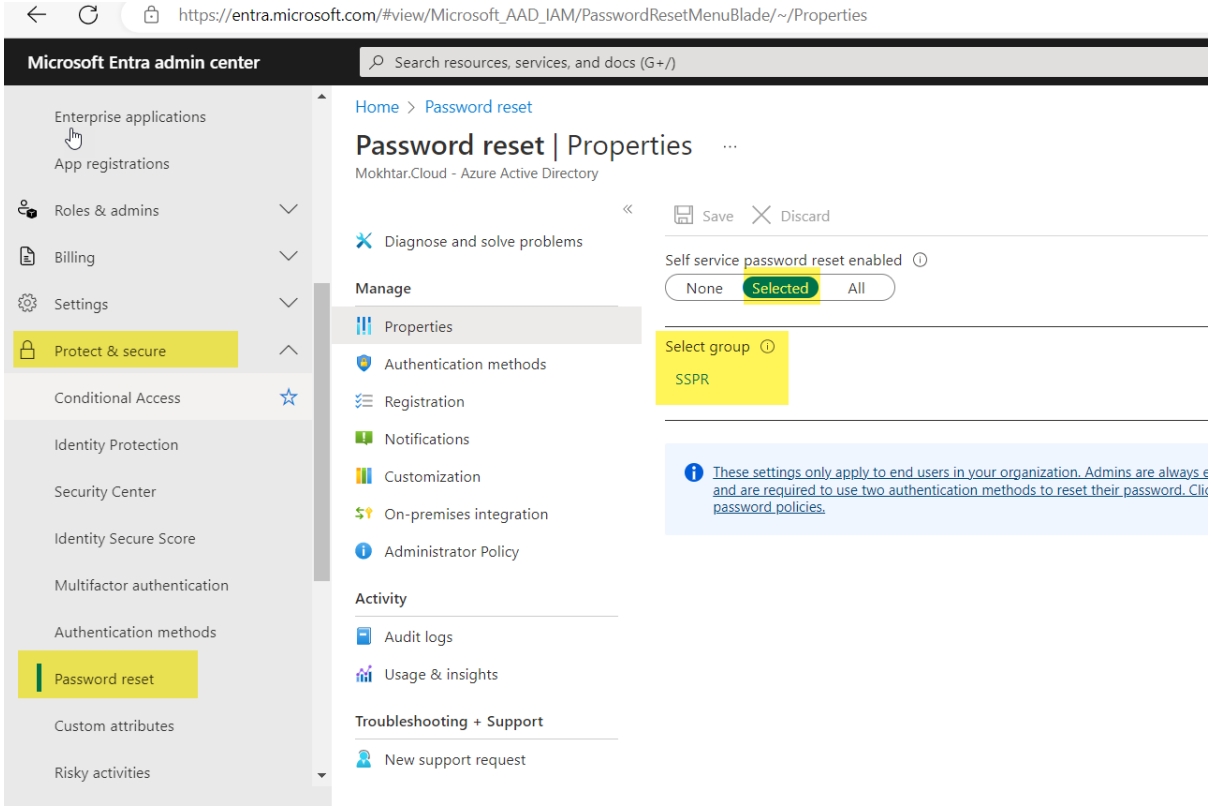
4) Do not allow Users to grant consent to unreliable applications

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



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.

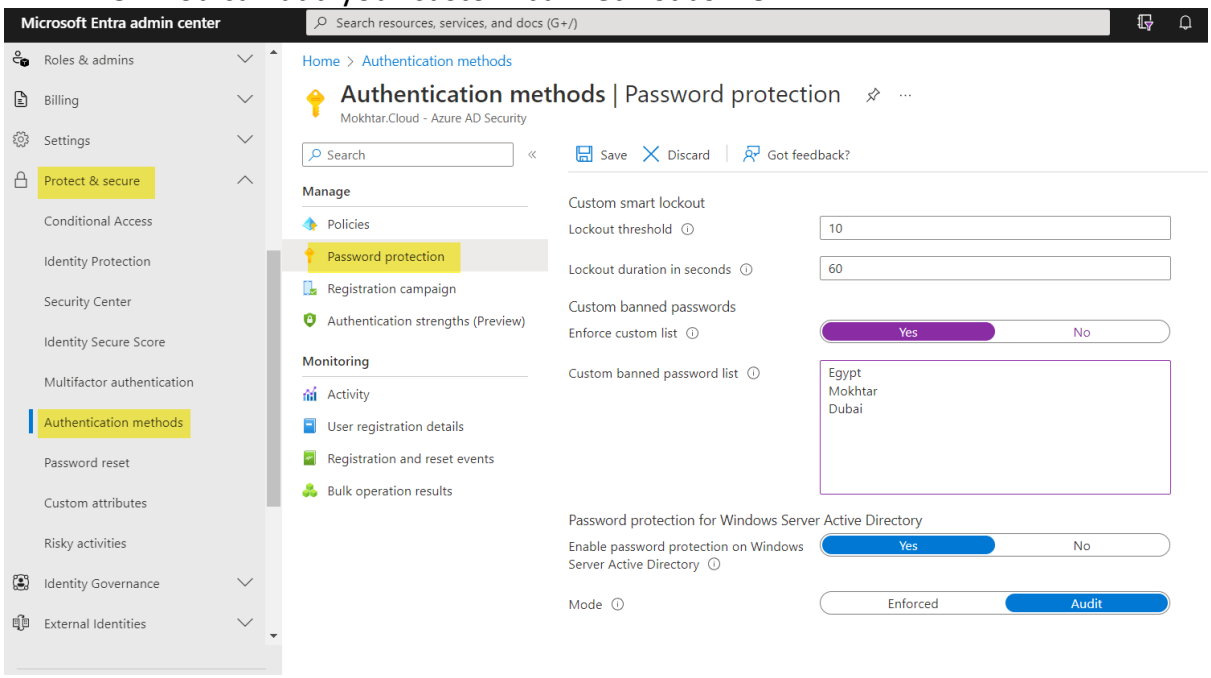


Now any user part of the above group SSPR, he will be able to use the self-service portal to reset his account.

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.

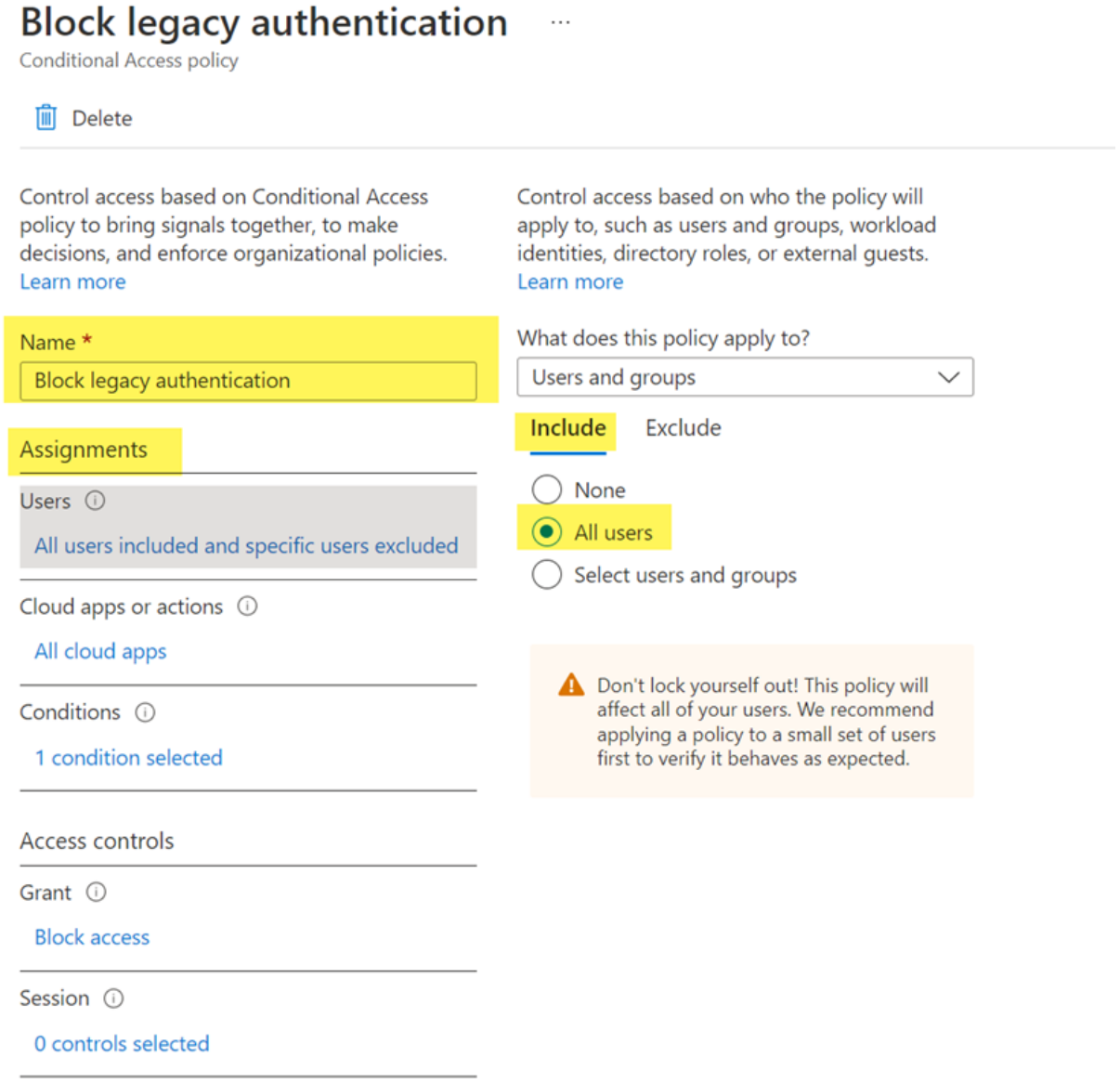


- Click Save at the top of the right pane.

7) Enable Conditional Access policies to block legacy authentication

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

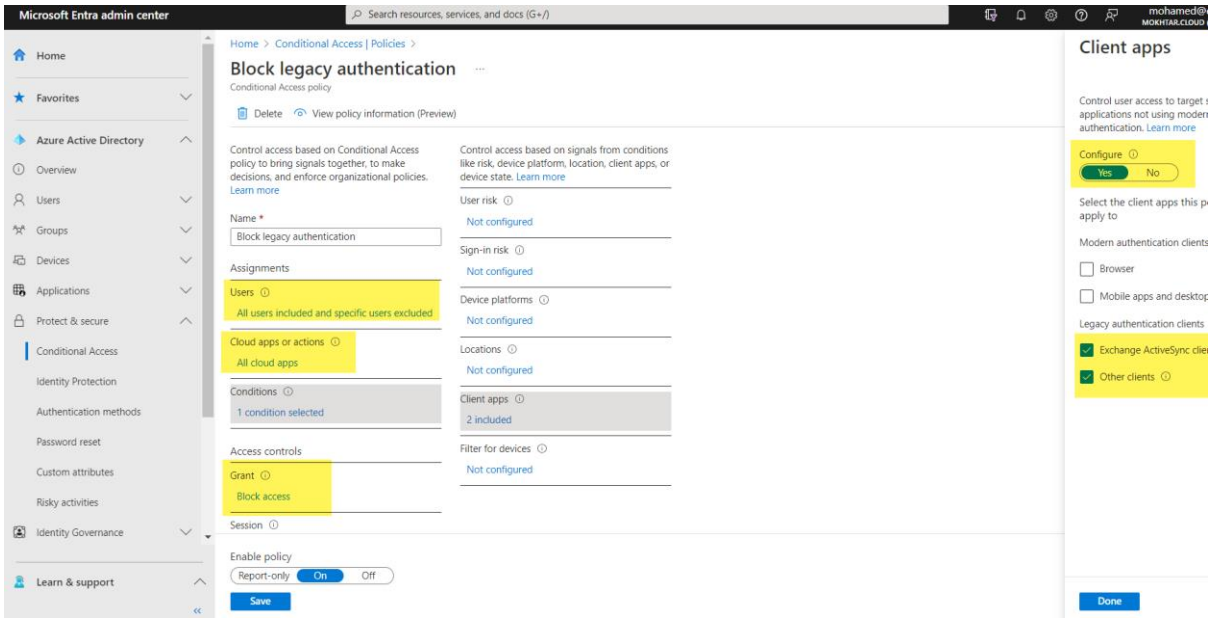
1. Log in to https://entra.microsoft.com/
2. Select Protect & Secure, then select Conditional Access.
3. Create a new policy by selecting new policy.
4. Set the following conditions within the policy.
5. Under Assignments enable All users



- 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.

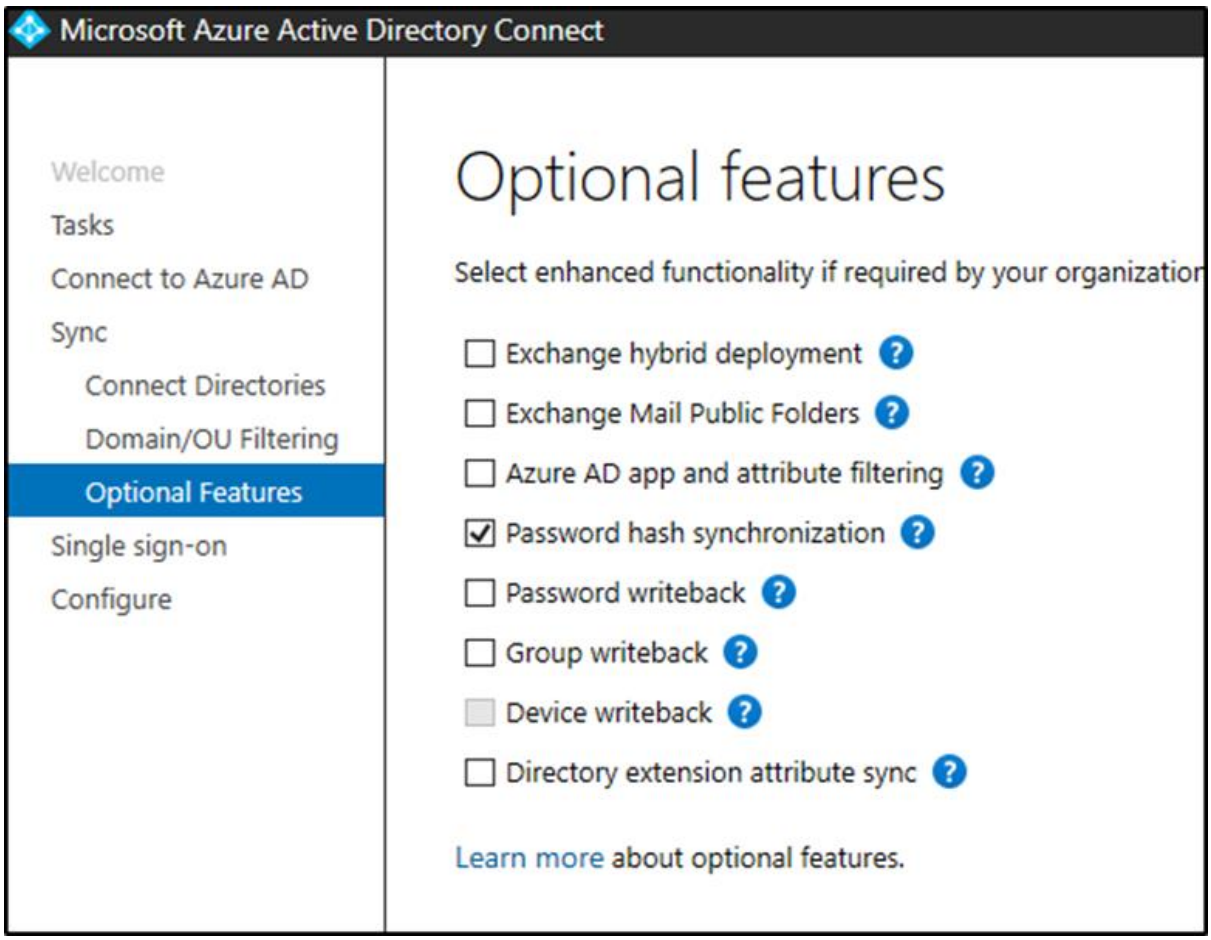
Select Conditions then Client apps, enable the settings for Exchange ActiveSync clients and other clients, select the grant action to be blocked



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.

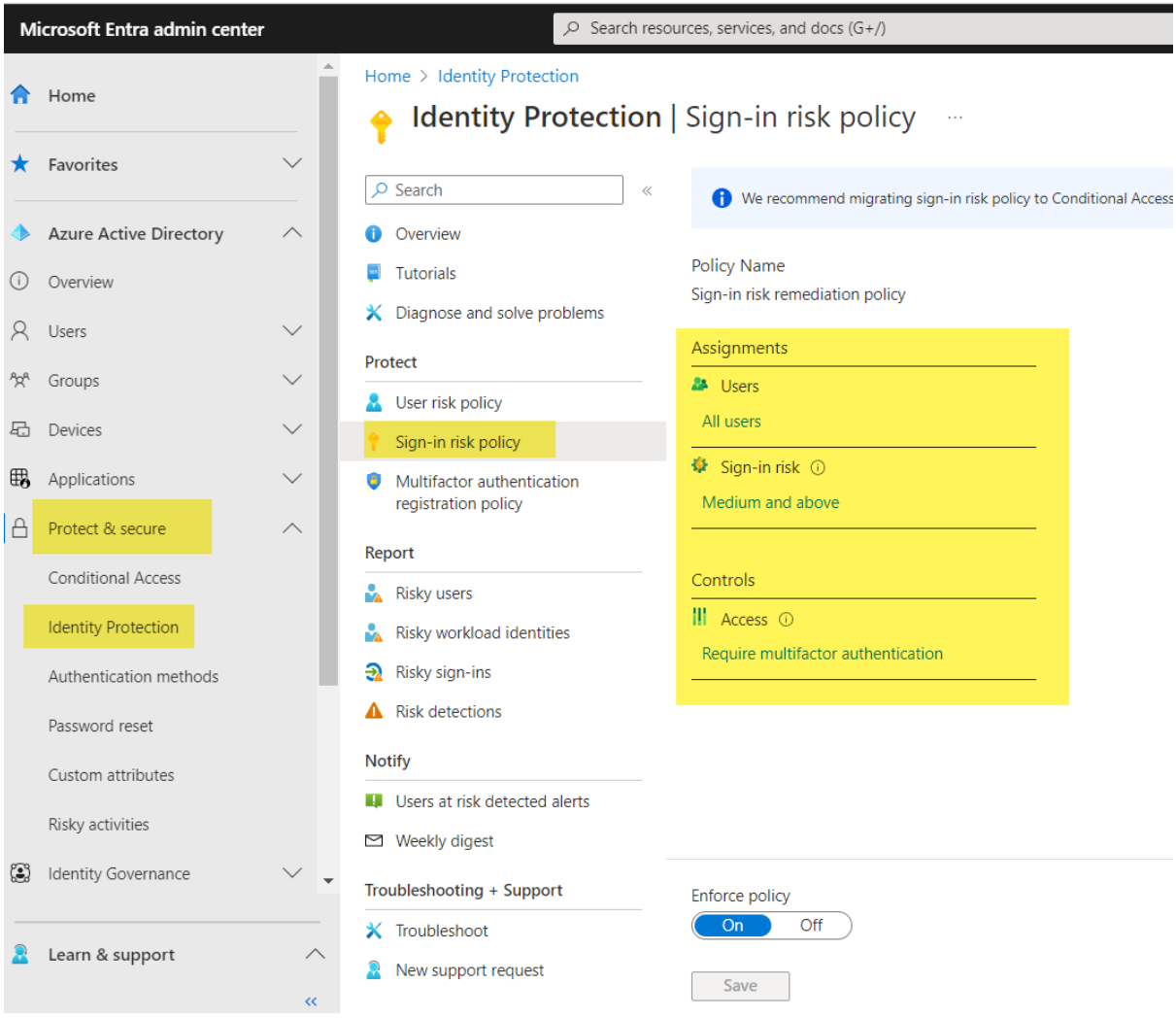


- On the Ready to configure screen click Configure.
- Once the configuration completes, click Exit.

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

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

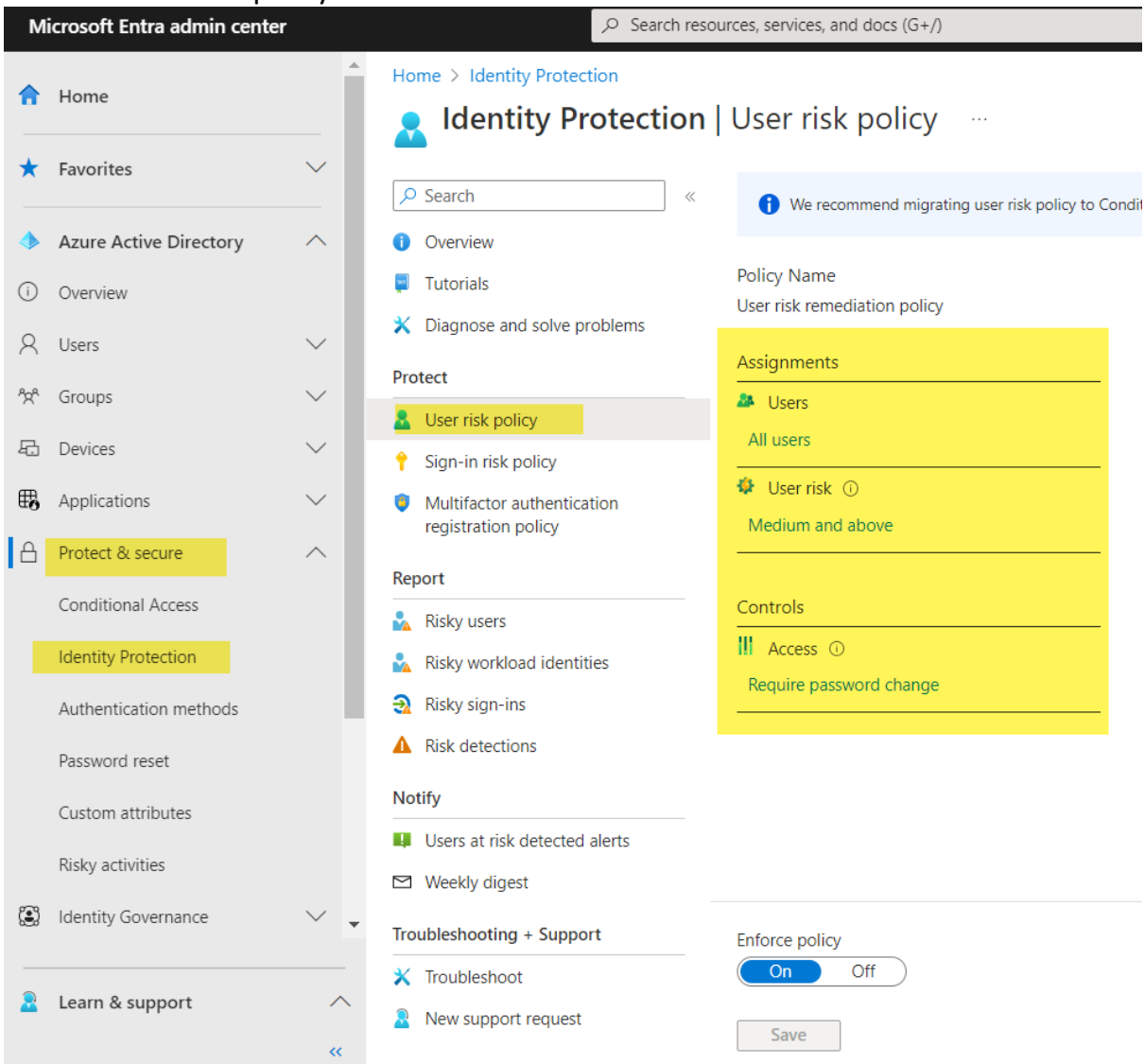
1. Log in to https://entra.microsoft.com/
2. Select Protect & Secure.
3. Select Identity Protection
4. Select Sign-in risk policy
5. Set the following conditions within the policy.
    1. Under Users choose All users
    2. Under Sign-in risk Select Medium and above.
    3. Under Access Controls select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



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



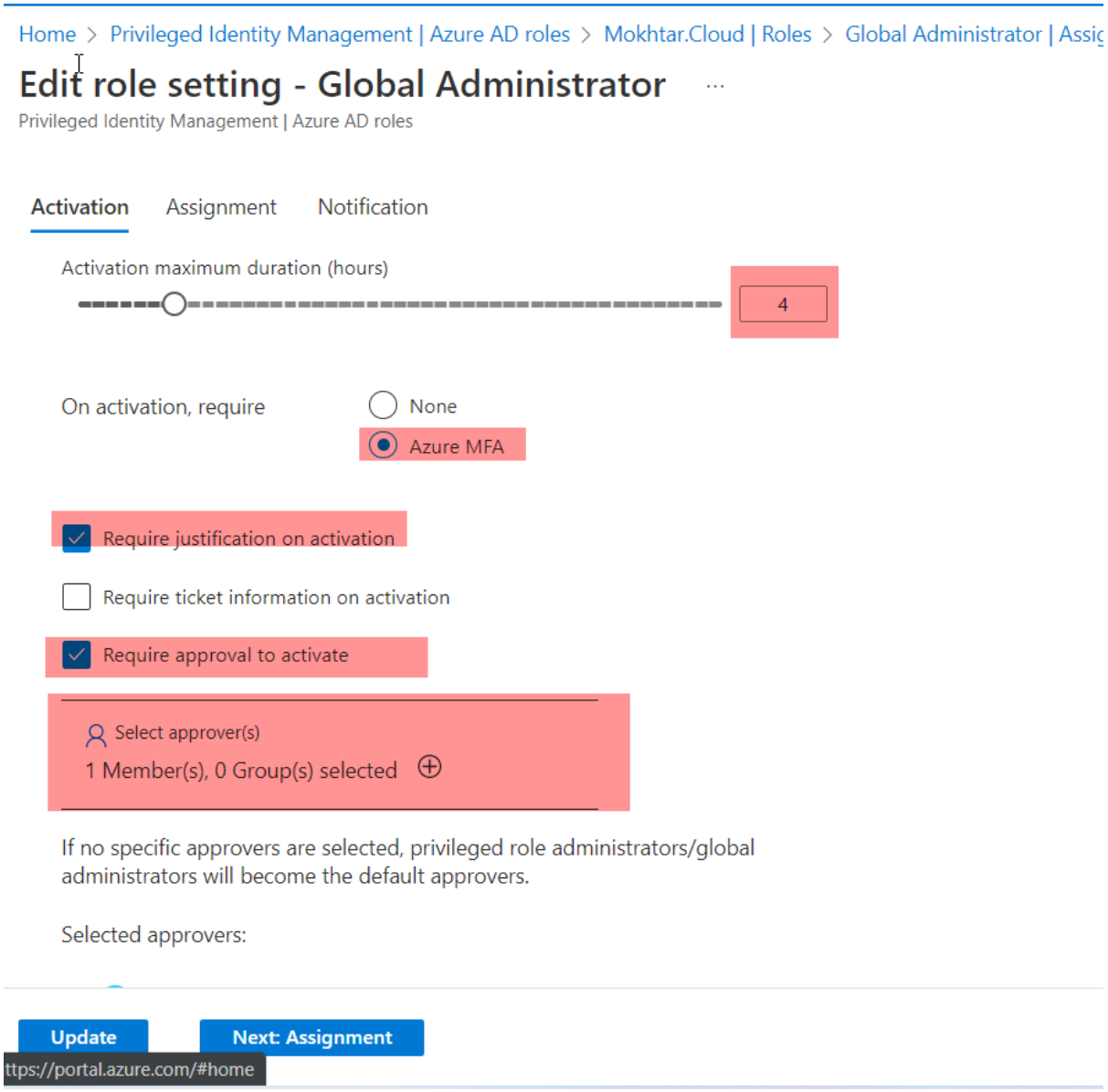
11) Use Just in Time privileged access to Office 365 roles

we will deploy the below simple table using PIM

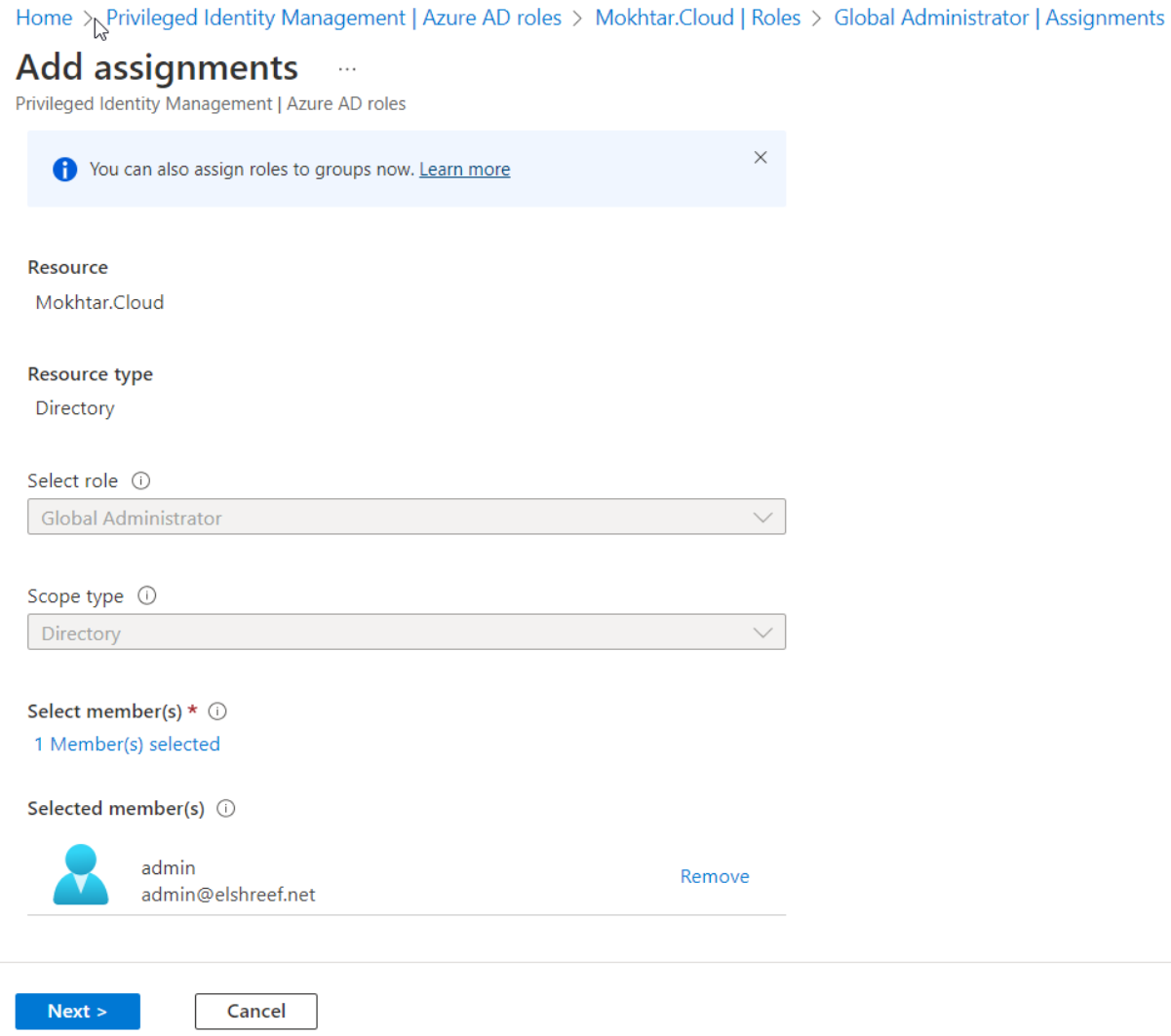
Role	Assignee	Justification	Approval	Person to Approve	Max Duration	Validity
Global Admin	Admin1	Required	Manual Approval	Mohamed Mokhtar	4 hours	1 year
Global Reader	Admin1	Required	Auto Approval	N/A	8 Hours	Permanent

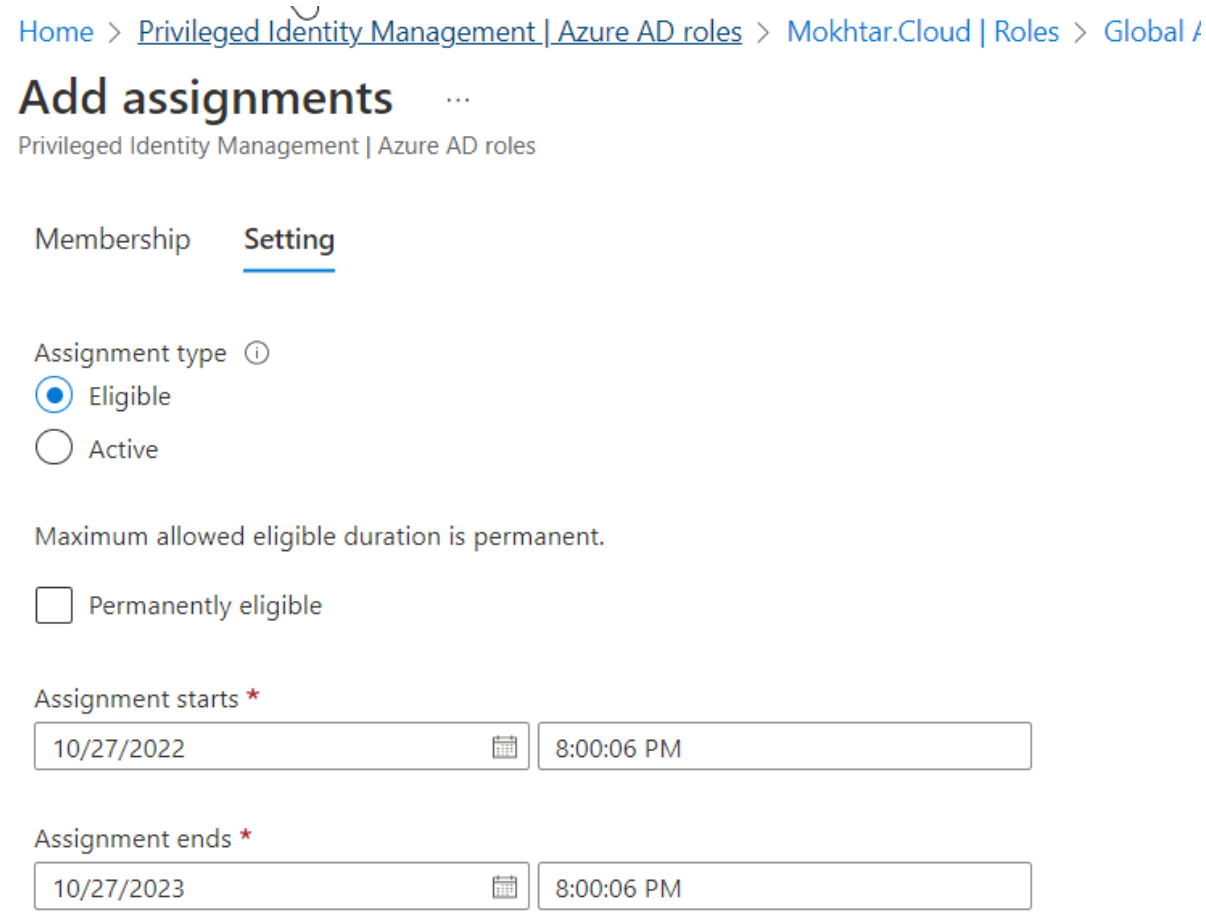
To configure Global Admin Role as per the above table

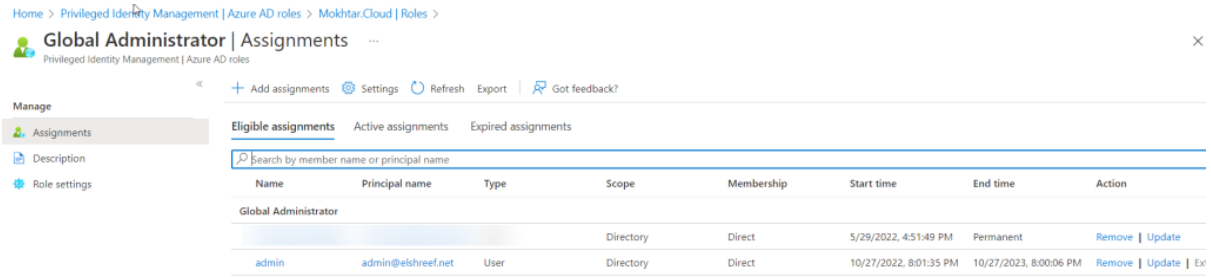
- Sign-on to your Microsoft Entra admin center as global administrator by going to https://entra.microsoft.com
- Select Identity Governance Then Privileged Identity management.
- Under Manage click on Azure AD Roles.
- look for Global admin Roles and open it
- Click on settings then edit and configure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


Home > Privileged Identity Management | Azure AD roles > Mokhtar.Cloud | Roles > Global Administrator | Assig
Edit role setting - Global Administrator
Privileged Identity Management | Azure AD roles
Activation
Assignment
Notification
Activation maximum duration (hours)
4
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
ttps://portal.azure.com/#home

Assign this role as eligible to admin1

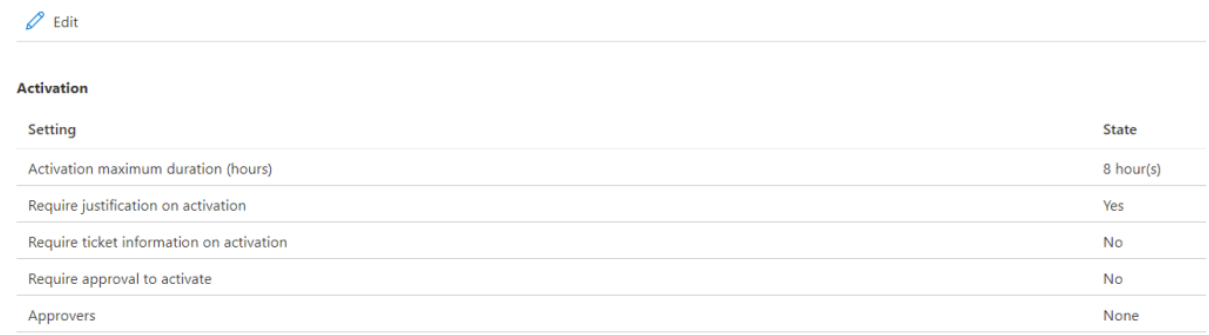






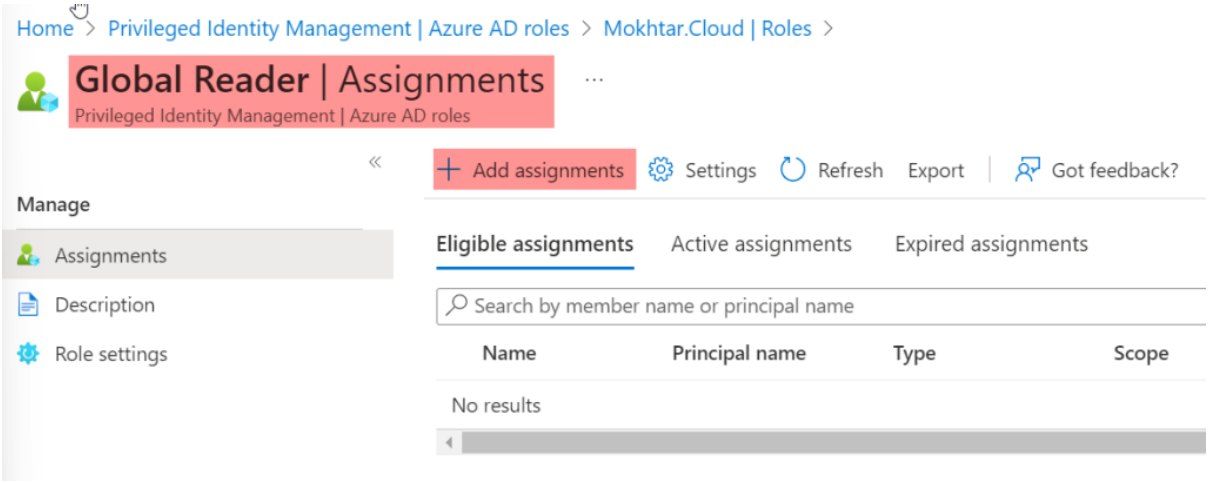
To configure Global Reader Role as per the above table

- 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

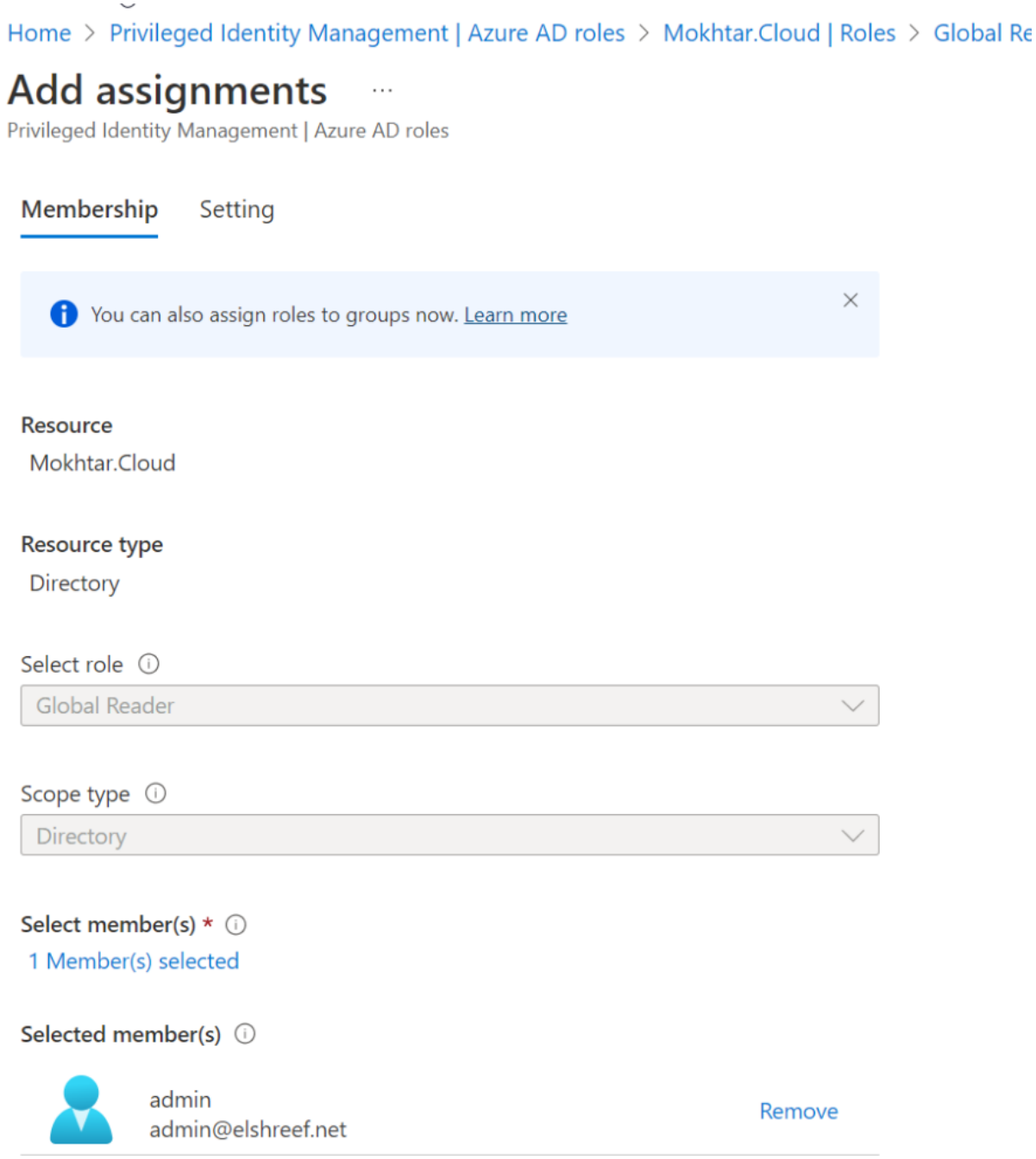


Assign this role as eligible to admin

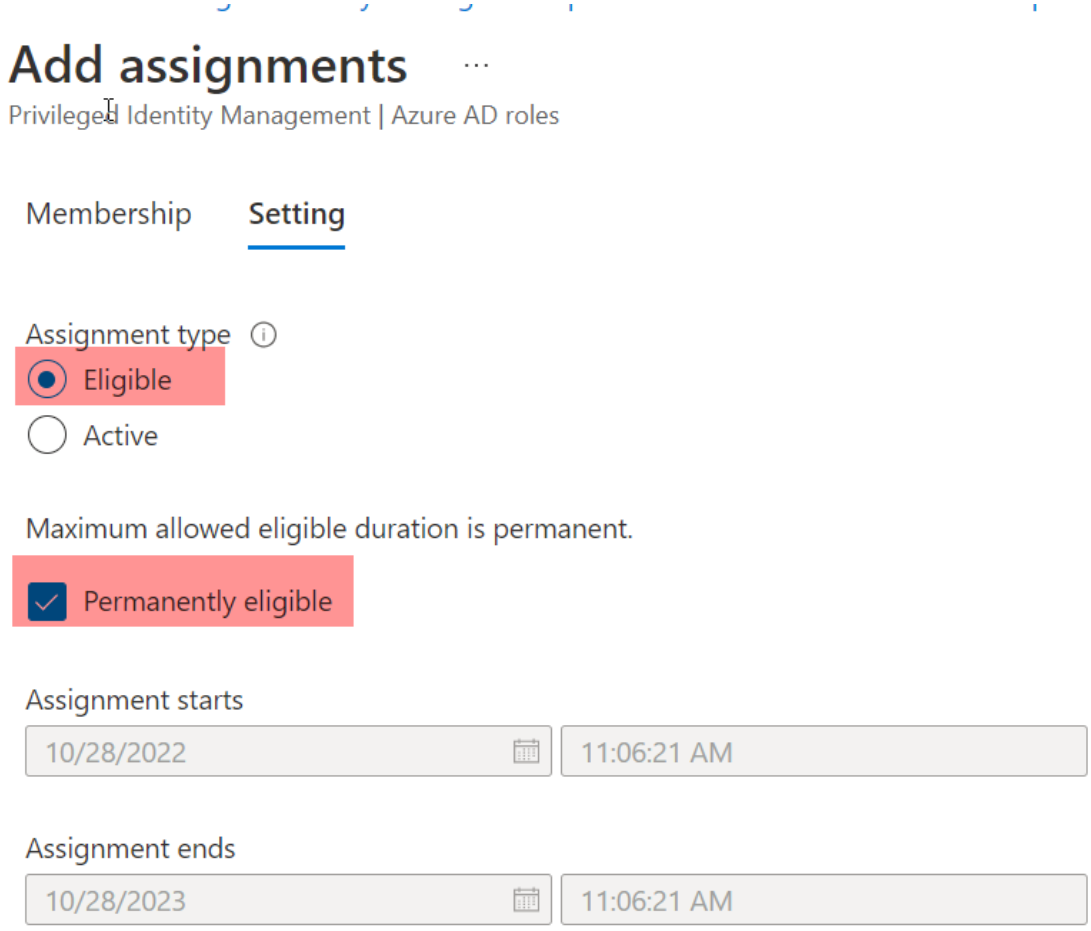
Click on add assignment



Select Admin



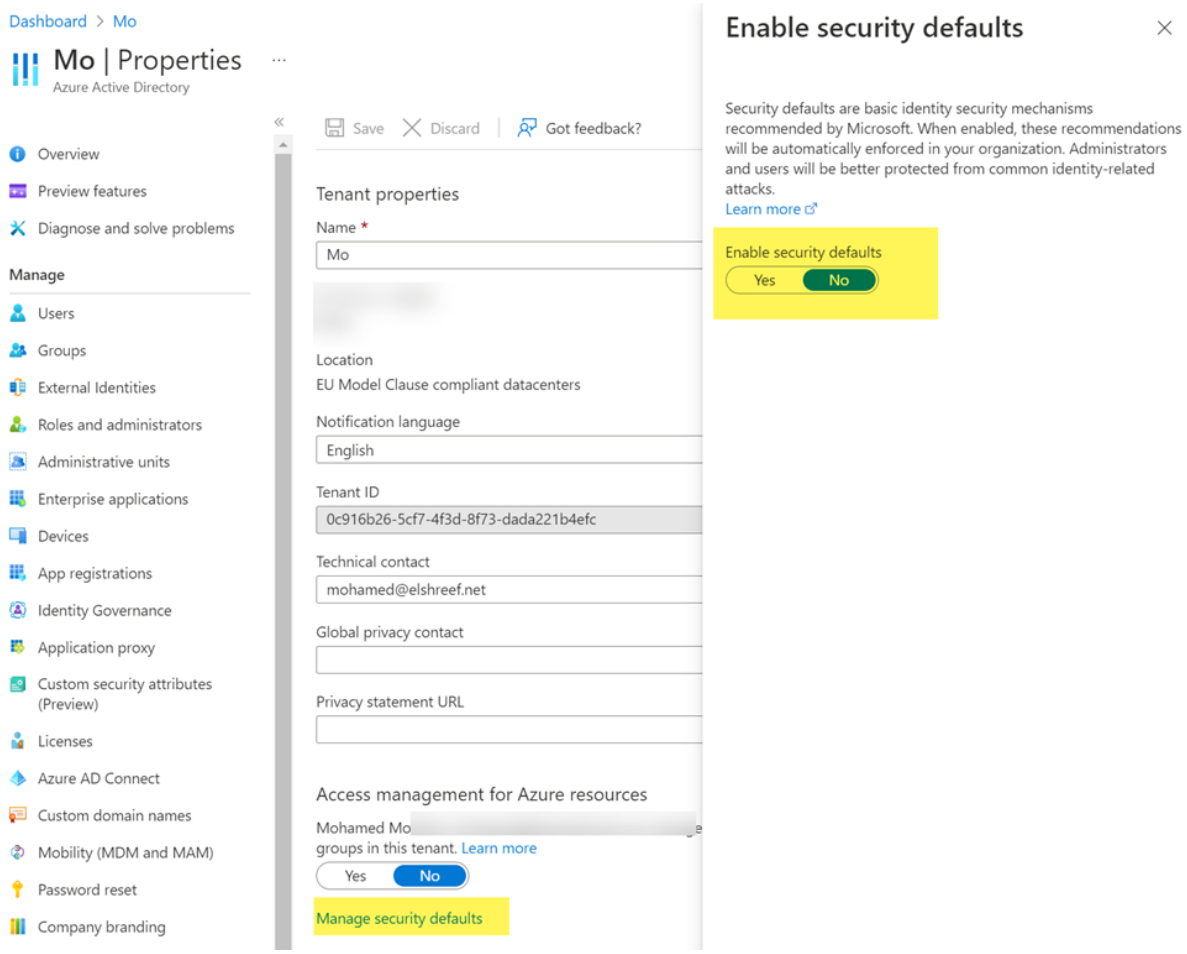
As per our simple deployment we will select the below to match the above table


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

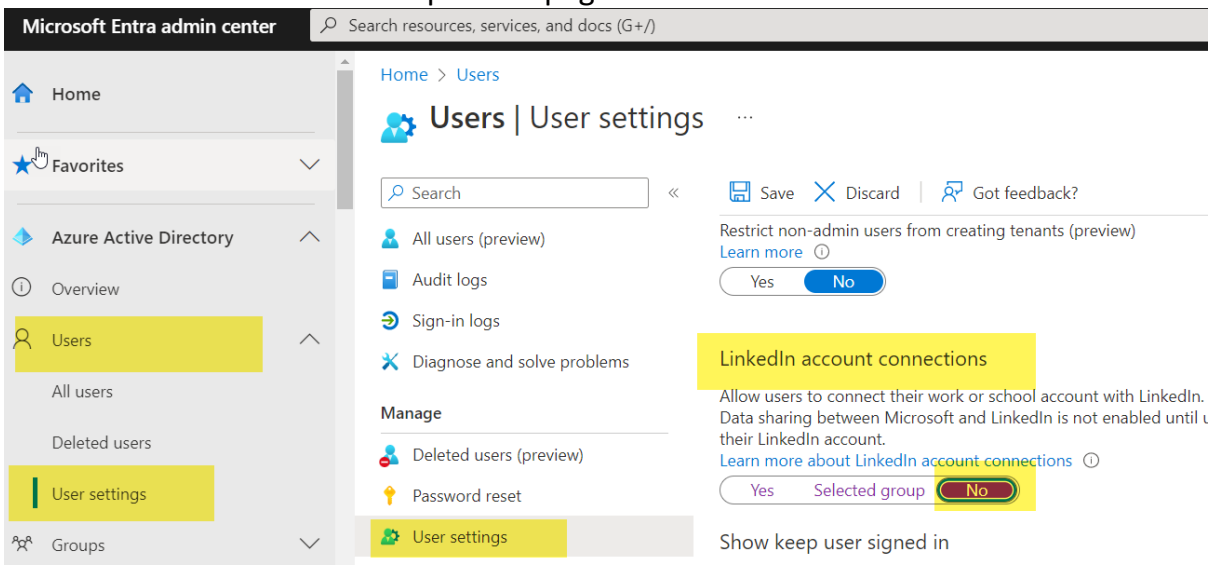
Instead of Security Defaults its recommended to use Conditional Access to control and manage the MFA,To disable security defaults in your directory:

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.



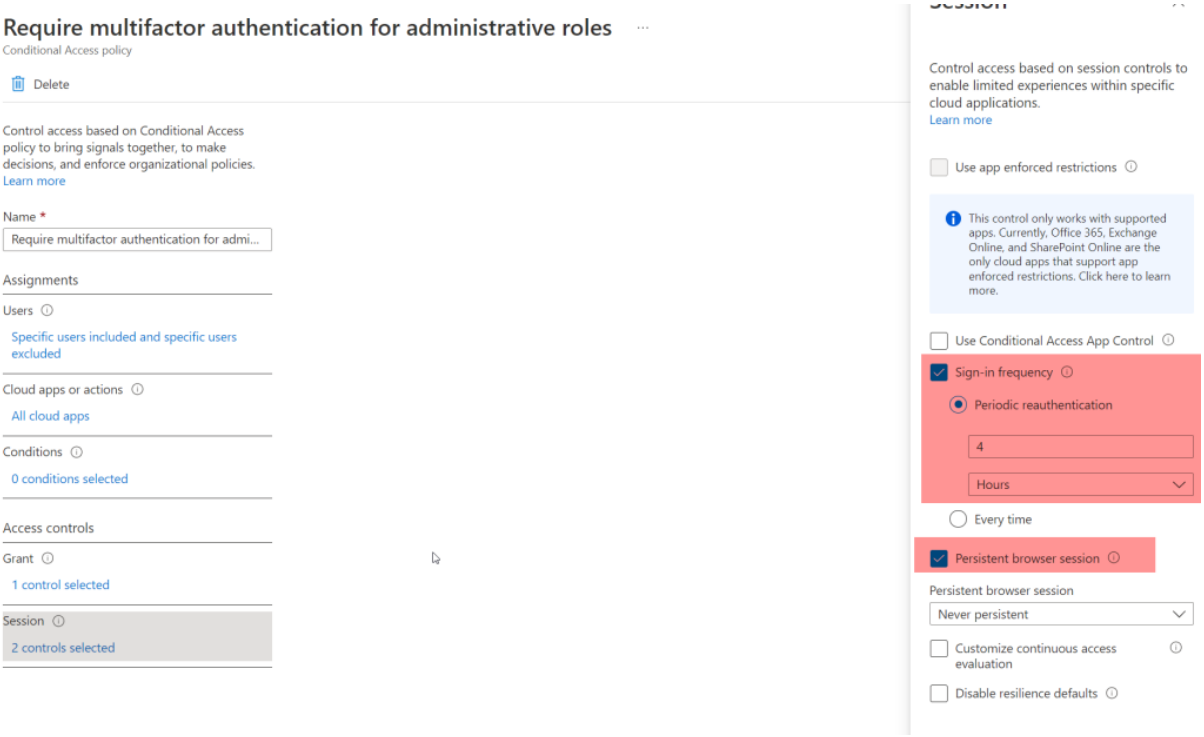
13) Ensure that LinkedIn contact synchronization is disabled.

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.



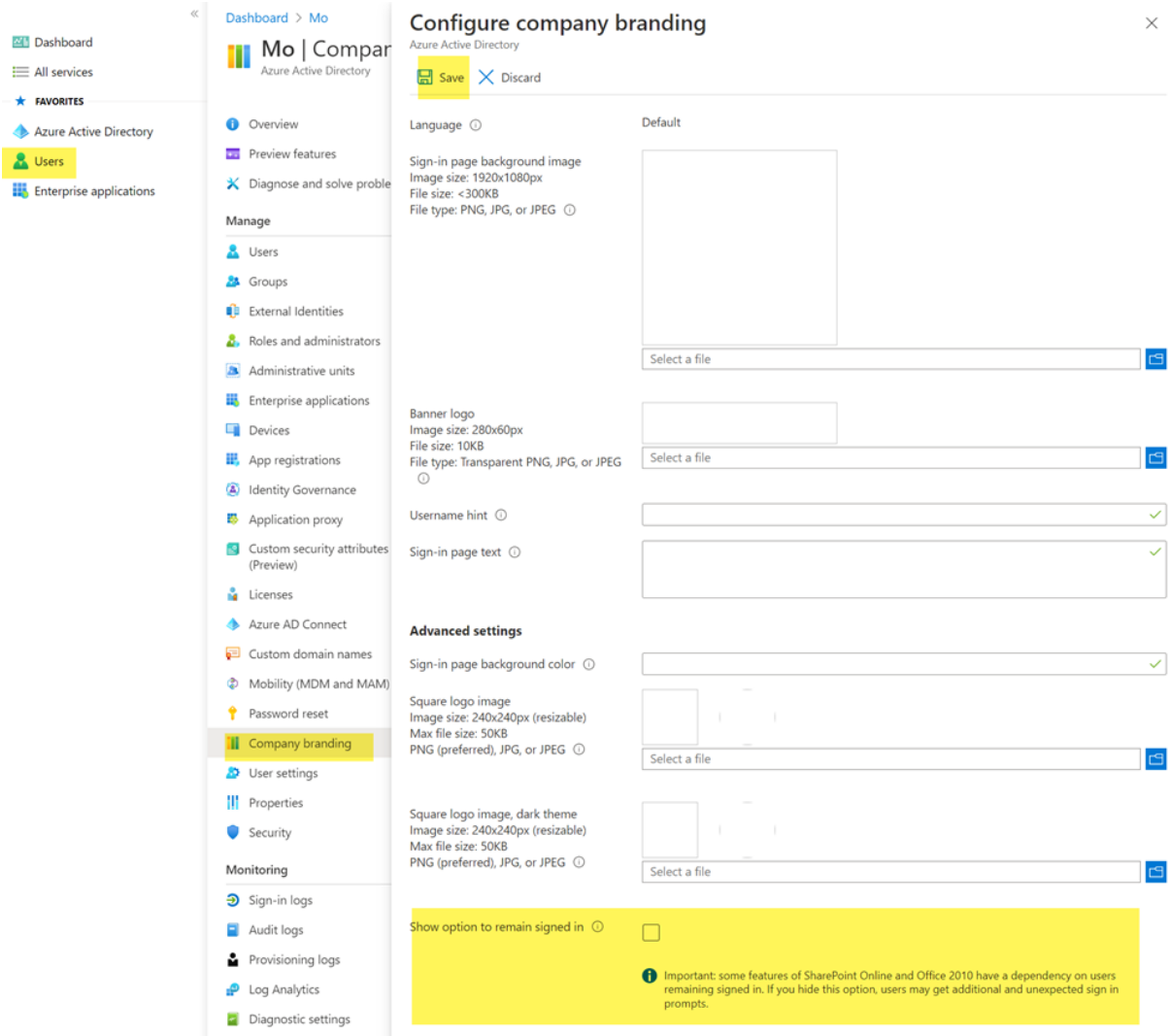
14) Ensure Sign-in frequency is Enabled, and browser sessions are not persistent for Administrative Users.

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 *
Require multifactor authentication for admi...
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
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
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

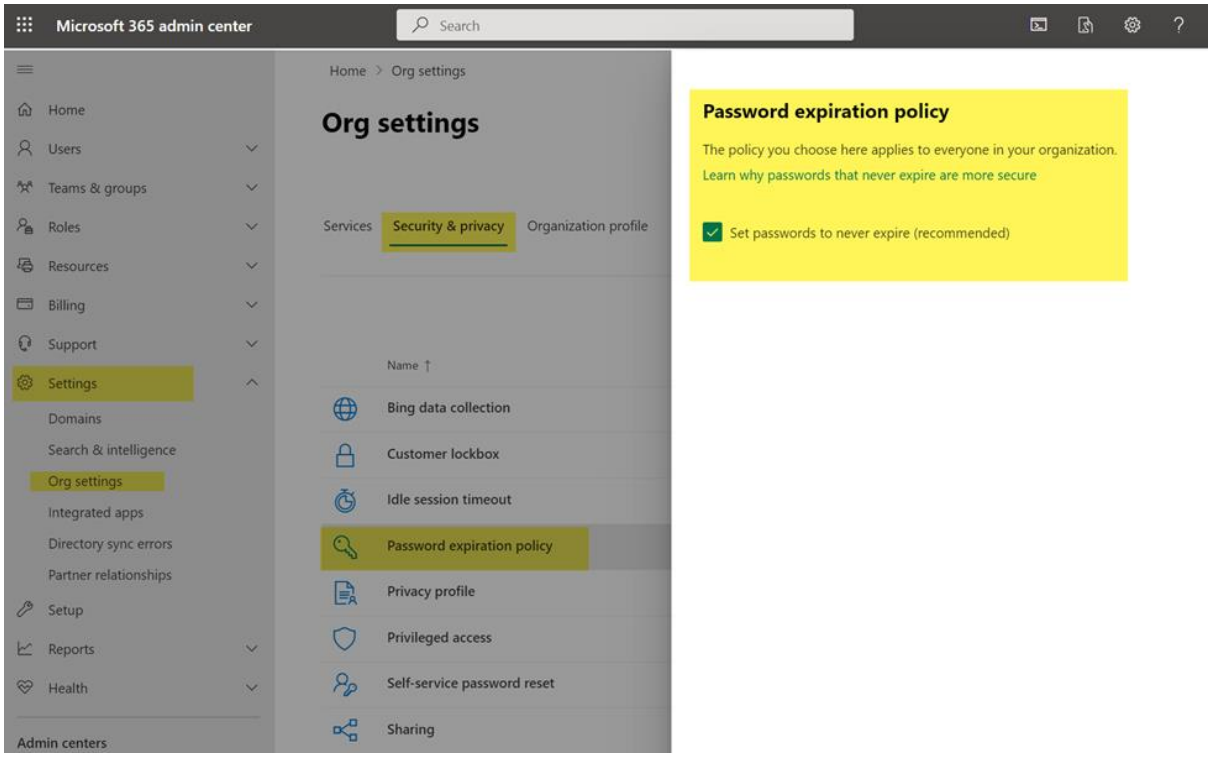
1. Log in to https://portal.azure.com
2. Click on Azure Active Directory
3. Under Manage select Company branding followed by the appropriate Locale policy.
4. If no policy exists, you will need to click Configure to create one
5. Scroll to the bottom of the newly opened pane and ensure Show option to 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

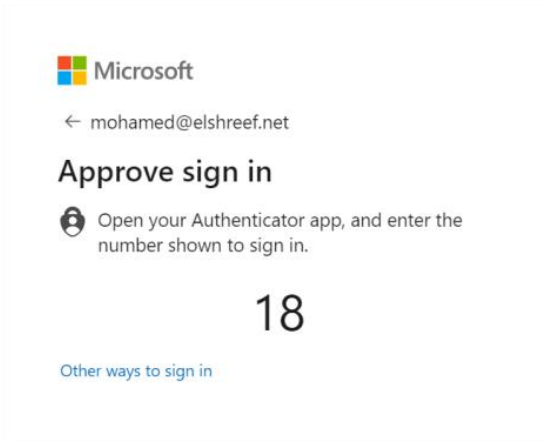
- Be sure to create separate accounts for users to do Global Administrator tasks.
- Make sure that your Global Administrators don't accidentally open emails or run programs with their administrator accounts.
- Be sure those accounts have their email forwarded to a working mailbox.
- Global Administrator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

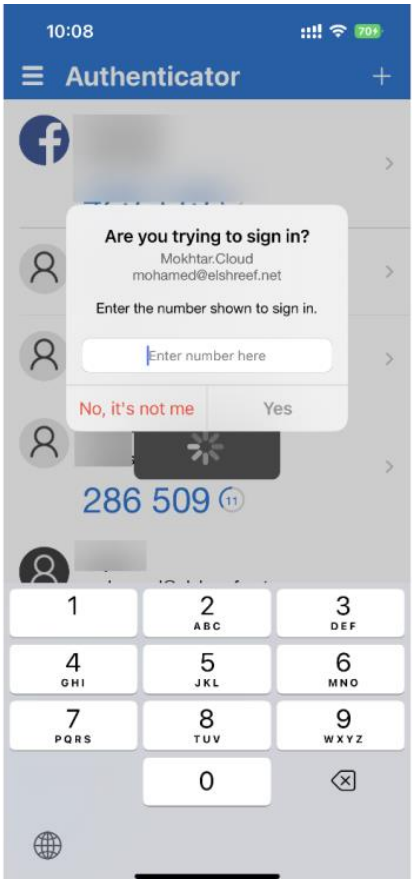
18) Passwordless sign-in with the Microsoft Authenticator app

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.



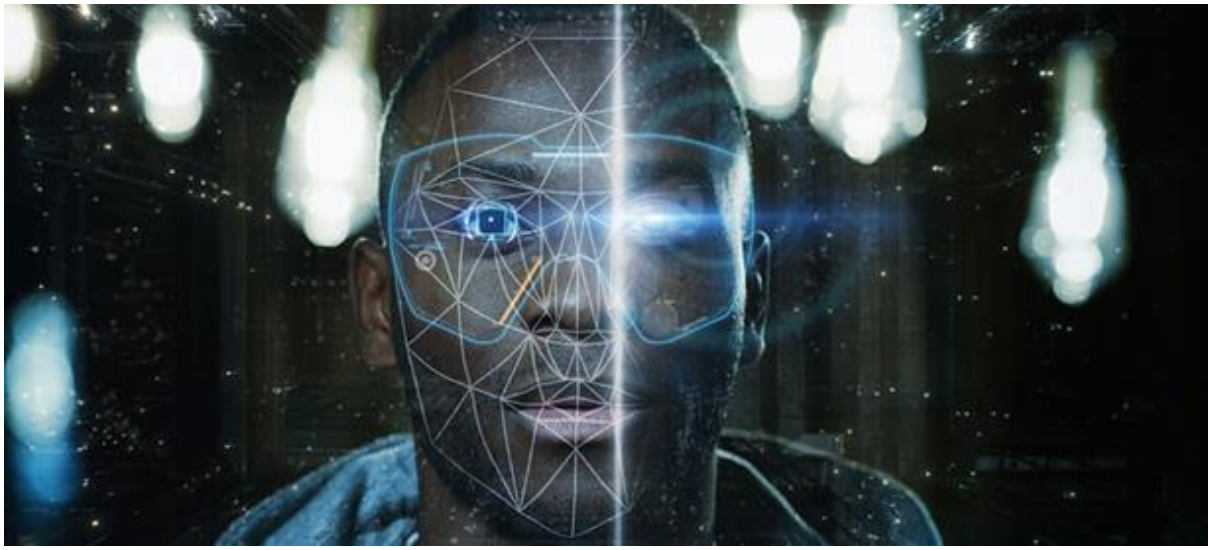


19) Passwordless: Windows Hello for Business

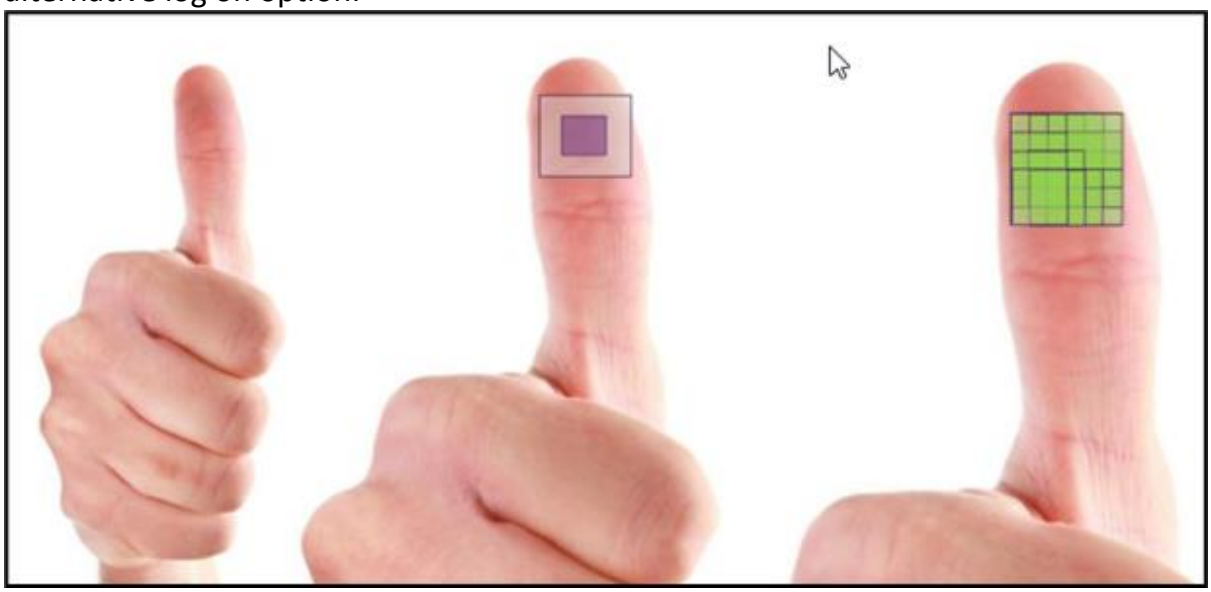
In Windows 10&11, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

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.

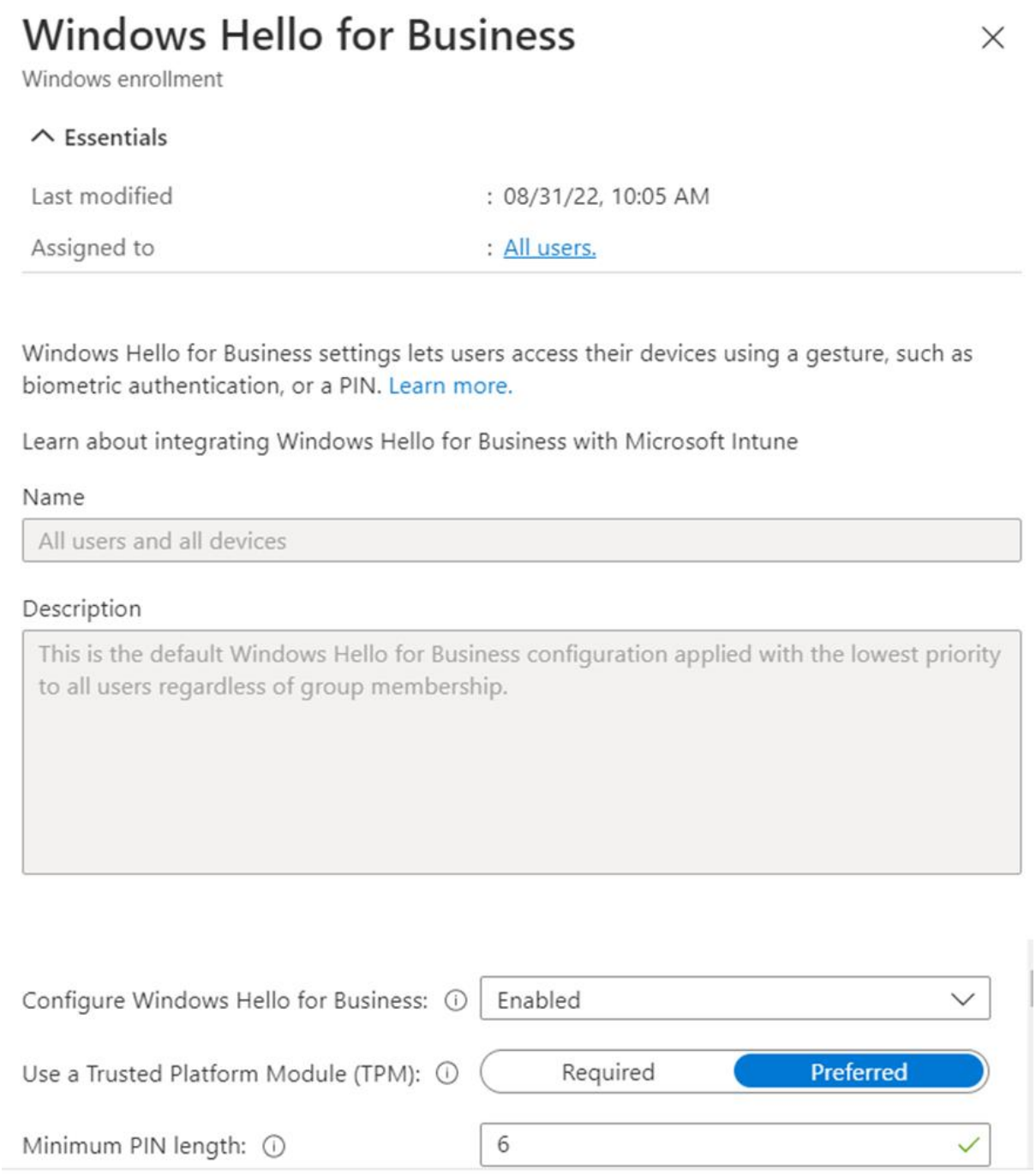


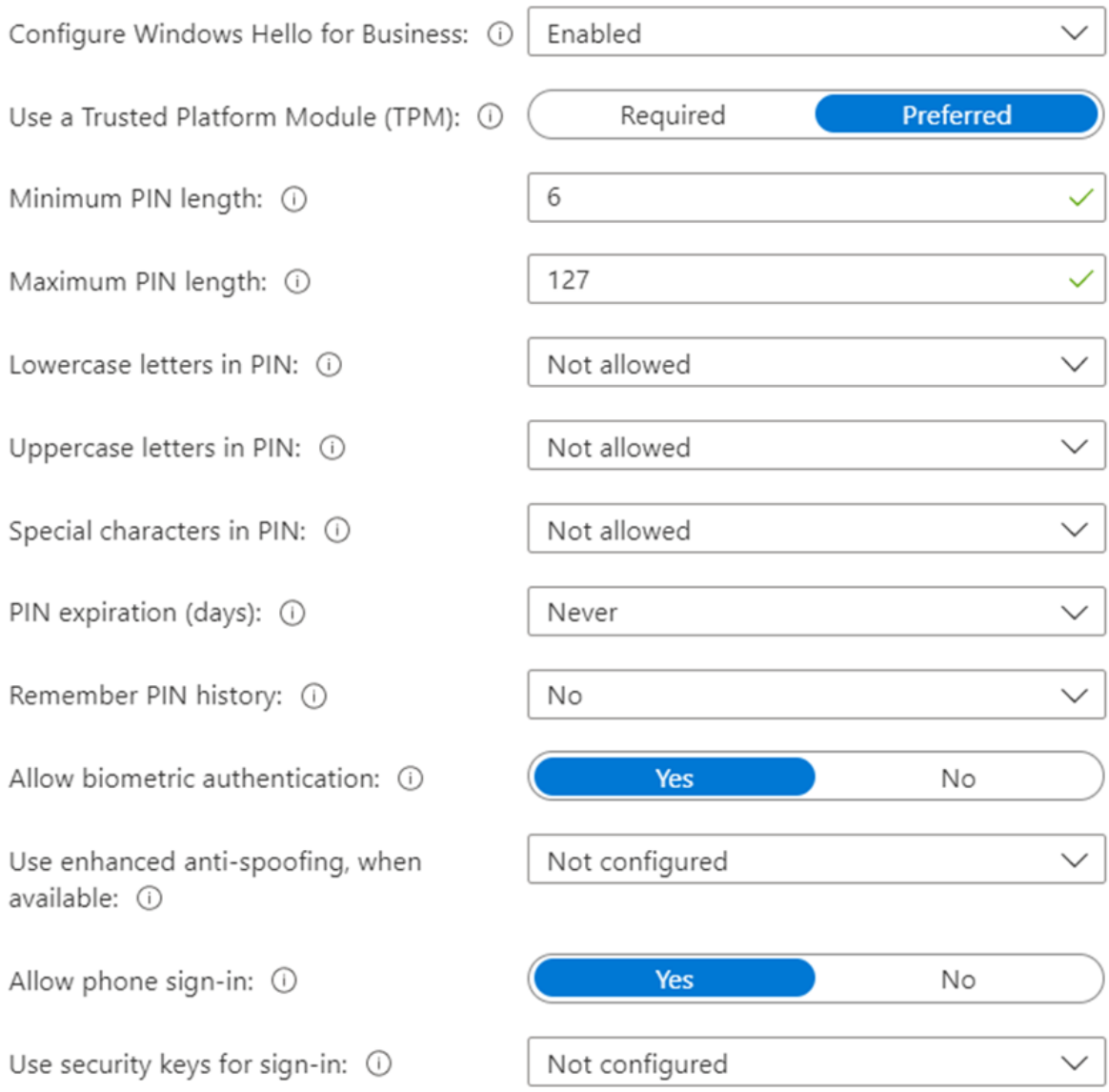
Fingerprint sensors, or sensors that use an employee's unique fingerprint as an alternative log on option.



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

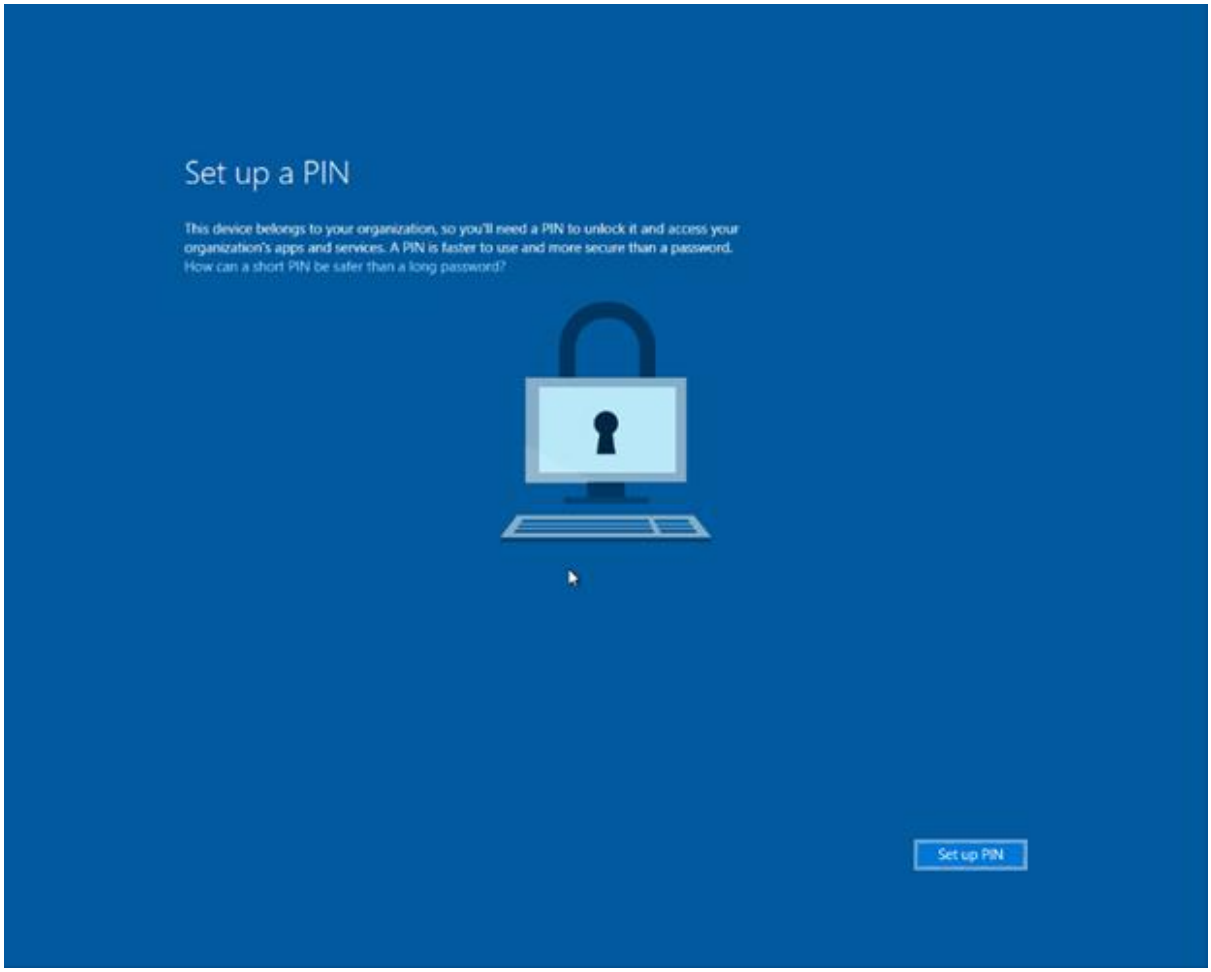
Enable Windows Hello for Business using Microsoft Endpoint Manager for all users (Alternative you can create a configuration profile rule if you want to apply WHfB for specific group)


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

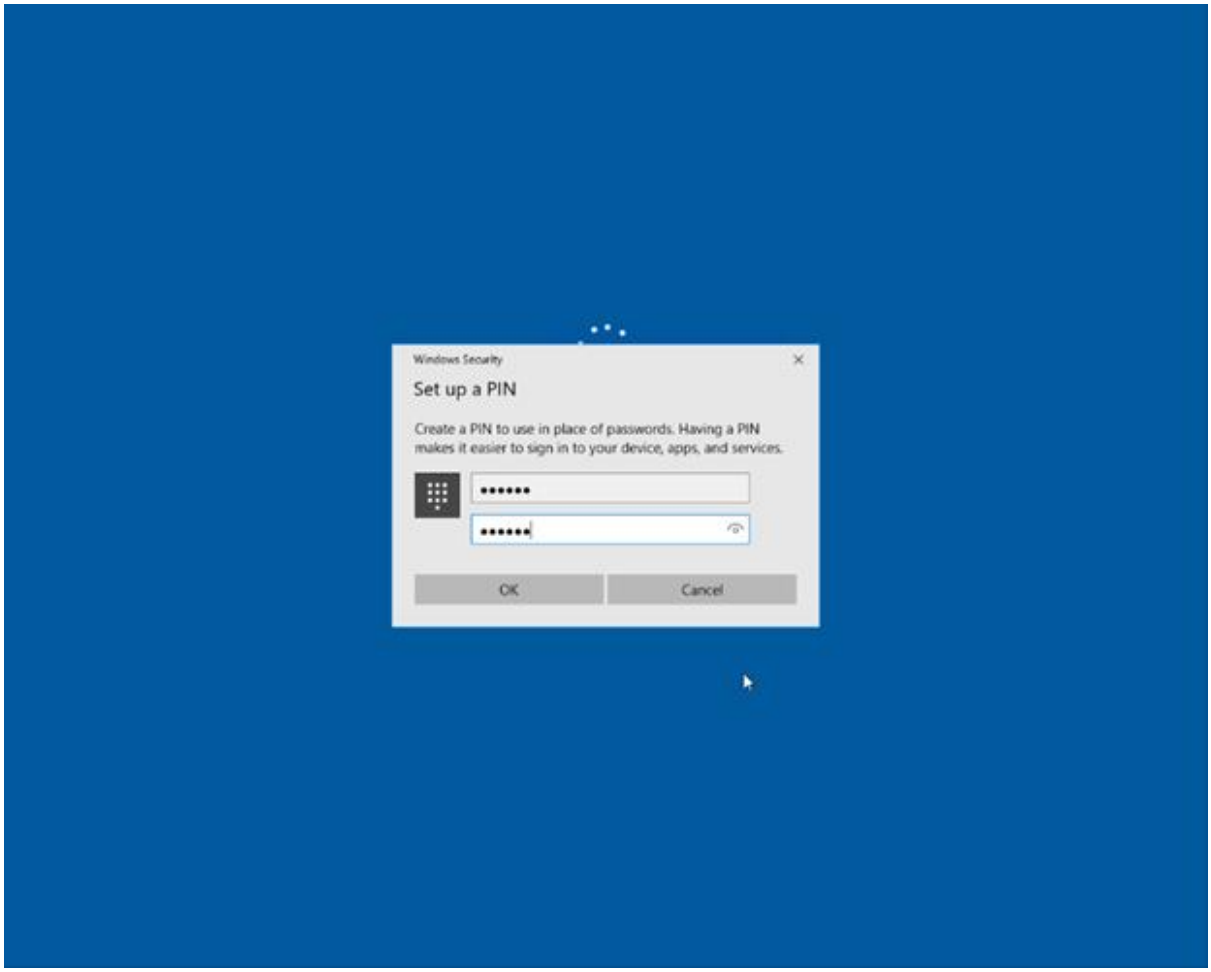


Registration

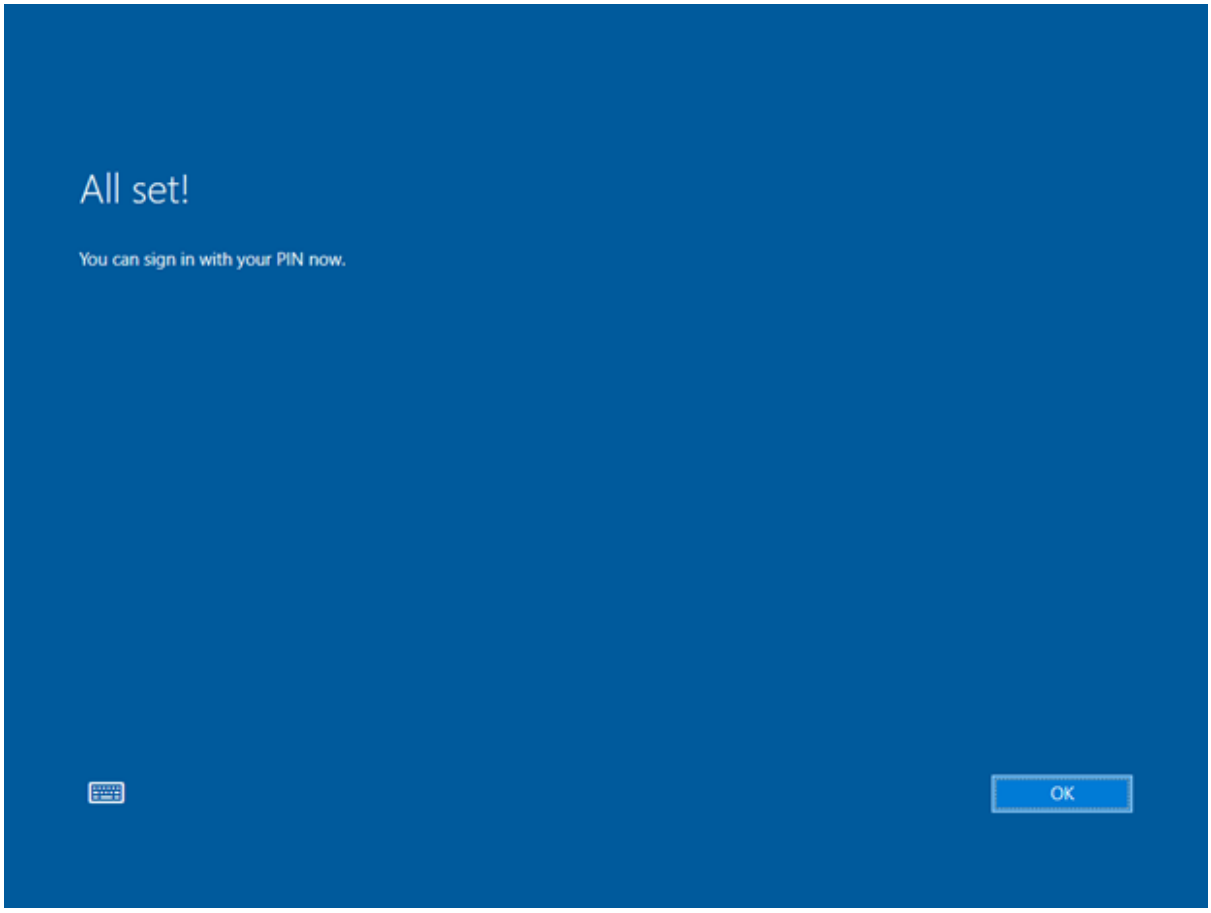
Windows Hello for Business provisioning begins with a full screen page with the title **Setup a PIN** and button with the same name. The user clicks **Setup a PIN**.



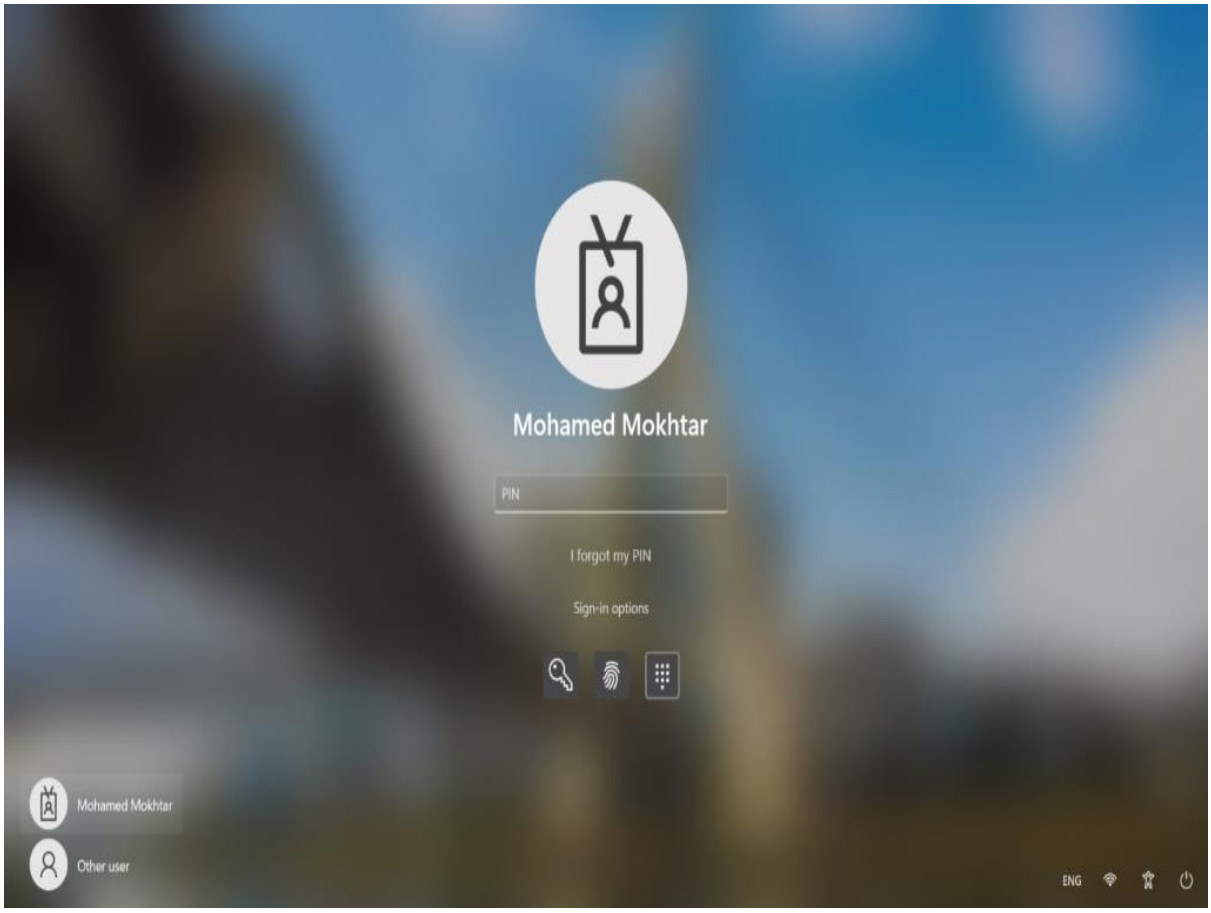
After a successful MFA, the provisioning flow asks the user to create and validate a PIN. This PIN must observe any PIN complexity requirements that you deployed to the environment.


Windows Security
Set up a PIN
Create a PIN to use in place of passwords. Having a PIN makes it easier to sign in to your device, apps, and services.
OK
Cancel

All set!

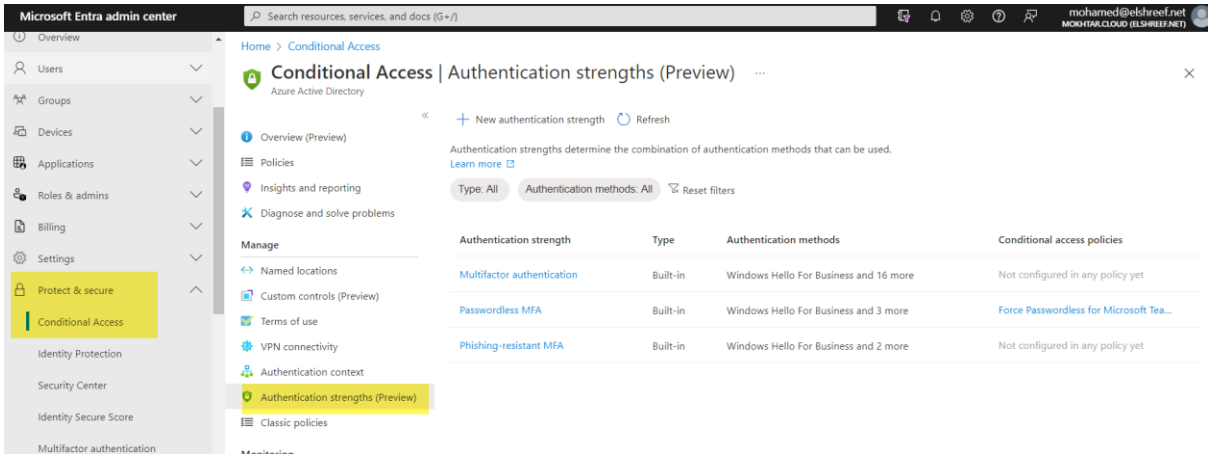


The last thing to do is to check if everything works fine

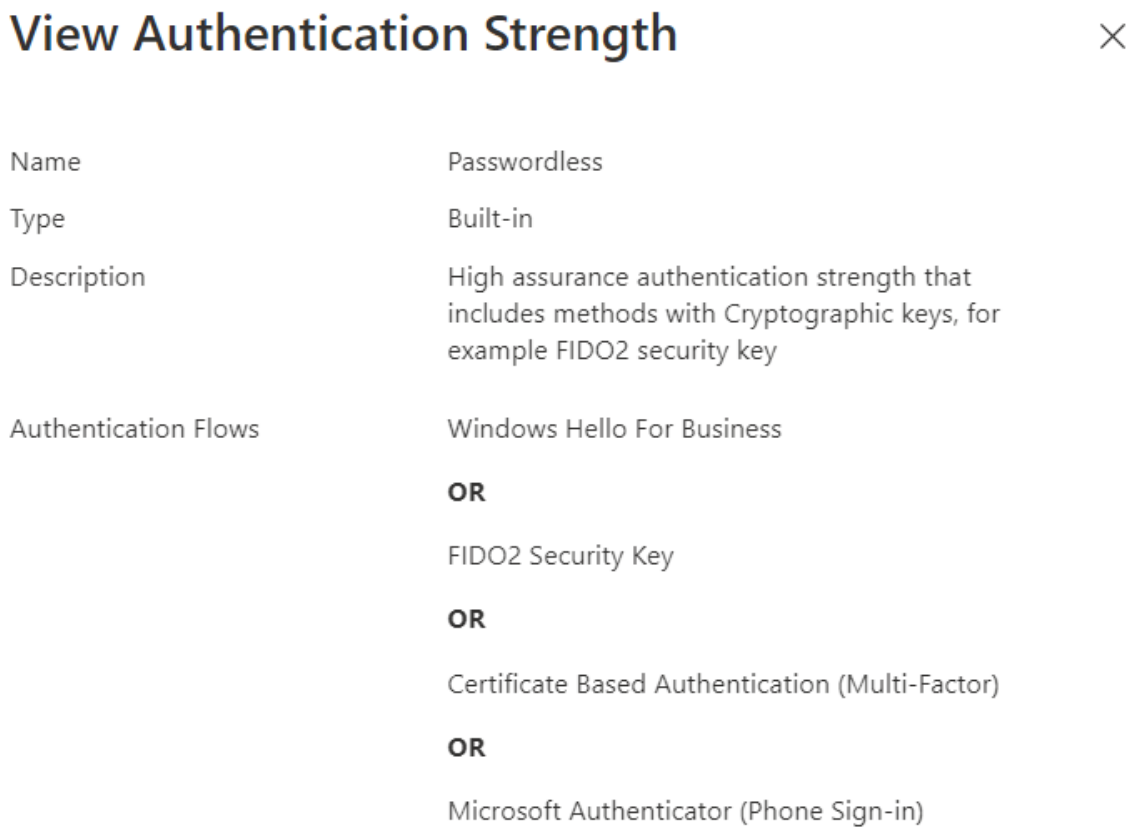

Mohamed Mokhtar
PIN
I forgot my PIN
Sign-in options
Mohamed Mokhtar
Other user
ENG

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

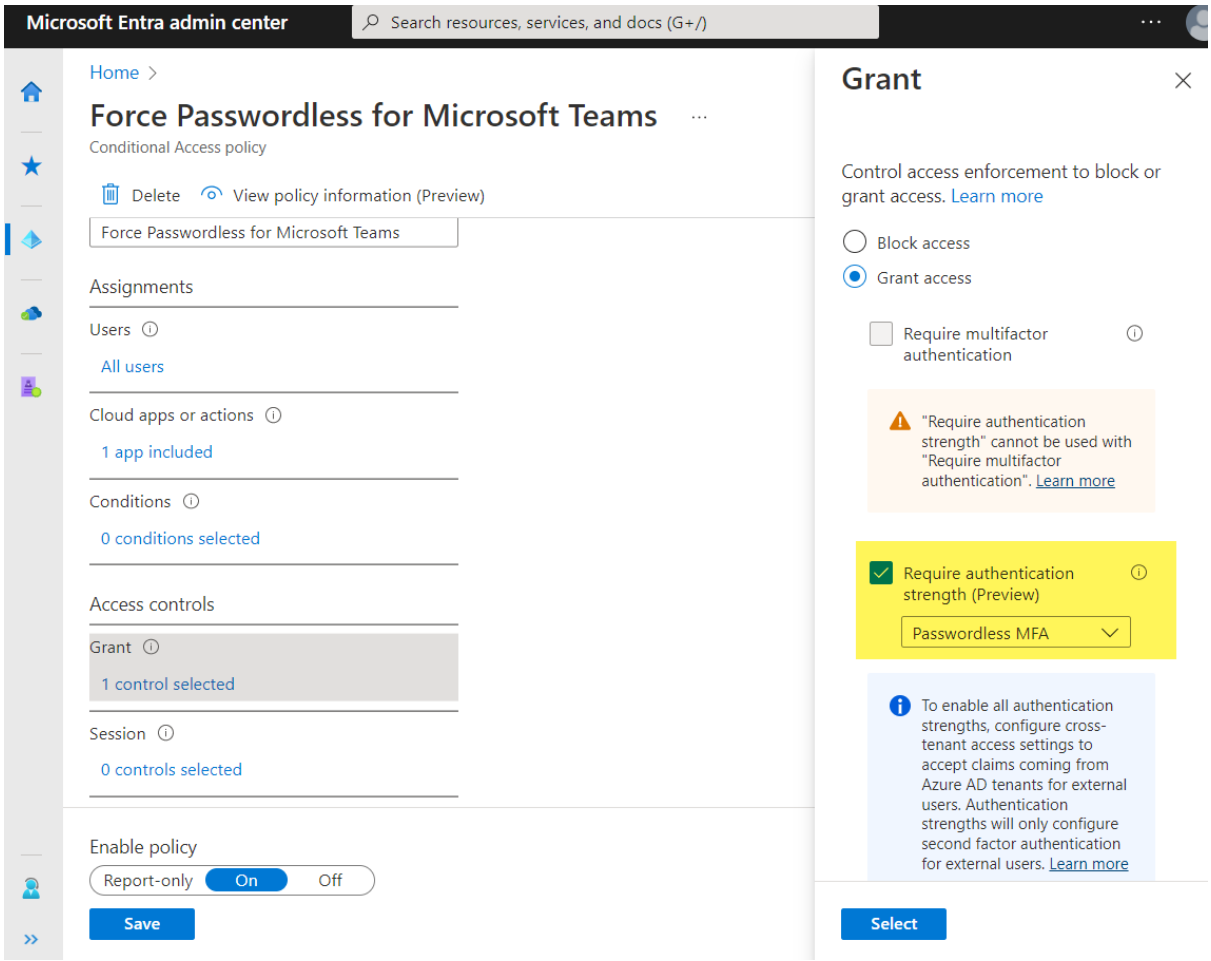
Authentication Strength enable the IT admin to force the combination of authentication methods that can be used with the conditional access.



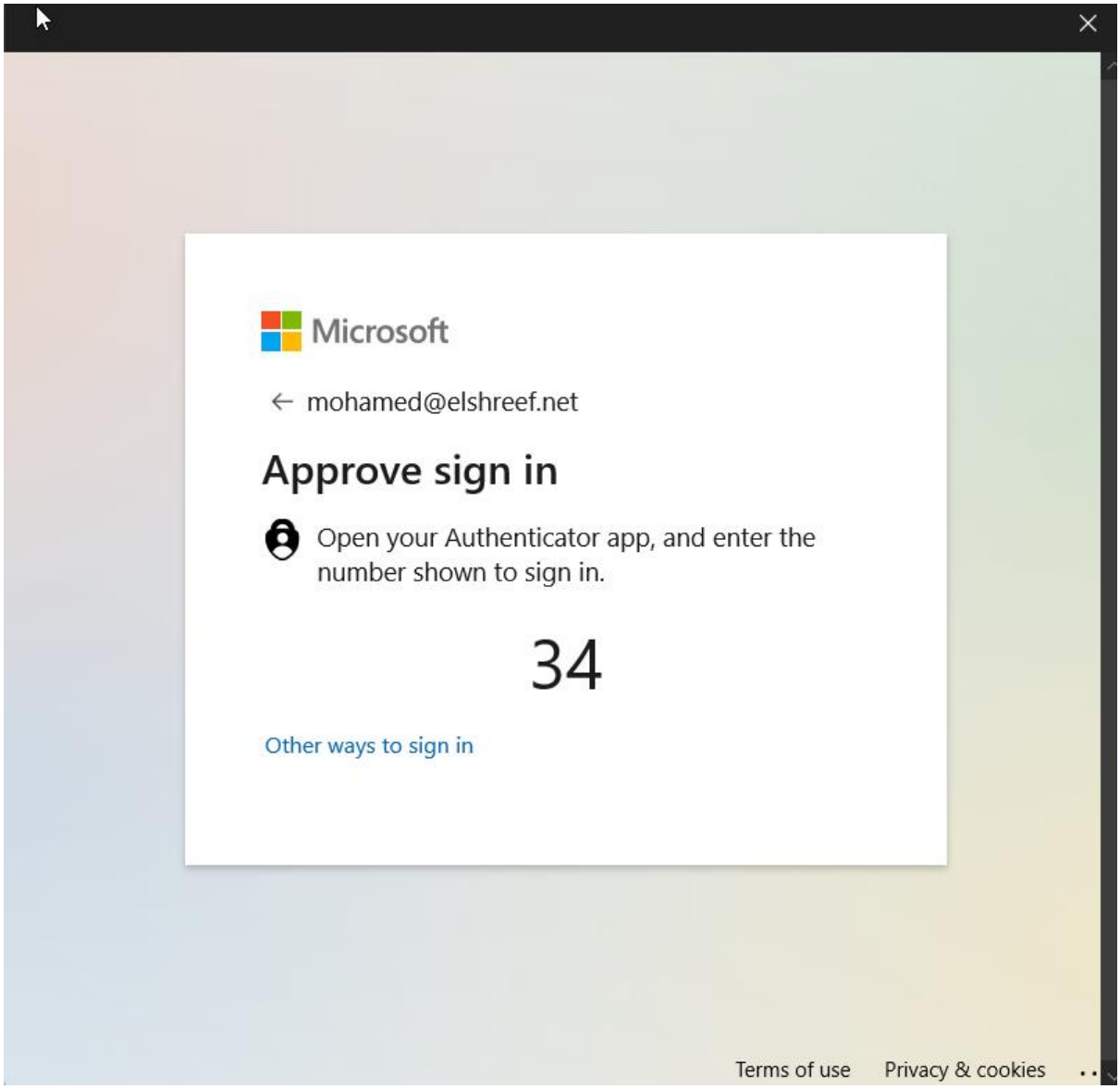
The following screenshot shows the properties of one of the built-in pre-created authentication strength



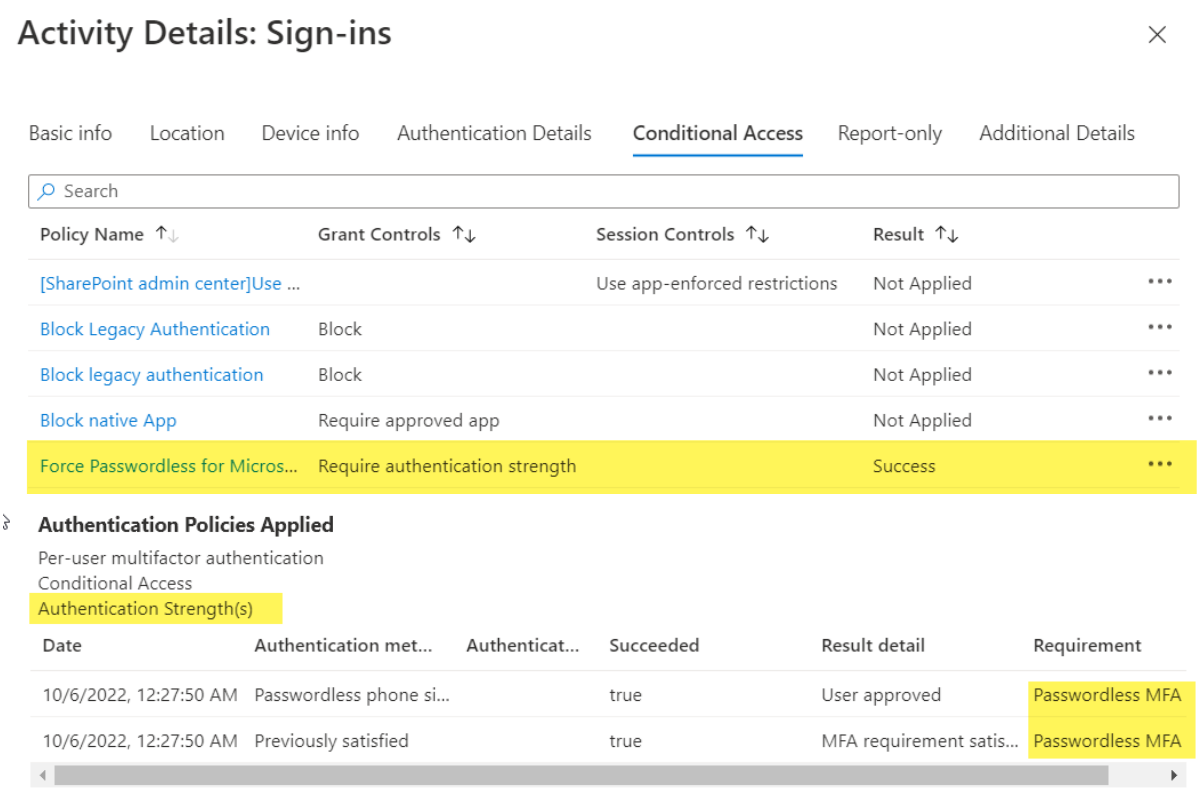
I created a conditional access policy to force passwordless while login to Microsoft teams as per the below



Testing


Microsoft
mohamed@elshreef.net
Approve sign in
Open your Authenticator app, and enter the number shown to sign in.
34
Other ways to sign in
Terms of use
Privacy & cookies

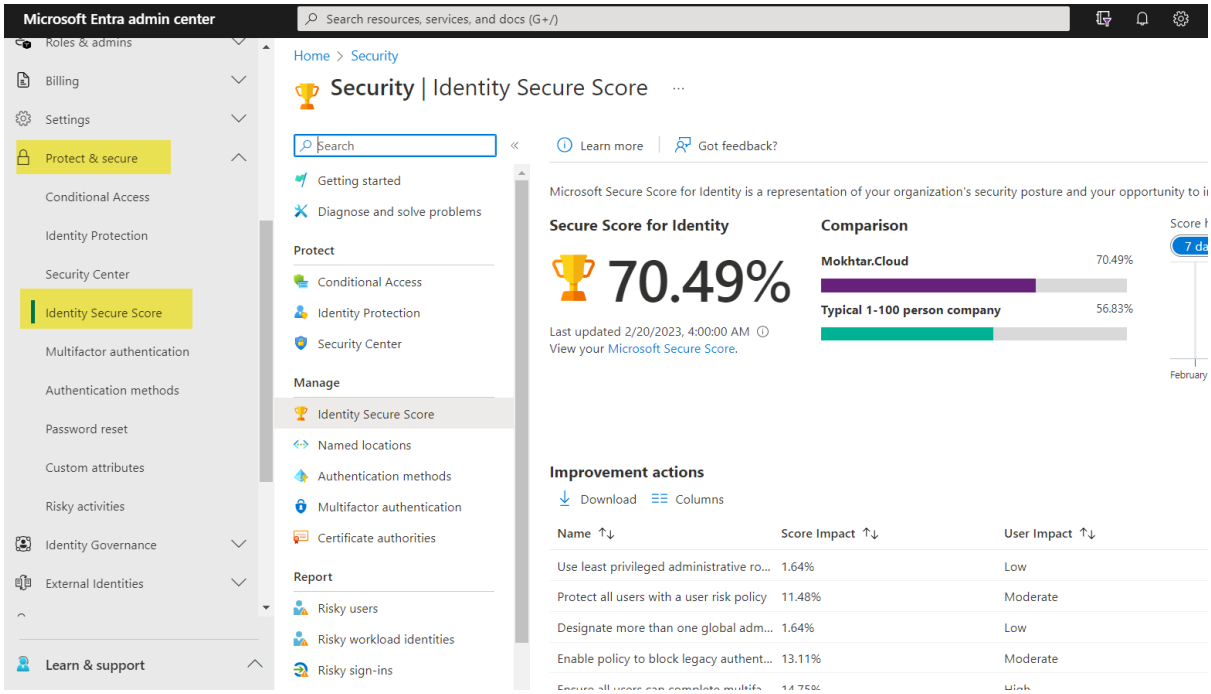
Validation


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.

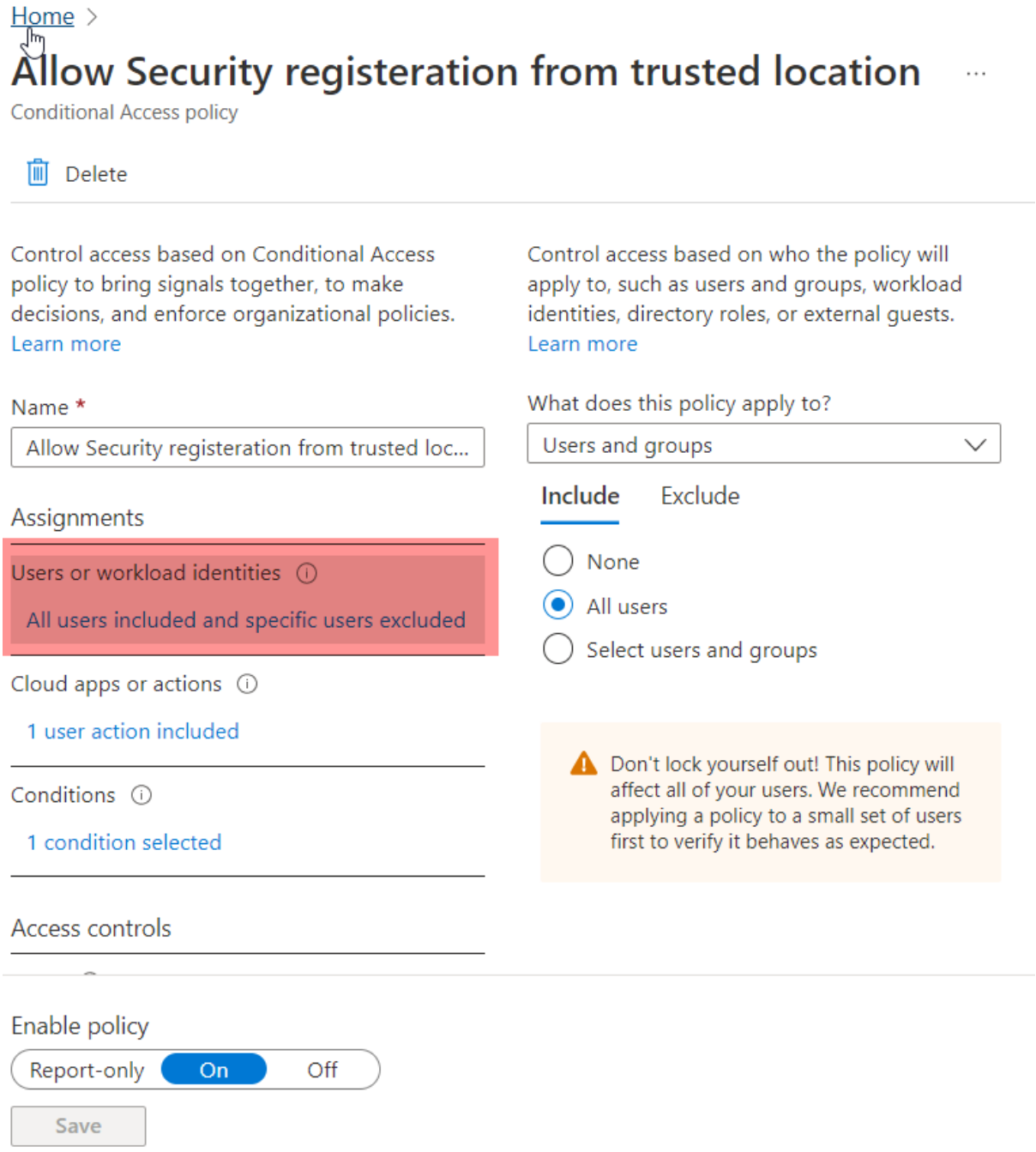
1. Log in to https://entra.microsoft.com/
2. Select Azure Active Directory Then Protect & Secure then Identity Secure Score



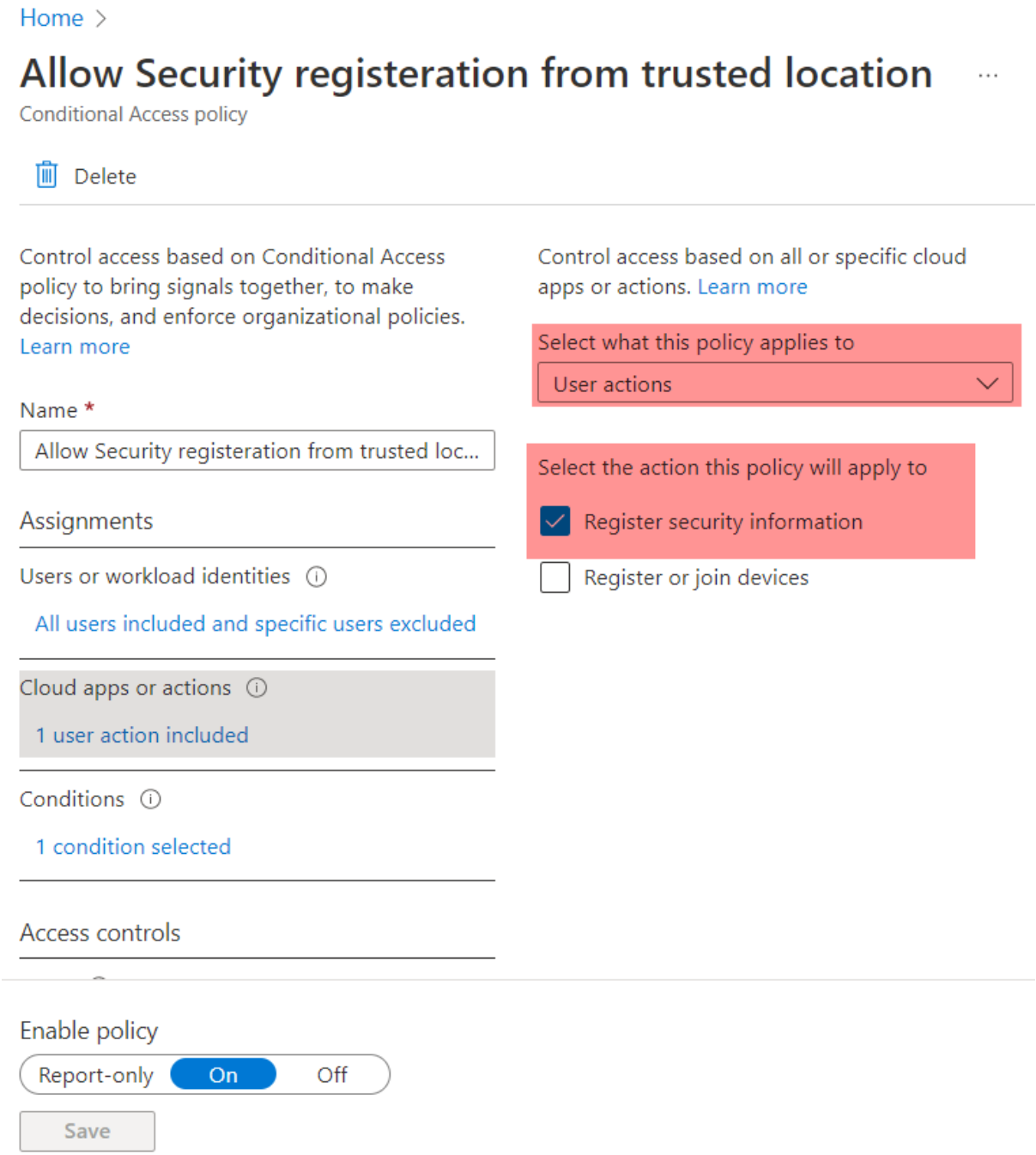
22) Require trusted location for MFA and SSPR registration

Log in to https://entra.microsoft.com/
Select Protect & Secure, then select Conditional Access.
Click New policy and provide the policy name

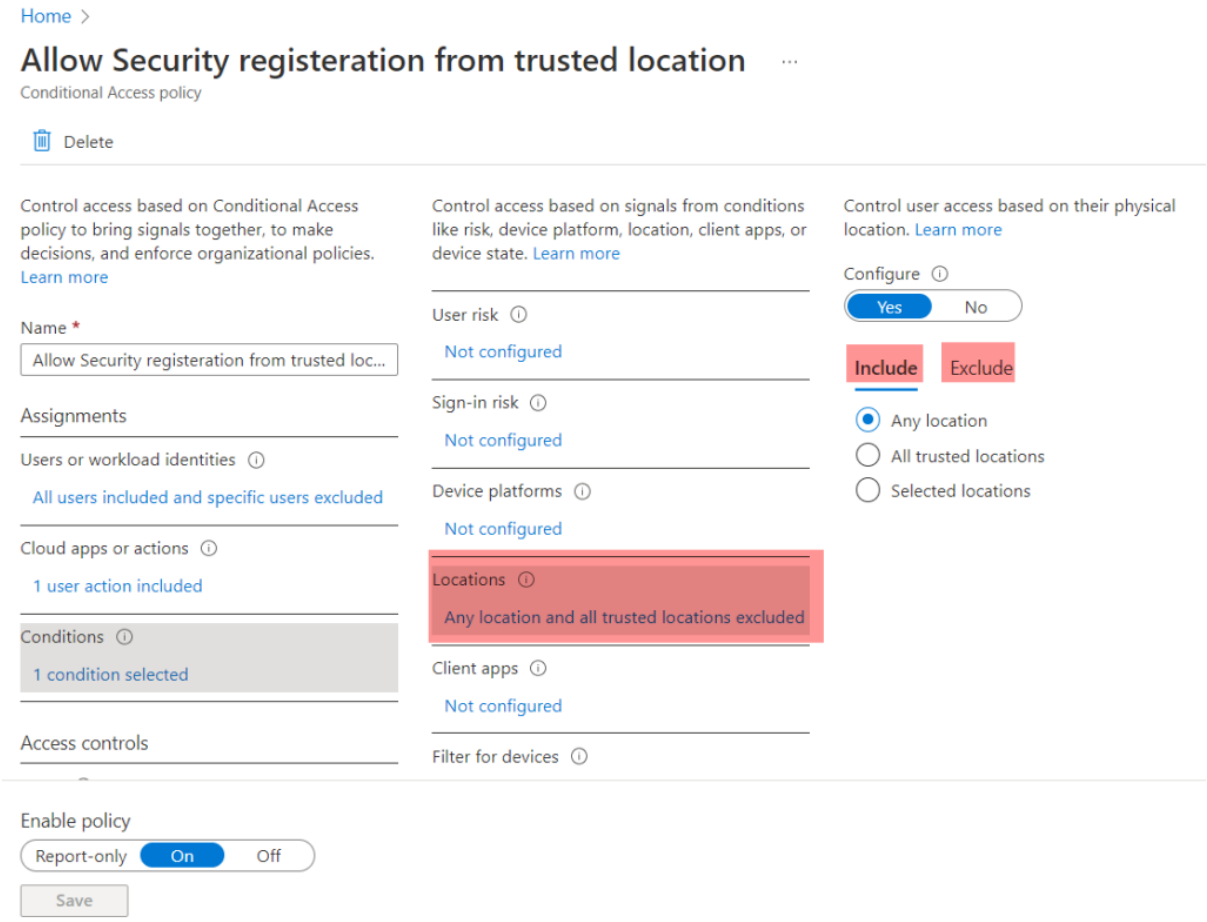
on assignment, assign this policy for all users and exclude emergency admin and other services accounts.



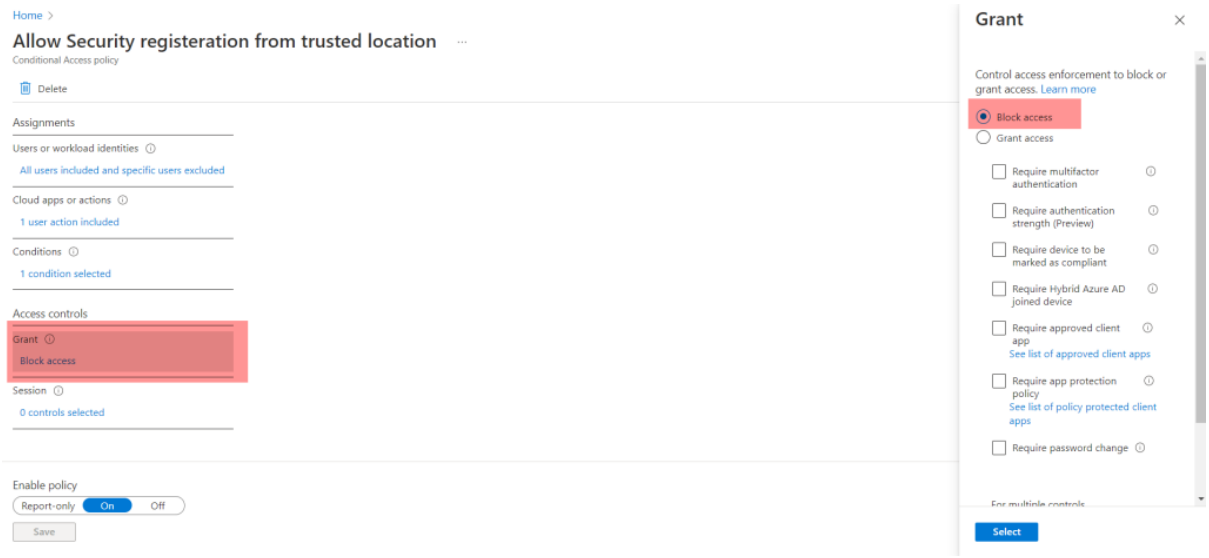
on cloud application, select user actions then register security information



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

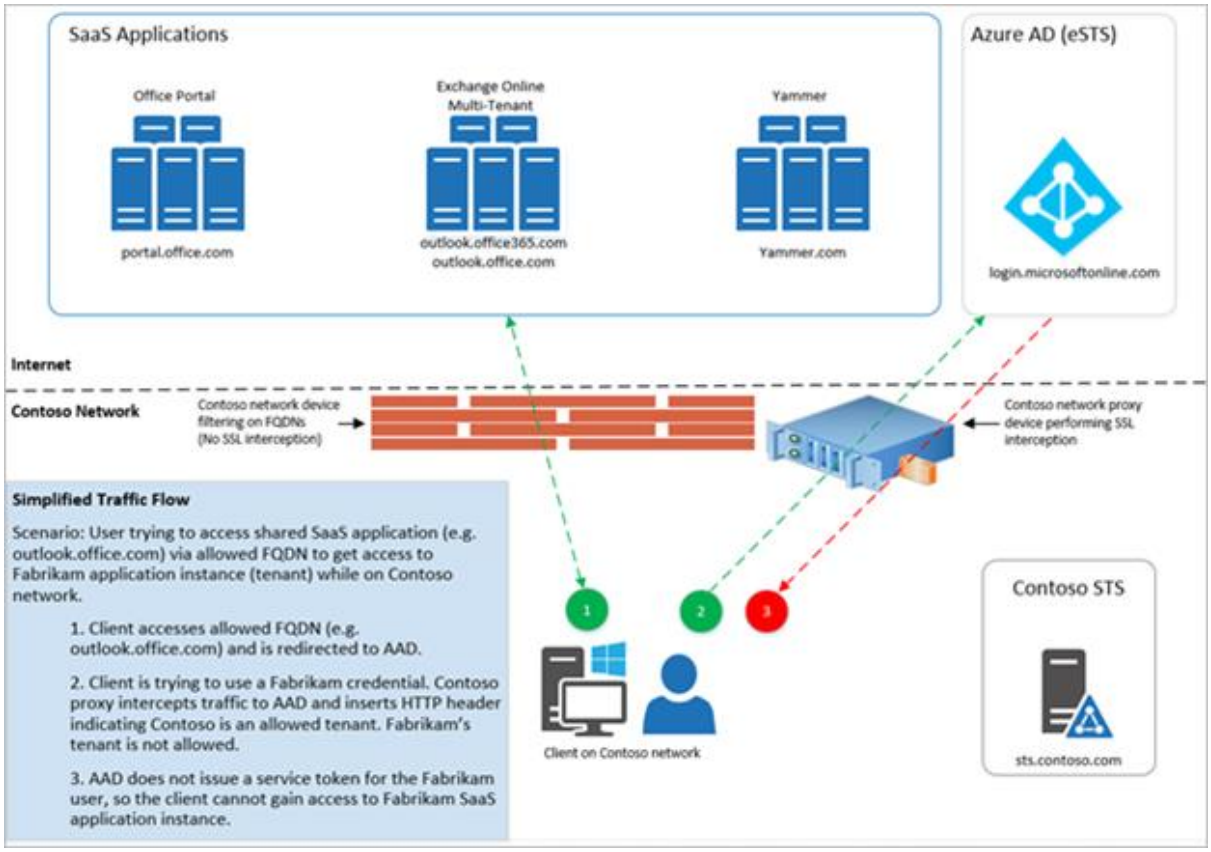


set the grant action to block



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: 456ff232-35l2-5h23-b3b3-3236w0826f3d

* Tenant Domain names

* Tenant ID

*Directory ID

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

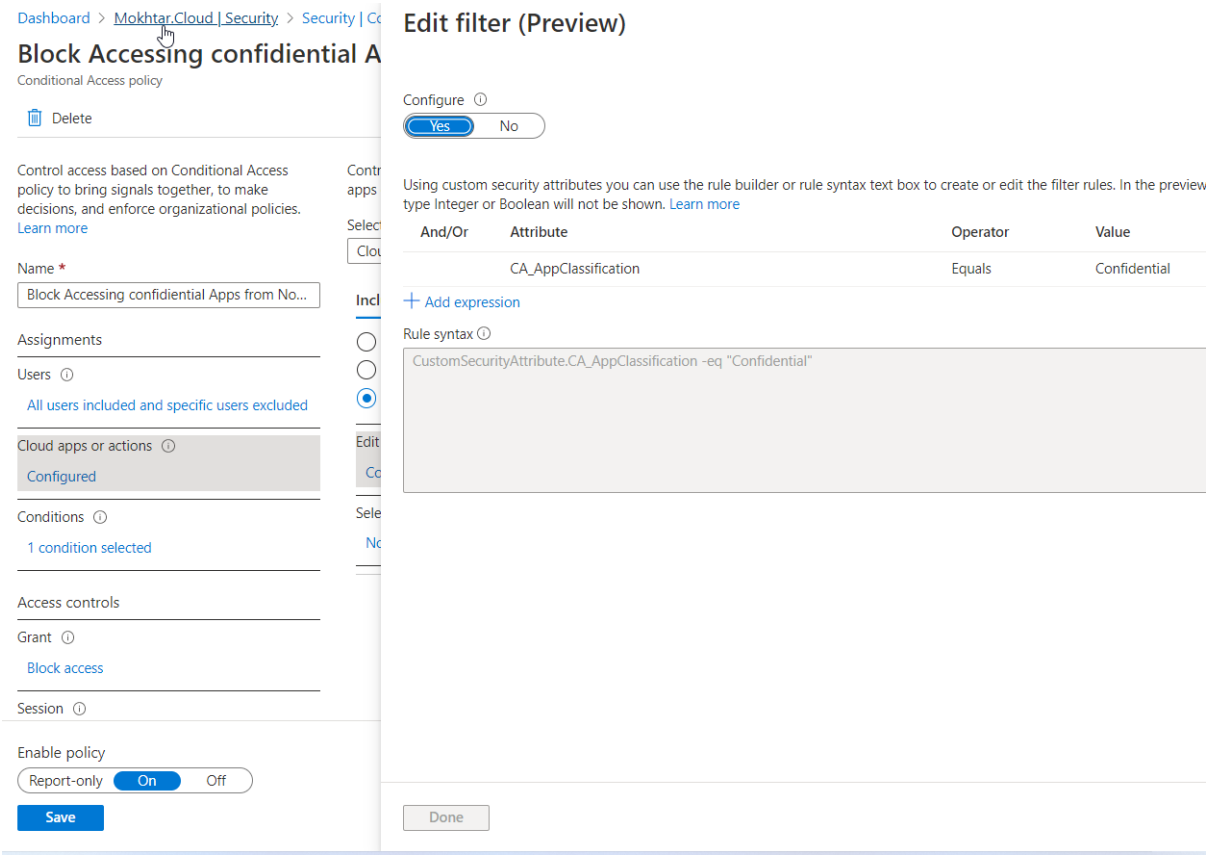
Admin logs

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

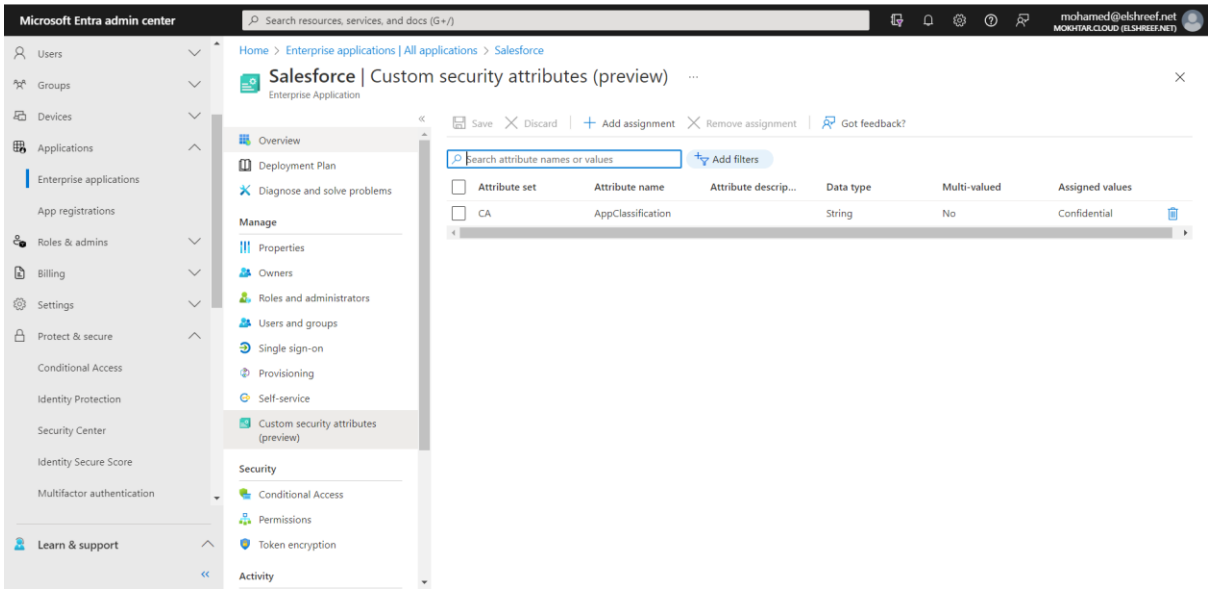
24) Conditional Access filters for apps

A new settings 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.

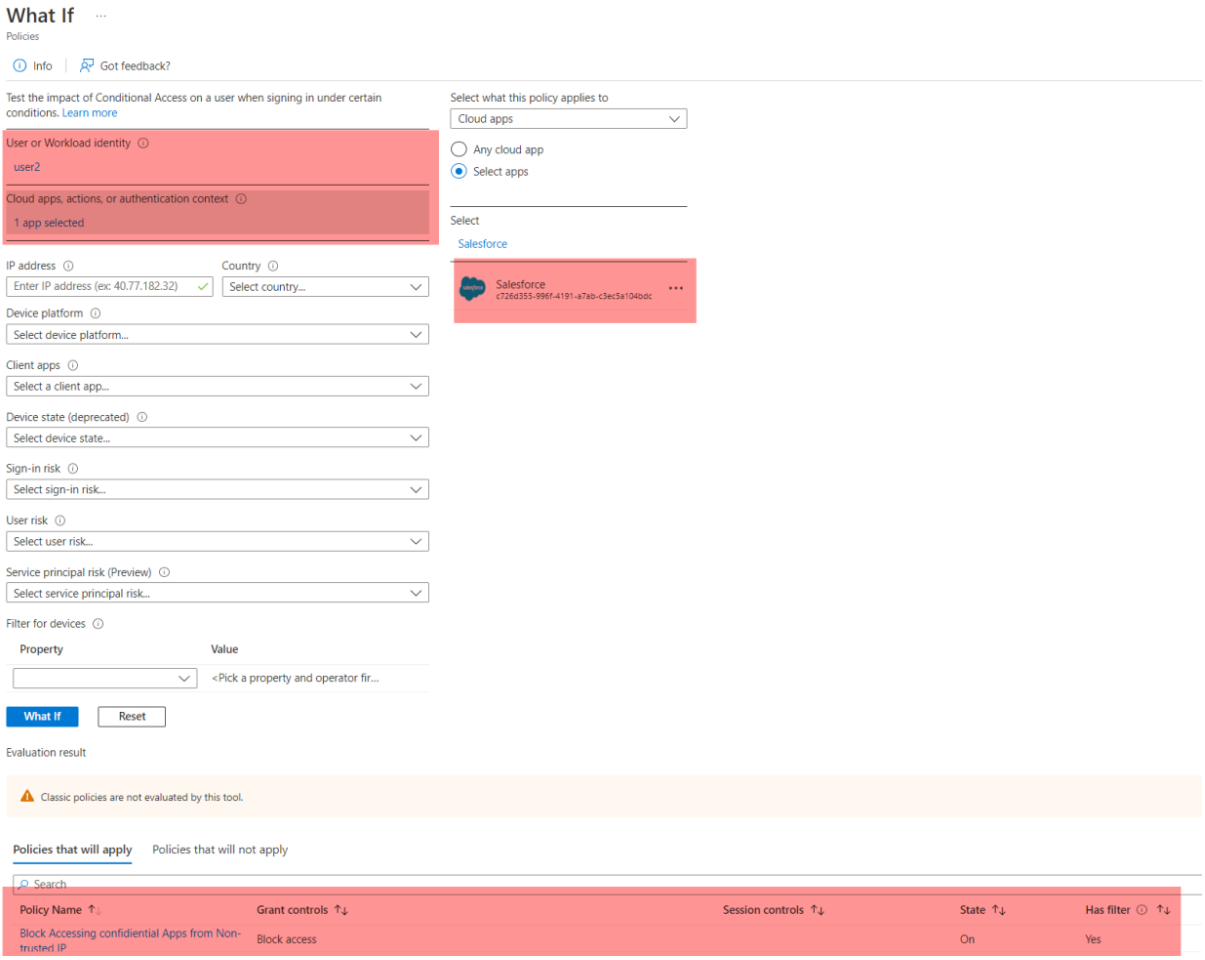
We will create a conditional access policy to block accessing confidential App from untrusted networks , you will find here that we used the new feature App filter to filter the confidential app using the custom security attribute CA_AppClassification



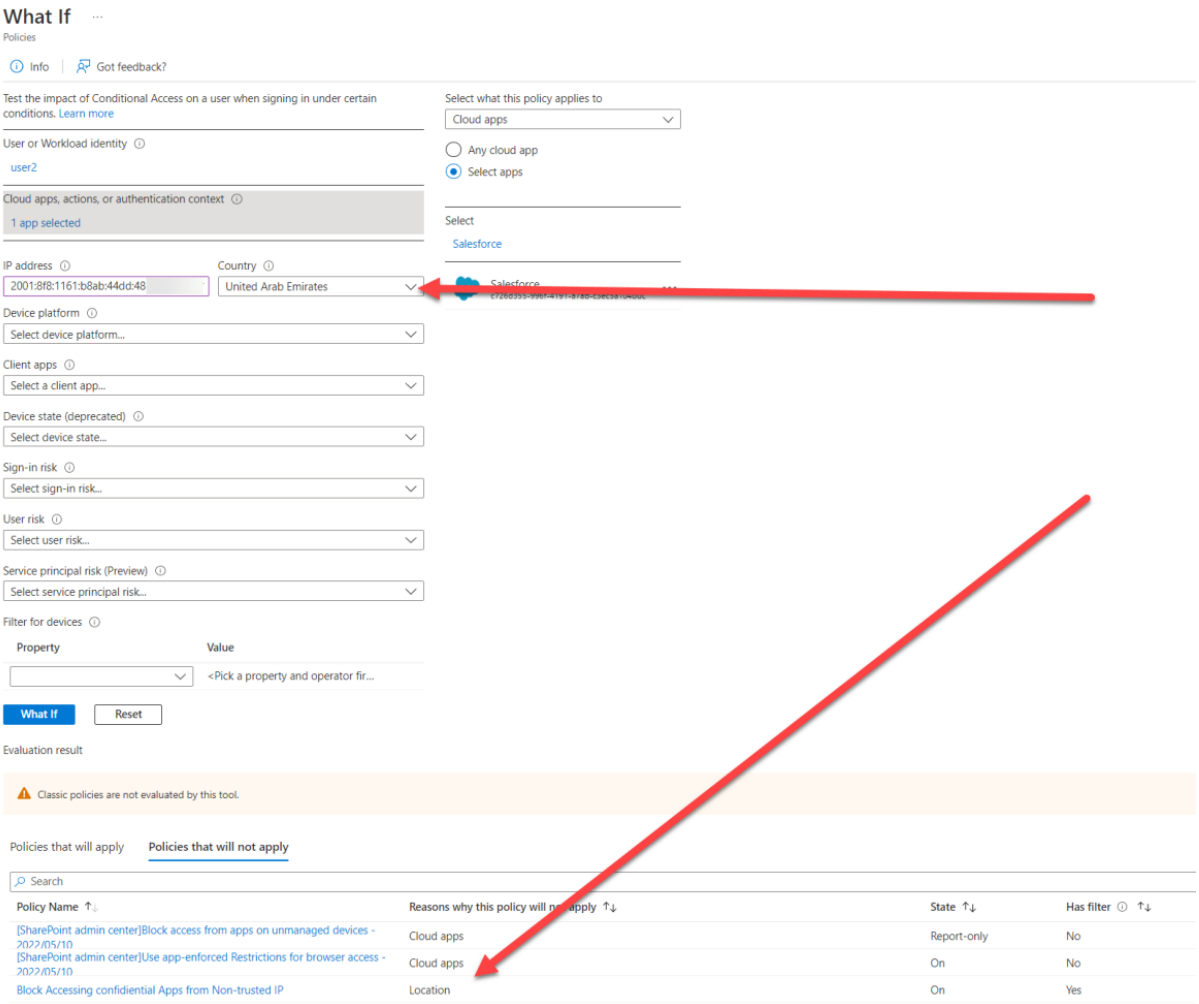
You will need your customized security attributes before creating the conditional access policy, as per the below



Validation "Rule Applied when access from untrusted location"



Validation2: "Rule Skipped when access from trusted location"


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
2001:8f8:1161:b8ab:44dc:48
Country
United Arab Emirates
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.
Select what this policy applies to
Cloud apps
Any cloud app
Select apps
Select
Salesforce
Salesforce
Policies that will apply
Policies that will not apply
Search
Policy Name
Reasons why this policy will not apply
State
Has filter
[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.