Mobile ID Multi-Factor-Authentication for Microsoft Entra ID External Authentication Methods (EAM)

Version 1.0

Table of contents

1 About Microsoft External Authentication Methods (EAM)

MobileID integrates with Microsoft Entra ID as an external authentication method, enabling Multi-Factor-Authentication (MFA) for Entra ID logon. MobileID provides seamless inline user enrolment, self-service device management, and supports a range of authentication methods, including highly secure crypto-SIM tokens and app-based push authentication for iOS and Android, with advanced options such as Number Matching and Geofencing.

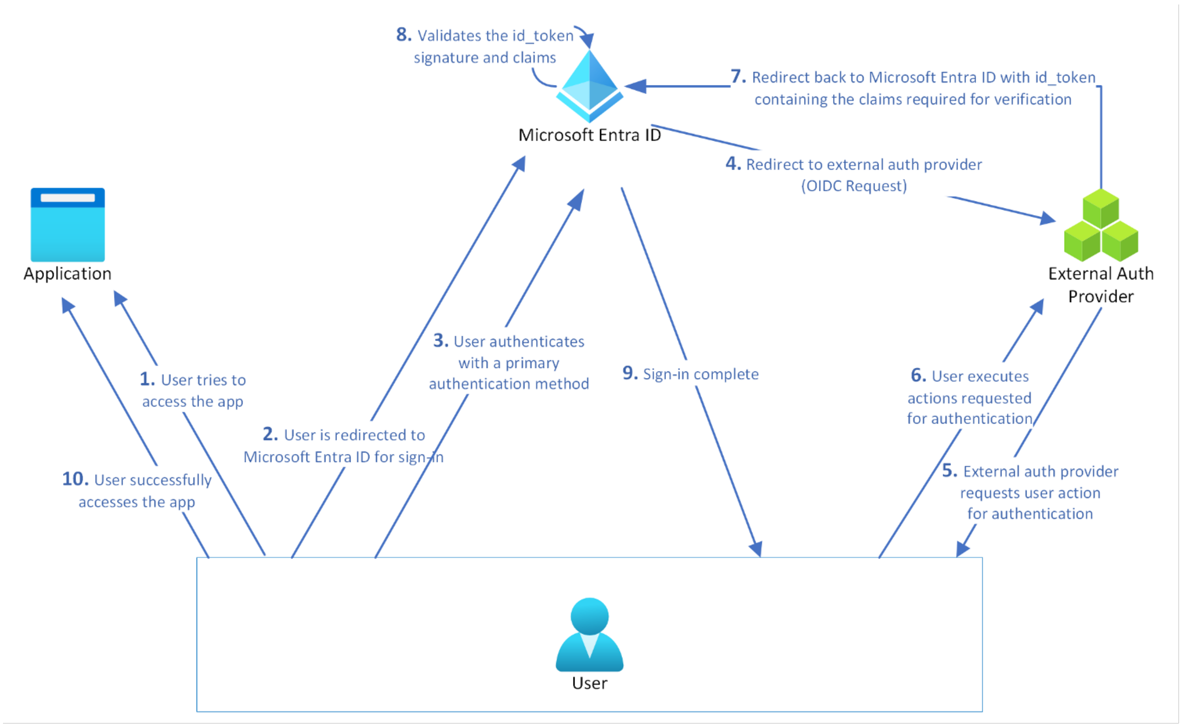
In 2020, Microsoft announced plans to replace custom controls with a new method for integrating third-party authentication. MobileID has been working closely with Microsoft to deliver an authentication solution for their new Microsoft **External Authentication Methods** (EAM) framework, available from May 2024.

MobileID via EAM is fully recognized as a multifactor authentication method within Entra ID, meeting MFA policy requirements. Once MobileID is defined as an EAM provider, you can create Entra ID conditional access policies with MFA using MobileID and assign these to specific users, groups, or applications.

For more information, check out the EAM public preview on the Microsoft blog.

Mobile ID for Entra ID External Authentication Methods is a Microsoft Early Access feature.

1.1 Sign-in Flow


8. Validates the id_token signature and claims
Microsoft Entra ID
7. Redirect back to Microsoft Entra ID with id_token containing the claims required for verification
4. Redirect to external auth provider (OIDC Request)
Application
External Auth Provider
1. User tries to access the app
2. User is redirected to Microsoft Entra ID for sign-in
3. User authenticates with a primary authentication method
9. Sign-in complete
6. User executes actions requested for authentication
5. External auth provider requests user action for authentication
10. User successfully accesses the app
User

1.2 Known Limitations

- Users must specifically select the MobileID EAM option during authentication. If they have other MFA methods configured besides MobileID, they may need to click "**Other options**" on the Microsoft "Verify your identity" prompt in order to choose MobileID.

  Microsoft plans to introduce system-preferred defaults for EAM in the future, which will automatically prioritize the default method displayed during authentication.
- EAM currently does not support logins for external guest users.
- Cross-tenant user authentication with the MobileID EAM has limitations. It will only work if:
  - The external Microsoft Entra organization trusts MFA claims from the user's home tenant.
  - The user has already established a valid MFA claim by authenticating to an application within their home tenant before accessing the cross-tenant application.
- Azure Government does not yet support Entra ID external authentication methods. Be sure to review Microsoft Entra feature availability for Azure Government. The "Microsoft Entra ID: External Authentication Methods" application is not accessible under MobileID Federal plans.

2 Getting Started

2.1 Prerequisites

To use MobileID MFA with Microsoft Entra ID, you'll need the following:

- Before you can integrate and use MobileID EAM, the client onboarding process must have been completed by Swisscom. You will need the following information from Swisscom to be able to create an EAM:

    - An **Application ID** is generally a multitenant application from your provider, which is used as part of the integration. You need to provide admin consent for this application in your tenant.

    - A **Client ID** is an identifier from your provider used as part of the authentication integration to identify Microsoft Entra ID requesting authentication.

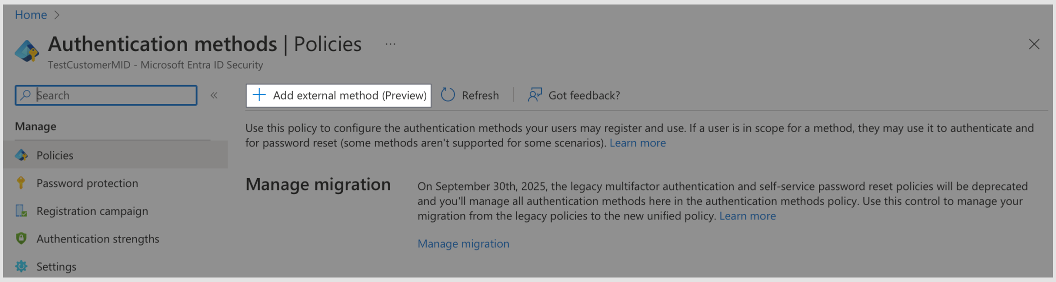
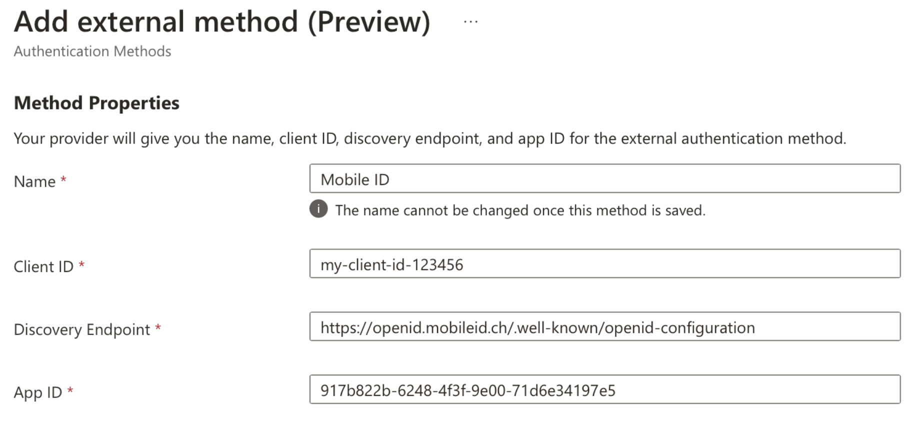
    - A **Discovery URL** is the OpenID Connect (OIDC) discovery endpoint for the external authentication provider.

  If you did not receive this information, it means that your onboarding process is not finished yet. Please check the state with your commercial contact or via Backoffice.Security@swisscom.com.

- An active Entra ID P1 or P2 subscription with Conditional Access enabled, and P1/P2 licenses assigned to each user who will log in using MobileID MFA. Plans like Microsoft 365 E3, E5, and F3, as well as Enterprise Mobility + Security E3 and E5, and Microsoft Business Premium, all include Entra ID Premium.

- A designated Entra ID admin service account to authorize the MobileID application access. This account requires the Entra ID Global Administrator or Privileged Role Administrator role during the MobileID setup process, though you can reduce the service account's role privileges afterward.

2.2 Configure Entra ID

STEP	DESCRIPTION
1	**LOG IN TO ENTRA ID** Go to the [Microsoft Entra admin center](https://entra.microsoft.com) and log in to your Entra ID tenant as a global administrator. If you're using the Azure portal (https://portal.azure.com), the navigation will differ slightly.
2	**NAVIGATE TO POLICIES** In the Entra Admin Center, go to **Protection** → **Authentication Methods** → **Policies**. If you're logged into the Azure portal instead, first select **Microsoft Entra ID**, then go to **Security** → **Authentication Methods** → **Policies**.
3	**ADD EXTERNAL METHOD** Click **+ Add External Method**.  Home > Authentication methods | Policies ... TestCustomerMID - Microsoft Entra ID Security Search + Add external method (Preview) Refresh Got feedback? Manage Policies Password protection Registration campaign Authentication strengths Settings Use this policy to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). Learn more Manage migration On September 30th, 2025, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy policies to the new unified policy. Learn more Manage migration
4	**CONFIGURE THE EXTERNAL METHOD** On the "Add external method" page, enter a **descriptive name** for the MobileID method. The default name might be "Mobile ID" but you can choose a name that will make sense to your users since they'll see this during authentication. Note: You cannot change the name after creation. Enter the information you have received from Swisscom in the corresponding field: • **Client ID** • **Discovery Endpoint** • **App ID**  Add external method (Preview) ... Authentication Methods Method Properties Your provider will give you the name, client ID, discovery endpoint, and app ID for the external authentication method. Name * : Mobile ID The name cannot be changed once this method is saved. Client ID * : my-client-id-123456 Discovery Endpoint * : https://openid.mobileid.ch/.well-known/openid-configuration App ID * : 917b822b-6248-4f3f-9e00-71d6e34197e5
5	**ENABLE THE METHOD** If you want to enable MobileID MFA right away, toggle **Enable** from "Off" to "On".

6 SPECIFY USERS

Before saving the new MobileID external method, decide which users should have access to it.

By default, it will apply to all users, meaning any Entra ID user with a Conditional Access Policy requiring multifactor authentication (MFA) will see MobileID as an option.

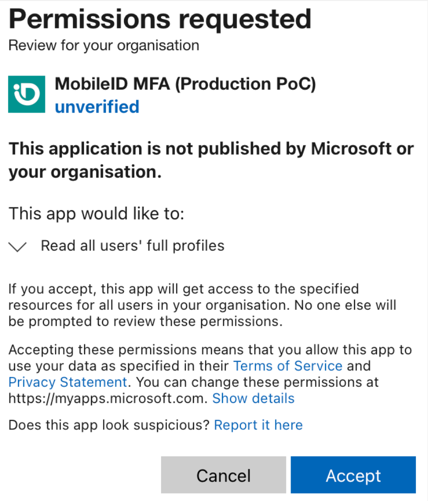
To apply it to specific users, click **+ Add Target** under the "Include" tab and choose **Select Targets**. On the "Add directory members" page, select one or more Entra ID directory groups that contain the users you want to target for MobileID authentication, then click **Select**.

7 SAVE THE CONFIGURATION

After entering all the required details, click **Save** to create the new MobileID external method.

8 GRANT ADMIN CONSENT

If the "Request admin consent" information shows a **Request permission** button instead of saying "Admin consent granted", click the **Request permission** button to authorize the grant the MobileID Authentication Method application, making sure to check the box next to **Consent on behalf of your organization** before clicking **Accept**.



Permissions requested

Review for your organisation

MobileID MFA (Production PoC)
unverified

This application is not published by Microsoft or your organisation.

This app would like to:

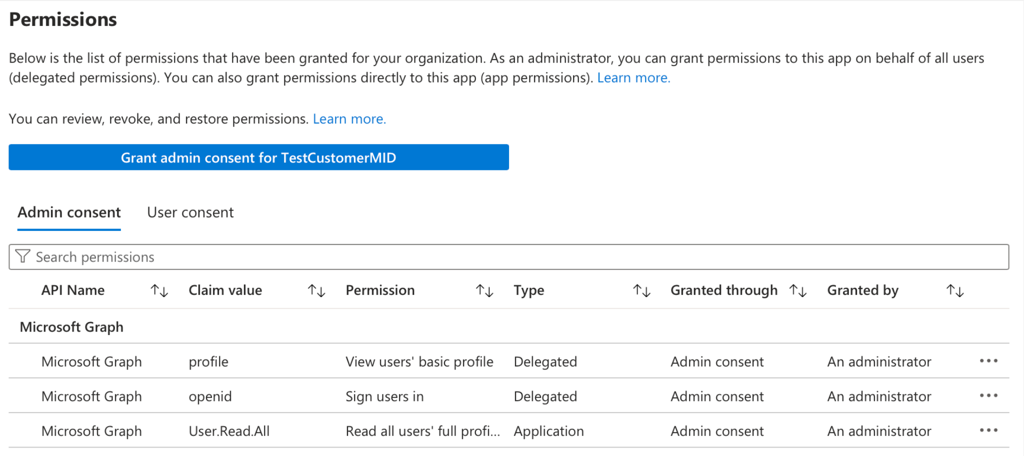
Read all users' full profiles

If you accept, this app will get access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

You can verify the permissions if you go to **Identity → Applications → Enterprise applications** and select the MobileID Application, then select **Permissions**. The list of permissions that have been granted for your organization should shown and it should look similar to this example below:



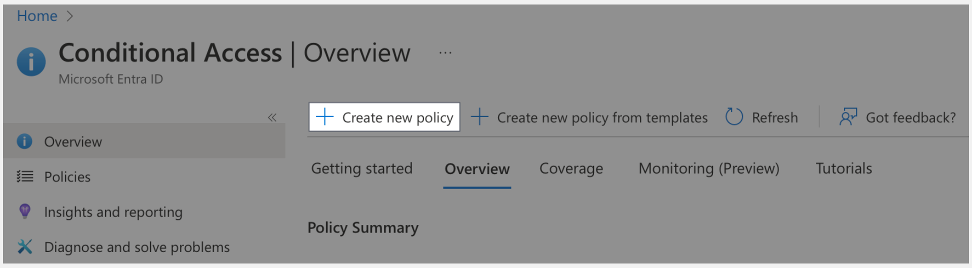
Permissions

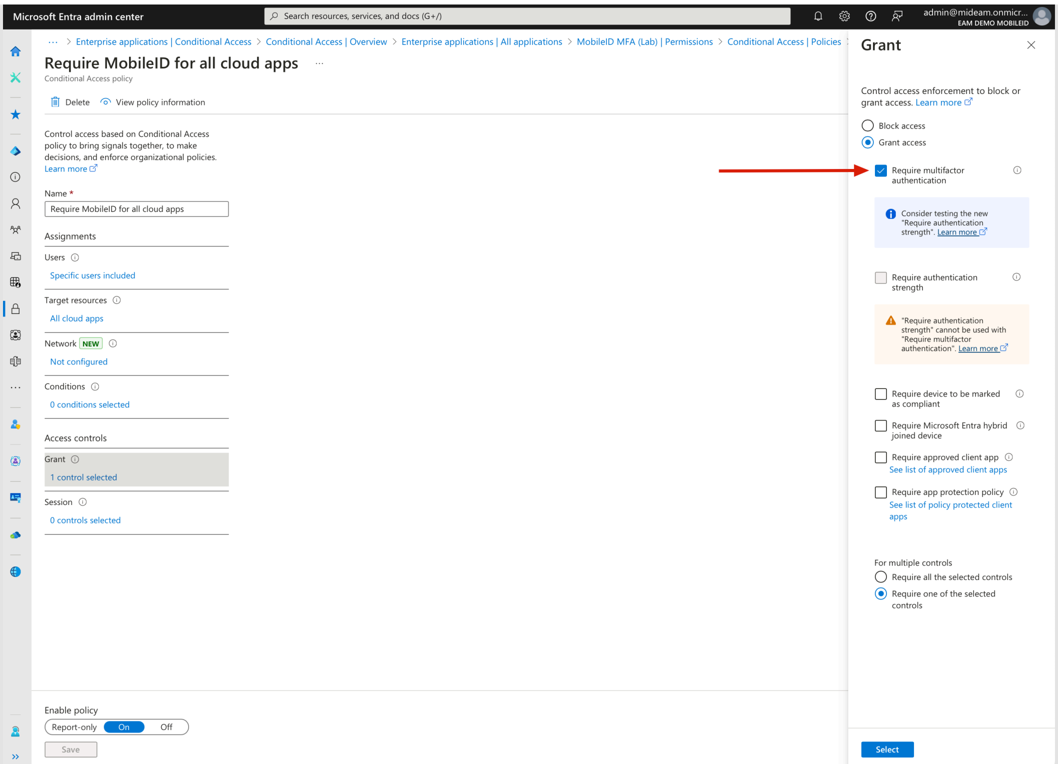
Below is the list of permissions that have been granted for your organization. As an administrator, you can grant permissions to this app on behalf of all users (delegated permissions). You can also grant permissions directly to this app (app permissions). Learn more.

You can review, revoke, and restore permissions. Learn more.

API Name	Claim value	Permission	Type	Granted through	Granted by
Microsoft Graph					
Microsoft Graph	profile	View users' basic profile	Delegated	Admin consent	An administrator
Microsoft Graph	openid	Sign users in	Delegated	Admin consent	An administrator
Microsoft Graph	User.Read.All	Read all users' full profi...	Application	Admin consent	An administrator

2.2.1 Create and Apply a Conditional Access Policy

Step	Description
1	**LOG IN TO ENTRA ID** Go to the [Microsoft Entra admin center]() and log in to your Entra ID tenant as a global administrator. If you're using the Azure portal ([https://portal.azure.com]()), the navigation will differ slightly.
2	**NAVIGATE TO CONDITIONAL ACCESS** click on **Conditional Access** in the left-hand menu, then click **+ Create New Policy**. If you are in the Azure portal, navigate to **Security** → **Conditional Access** → **Policies**.  Home > Conditional Access | Overview Microsoft Entra ID Create new policy Create new policy from templates Refresh Got feedback? Overview Policies Insights and reporting Diagnose and solve problems Getting started Overview Coverage Monitoring (Preview) Tutorials Policy Summary
3	**NAME THE POLICY** Enter a descriptive name for the new policy, such as **"MobileID MFA for Acme Users"**.
4	**ASSIGN THE POLICY** You can assign this policy to specific users or groups, Entra ID cloud apps, or other conditions like client platforms or networks. **Example for assigning to users**: Click **Users** under "Assignments", then select **Users and groups** on the "Include" tab. Choose **Users and groups** and click **0 users and groups selected** to locate the users or Entra ID security groups for whom you want to enforce MobileID MFA. Select the users or groups, then click **Select** to apply your choices. • If you targeted specific groups when creating the MobileID external method, ensure that you apply this new policy to the same groups. • Example: The new MobileID policy assignment could include the Entra ID group **"MobileID Acme EAM"**, so members of that group will see MobileID as an authentication method when logging in. **Example for assigning to resources**: Click **Target resources**. On the "Include" tab, select **Apps**, and choose the Entra ID applications where you want MobileID MFA to be applied. • Example: The MobileID policy could target "Office 365" as the cloud app, meaning only logins to Office 365 will require MobileID MFA. **Important**: Avoid assigning the MobileID policy to all users or all cloud apps at the start, especially for tenant administrators, to prevent potential admin lockouts. Always test the policy with selected users first. Additionally, ensure you create a fail-safe Entra ID administrator account that is excluded from MobileID MFA policies to maintain uninterrupted access. Secure this account with a strong password and a different access condition, such as one based on a trusted network.
5	**CONFIGURE ACCESS CONTROLS** Click **Grant** under "Access controls", select **Grant access**, and check the box for **Require multi-factor authentication**. Click **Select** when done.



Microsoft Entra admin center

Search resources, services, and docs (G+/)

admin@mideam.onmicr...
EAM DEMO MOBILEID

... > Enterprise applications | Conditional Access > Conditional Access | Overview > Enterprise applications | All applications > MobileID MFA (Lab) | Permissions > Conditional Access | Policies

Require MobileID for all cloud apps ...

Conditional Access policy

Delete View policy information

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

Name *

Require MobileID for all cloud apps

Assignments

Users
Specific users included

Target resources
All cloud apps

Network NEW
Not configured

Conditions
0 conditions selected

Access controls

Grant
1 control selected

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

Consider testing the new "Require authentication strength". Learn more

□ Require authentication strength

"Require authentication strength" cannot be used with "Require multifactor authentication". Learn more

□ Require device to be marked as compliant

□ Require Microsoft Entra hybrid joined device

□ Require approved client app
See list of approved client apps

□ Require app protection policy
See list of policy protected client apps

For multiple controls
○ Require all the selected controls
● Require one of the selected controls

Select

6 ENABLE THE POLICY

The final step is to enable the new MobileID conditional access policy. Click the “**On**” toggle switch under "Enable policy", then click **Create**. The policy will be created and applied to your selected groups or users, enforcing MFA via MobileID.

Additional Configuration to Prioritize MobileID MFA

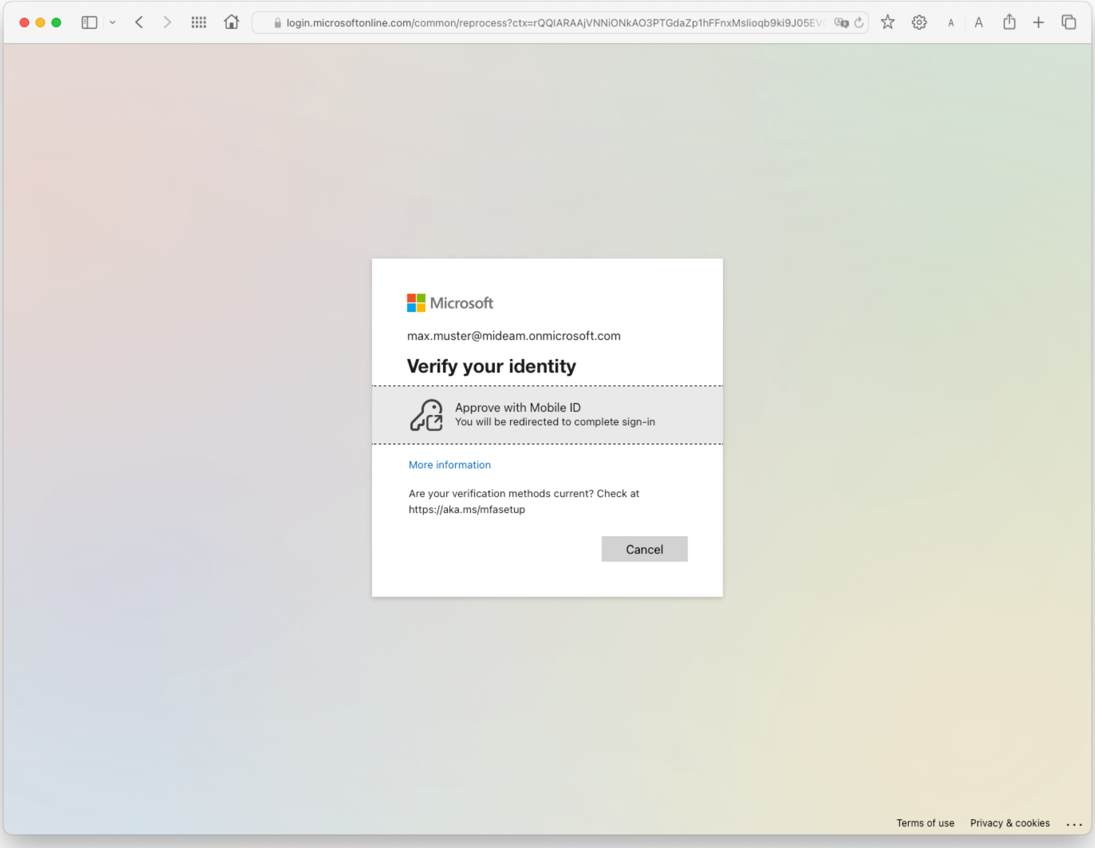
If you want users to exclusively use MobileID instead of the Microsoft Authenticator app, follow these steps:

Step	Description
1	**DISABLE THE MICROSOFT AUTHENTICATOR REGISTRATION CAMPAIGN** In the Entra ID admin center, go to **Protection** → **Authentication Methods** → **Registration Campaign**. • Click **Edit**, change the **State** to **Disabled**, and click **Save**. • Alternatively, you can leave the registration campaign enabled and exclude the groups of users who are covered by the MobileID conditional access policy.
2	**DISABLE SYSTEM PREFERRED MFA FOR MICROSOFT AUTHENTICATOR** Go to **Protection** → **Authentication Methods** → **Settings** → **System Preferred Multifactor Authentication**. • Click **Edit**, change the **State** to **Disabled**, and click **Save**.
3	**TURN OFF MICROSOFT AUTHENTICATOR** Navigate to **Protection** → **Policies**, click **Microsoft Authenticator**. • On the “Enable and Target” tab, toggle the **Enable** switch to **Off** and click **Save**.

2.2.2 Test Your Setup

Log in to Entra ID using a user account that has been assigned the Conditional Access policy requiring MFA and is a target for the newly created MobileID external method.

If you applied the MobileID Conditional Access policy to "All cloud apps", when you log into the Office portal (e.g., https://office.com) and submit your primary Entra ID credentials, you'll see your MobileID external authentication method as an option for identity verification. The name displayed will be the one you entered when setting up the MobileID external method in Entra ID.



login.microsoftonline.com/common/reprocess?ctx=rQQIARAAjVNNiONkAO3PTGdaZp1hFFnxMslioqb9ki9J05EV

Microsoft

max.muster@mideam.onmicrosoft.com

Verify your identity

Approve with Mobile ID
You will be redirected to complete sign-in

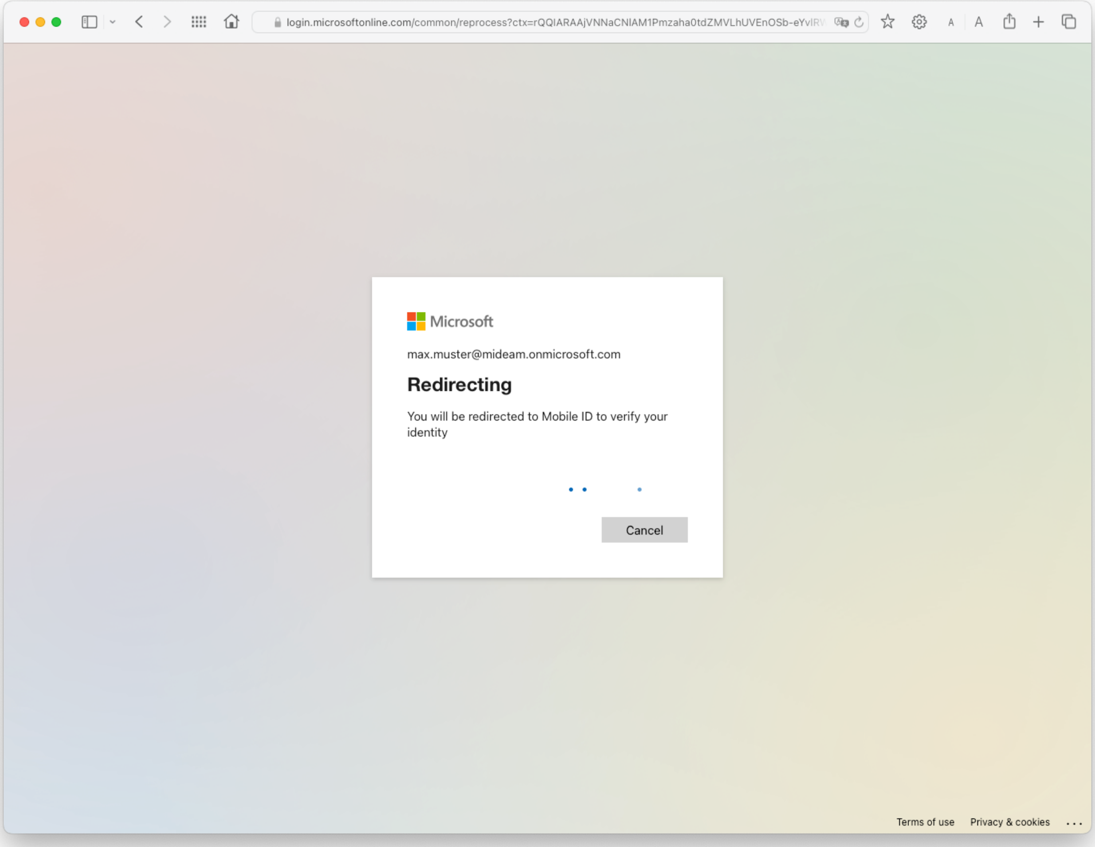
More information

Are your verification methods current? Check at https://aka.ms/mfasetup

Cancel

Choose the “Mobile ID” method to begin MobileID MFA authentication.

If you have multiple Entra ID authentication methods enabled, you may need to click “**Other options**” to view and select the MobileID method.


login.microsoftonline.com/common/reprocess?ctx=rQQIARAAjVNNaCNlAM1Pmzaha0tdZMVLhUVEnOSb-eYvlRV
Terms of use
Privacy & cookies
...

Microsoft

max.muster@mideam.onmicrosoft.com

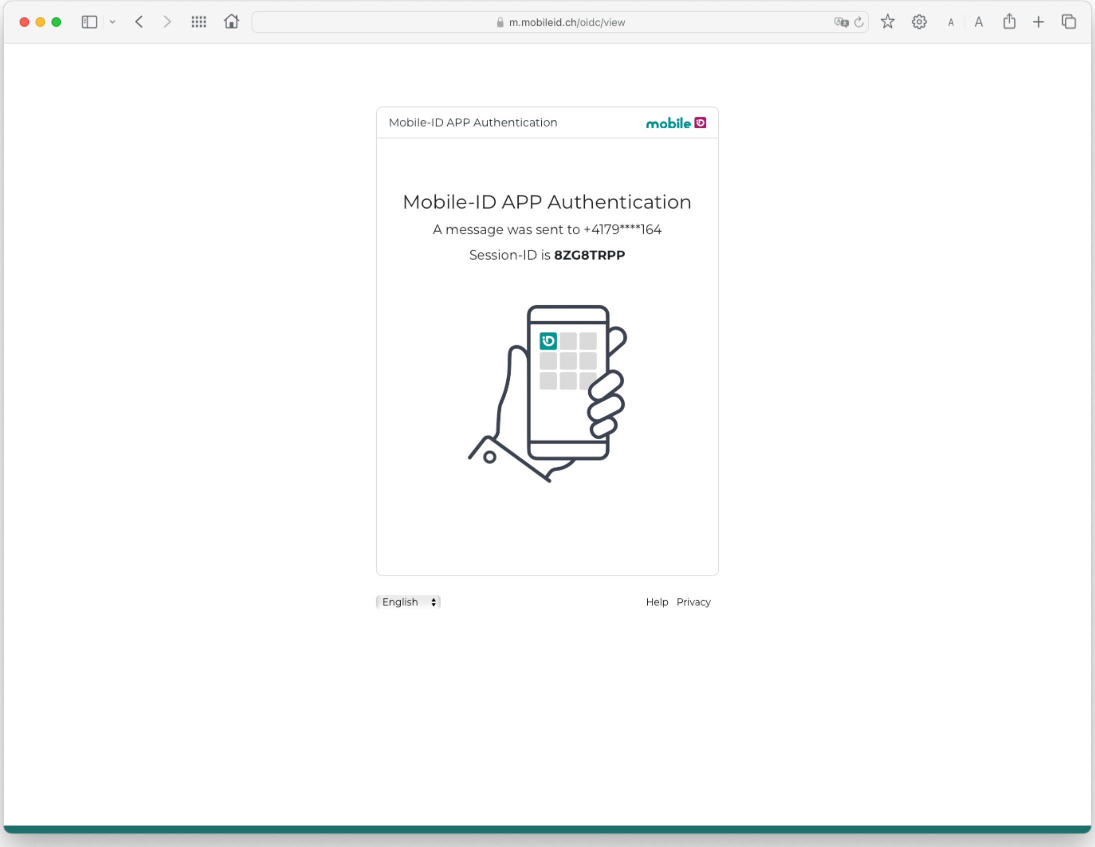
Redirecting

You will be redirected to Mobile ID to verify your identity

Cancel

You will be redirected to the MobileID prompt or user enrolment, depending on your configuration.

Once you complete the MobileID authentication, you'll return to Entra ID to finish logging in to the application.



Mobile-ID APP Authentication

Mobile-ID APP Authentication

A message was sent to +4179****164

Session-ID is **8ZG8TRPP**

If your Conditional Access policy requiring MFA is only applied to specific applications, the initial login to the Office portal will not prompt for MobileID MFA. However, accessing the protected application within the Office portal or directly will trigger the MobileID MFA prompt.

If you encounter the "*Looks like something went wrong*" error from Microsoft, the new EAM settings might need additional time to propagate. If the error persists, you may request support from Swisscom.

3 Troubleshooting

Need some help? Please ask your commercial contact or get in touch with Backoffice.Security@swisscom.com to ask for support.