وزارة التعليم
Ministry of Education

وزارة التعليم – مشروع الدخول الموحد
Ministry of Education – SSO Project

دليل المستخدم
End-User Guide

August 2024

Table Of Content الفهرس

1 دليل خطوات تسجيل الدخول عبر نظام– SSO باللغة العربية

1.1 *حسابات جديدة - تسجيل الدخول لأول مرة*

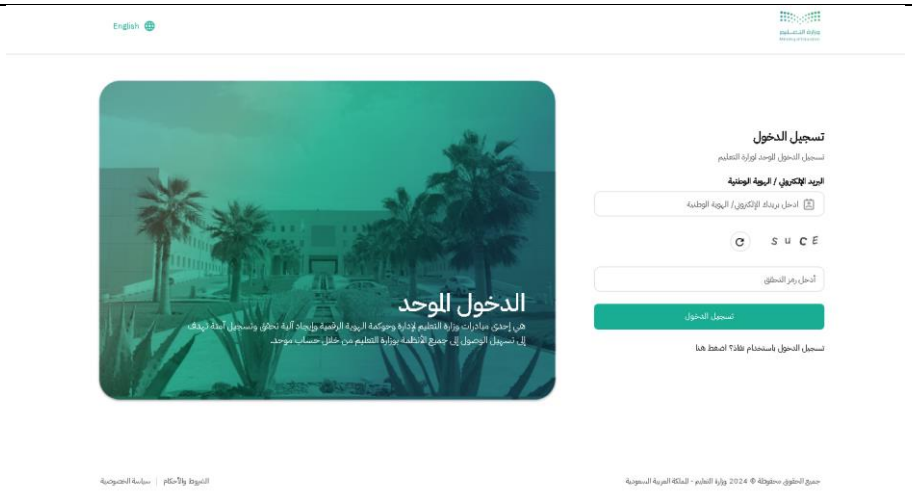
الوصف:	يصف هذا السيناريو الخطوات التي يجب أن يتبعها المستخدم للدخول عبر منصة SSO بعد أن يتم إنشاؤه كمستخدم جديد ويتلقى رسالة نصية SMS تحتوي على تفاصيل الحساب
أنواع المستخدمين / الشخصيات:	- موظفو وزارة التعليم - المديرون في التعليم / الكادر الفني - الموظفون الإداريون / الأكاديميون في التعليم - الطلاب الذين يمتلكون حسابًا علىAzure AD
الشروط:	- المستخدم لديه البريد الإلكتروني الجديد الذي تم إنشاؤه من خلال الرسالة النصية أو مكتب الخدمة. - تسجيل الدخول لأول مرة باستخدام هذا الحساب . - لم يتم تعيين كلمة مرور للمستخدم الذي تم إنشاؤه بعد .

الخطوات التفصيلية :

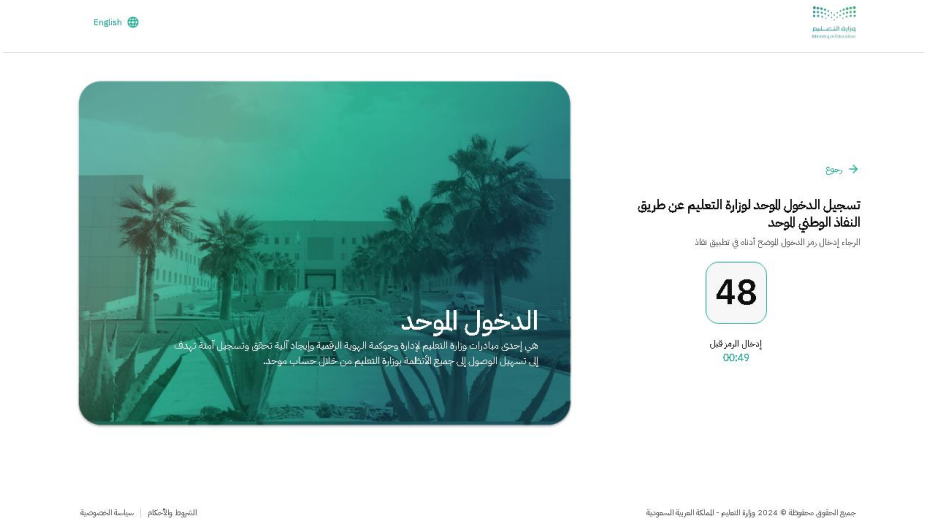
الخطوات التي سيتبعها المستخدم الذي تم إنشاؤه حديثاً من قبل نظام IAM :

1. يتلقى المستخدم الرسالة النصية الموضحة أدناه من نظام IAM الذي يؤكد إنشاء المستخدم.

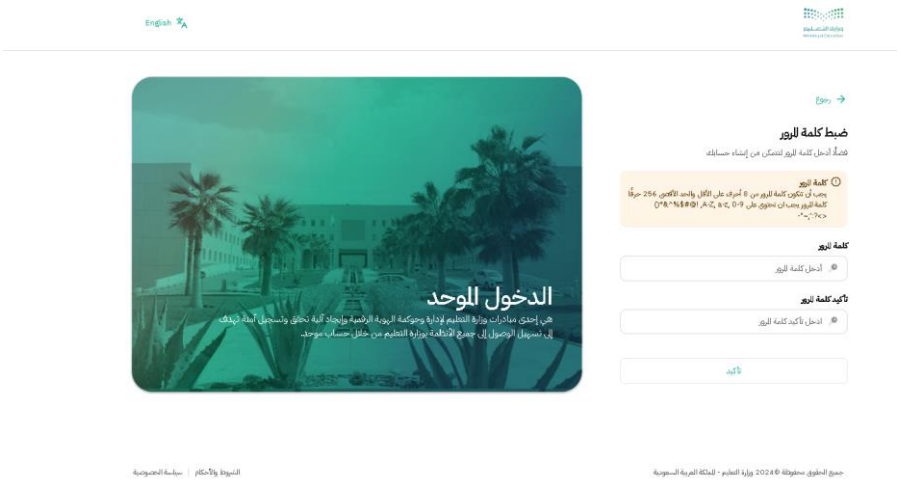
2. يقوم المستخدم بإدخال الرابط الخاص بالتطبيق الذي يرغب في الدخول عليه (مثال: فارس، نور ، خدماتي) واختيار خيار الدخول عن طريق نظام الدخول الموحد SSO .
3. يتم تحويل الصفحة للصفحة الرئيسية لنظام الدخول الموحد الخاص بالوزارة.
4. يقوم المستخدم بإدخال البريد الإلكتروني وكلمه التحقق.



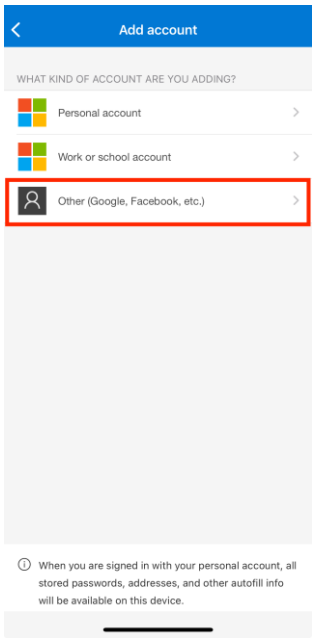
5. يتم إعادة التوجيه للصفحة الخاصة بنظام نفاذ لتأكيد الهوية .



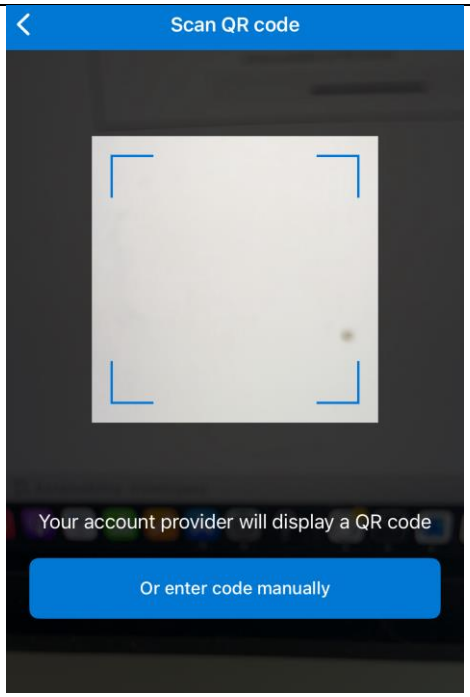
6. بعد التحقق من الهوية بنجاح يتم إعادة التوجيه لصفحة ضبط كلمة المرور حيث يقوم المستخدم بإدخال، ضبط كلمة المرور الجديدة .

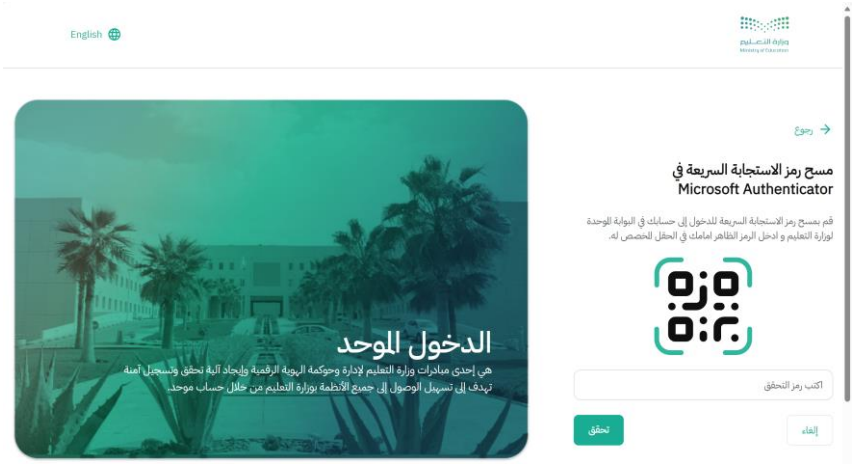


7. بعد التحقق من الهوية بنجاح يتم إعادة التوجيه للصفحة الخاصة ببرنامج التوثيق حيث تطلب هذه الخطوة تنزيل برنامج التوثيق "Microsoft Authenticator" من خلال Apple Store أو Android Google Play.
8. في الشاشة الأولى للبرنامج، يقوم المستخدم بالضغط على علامة الإضافة "+" واختيار الخيار الأخير "Other (Google, Facebook, etc,)"

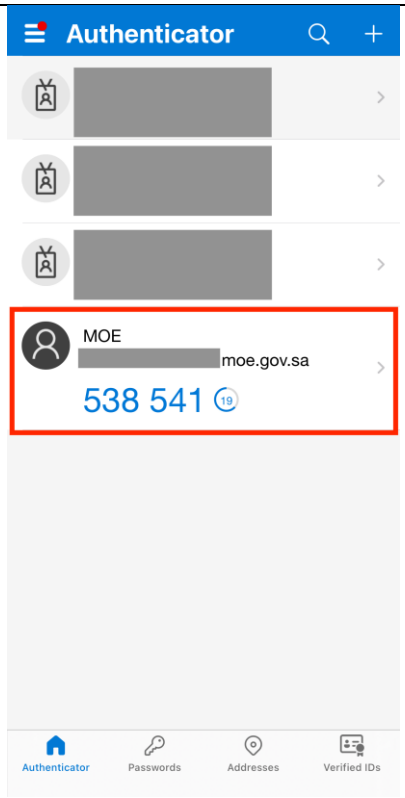


9. يقوم المستخدم بالموافقة على استخدام الكاميرا ومسح رمز الاستجابة السريع من الشاشة الخاصة بنظام الدخول الموحد.





10. بمجرد مسح رمز الاستجابة السريع، يظهر على التطبيق الكود الخاص بالدخول والمكون من ٦ أرقام .



11. بعد إدخال الكود يتم التوجيه لصفحة الشروط والأحكام .

12. يتم توجيه المستخدم لصفحة التطبيق المطلوب .

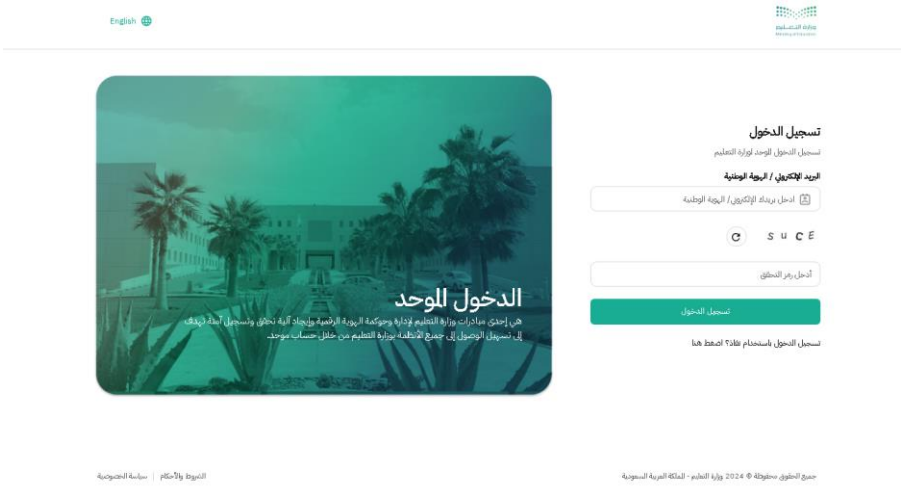
1.2 *المستخدم الحالي - تسجيل الدخول لأول مرة*

الوصف :	يصف هذا السيناريو الخطوات التي ينبغي أن يتخذها المستخدم للدخول من خلال منصة SSO لاول مره باستخدام الحساب الموجود بالفعل علي انظمه الوزارة (AD/Azure) .
أنواع المستخدمين / الشخصيات:	- موظفو وزارة التعليم - المديرون في التعليم / الكادر الفني - الموظفون الإداريون / الأكاديميون في التعليم

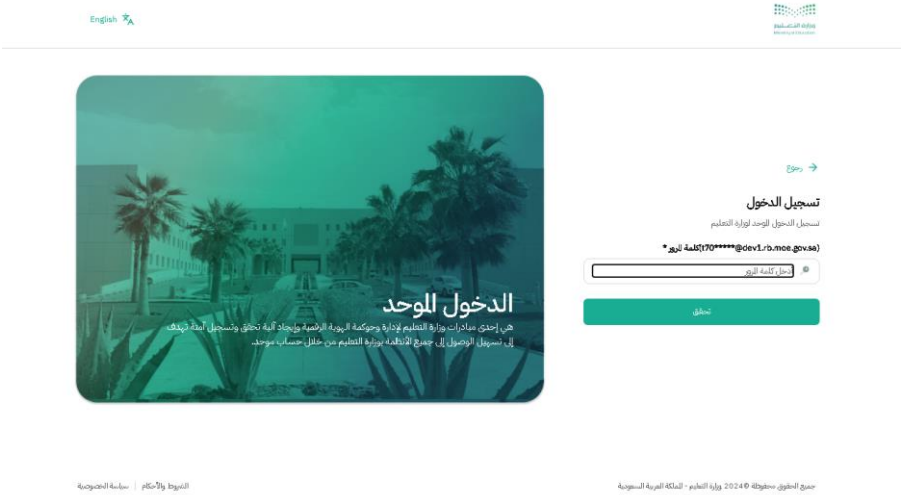
	- الطلاب الذين يمتلكون حسابًا علىAzure AD
الشروط :	- المستخدم لديه حساب موجود بالفعل في قواعد بيانات الوزارة وله حساب نشط. - يمتلك المستخدم اسم المستخدم وكلمة المرور الخاصة به.

الخطوات التفصيلية:

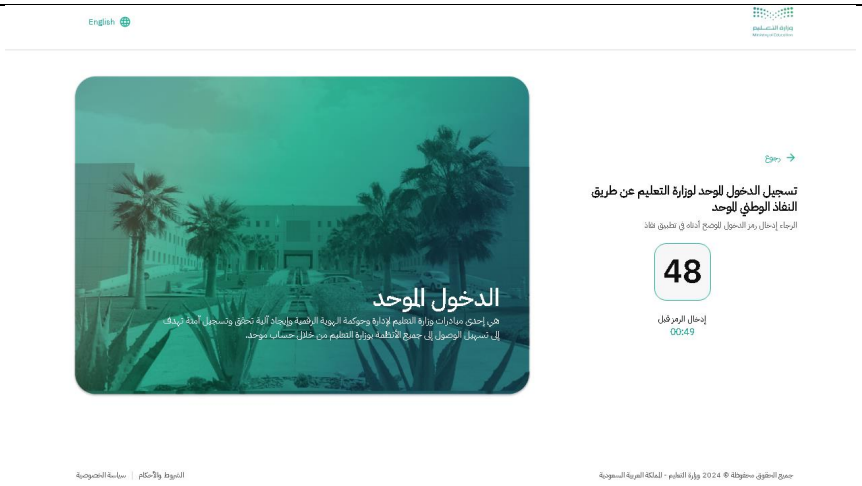
1. يقوم المستخدم بإدخال الرابط الخاص بالتطبيق الذي يرغب في الدخول عليه (مثال: فارس، نور، خدماتي) واختيار خيار الدخول عن طريق نظام الدخول الموحد SSO .
2. يقوم المستخدم بإدخال اسم المستخدم (AD/Azure email) أو رقم الهوية / الإقامة المسجلة بالنظام وكذلك رمز التحقق والضغط على التالي.



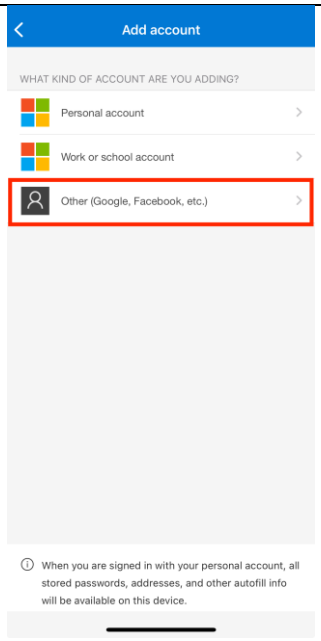
3. يقوم المستخدم بإدخال كلمة المرور الخاصة ب (AD/Azure AD Password)، ثم الضغط على login.



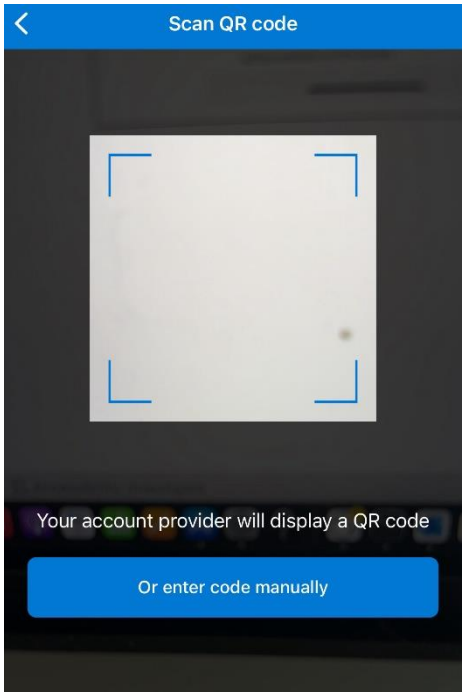
4. بعد التحقق من اسم المستخدم وكلمه المرور يتم إعادة التوجيه للصفحة الخاصة بنظام نفاذ لتأكيد الهوية.

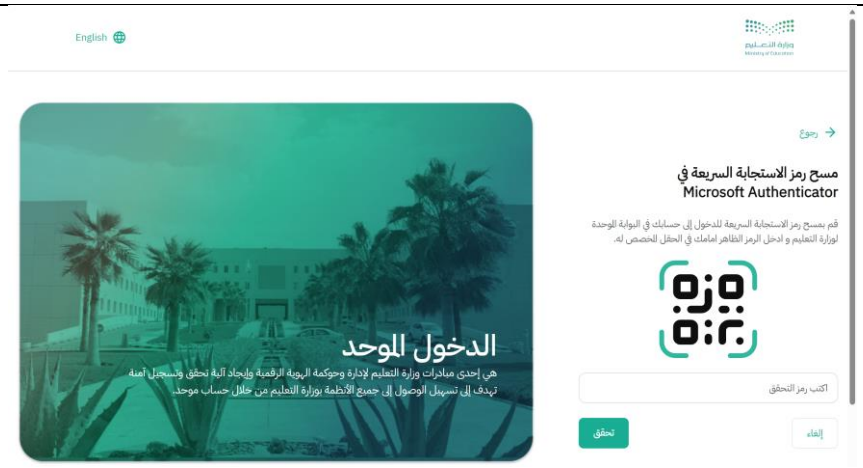


5. بعد التحقق من الهوية بنجاح يتم إعادة التوجيه للصفحة الخاصة ببرنامج التوثيق حيث تطلب هذه الخطوة تنزيل برنامج التوثيق "Microsoft Authenticator" من خلال Apple Store أو Android Google Play .
6. في الشاشة الأولى للبرنامج، يقوم المستخدم بالضغط على علامة الإضافة "+" واختيار الخيار الاخير "Other" (Google, Facebook, etc,)

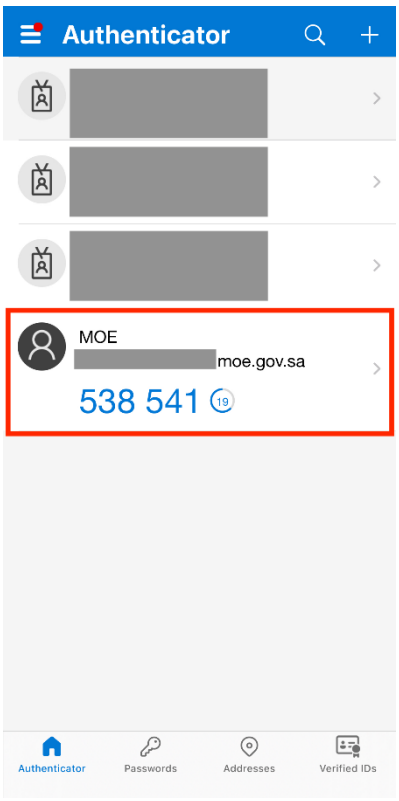


7. يقوم المستخدم بالموافقة على استخدام الكاميرا ومسح رمز الاستجابة السريع من الشاشة الخاصة بنظام الدخول الموحد.





8. بمجرد مسح رمز الاستجابة السريع، يظهر علي التطبيق الكود الخاص بالدخول والمكون من ٦ أرقام .



9. بعد إدخال الكود يتم التوجيه لصفحة الشروط والأحكام.

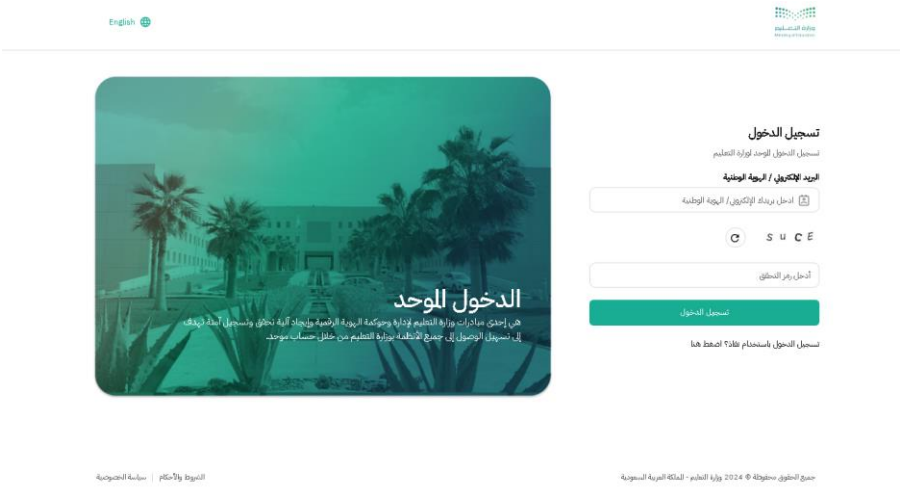
10. يتم توجيه المستخدم لصفحة التطبيق المطلوب .

1.3 *المستخدم الحالي - تسجيل الدخول العادي/المنتظم*

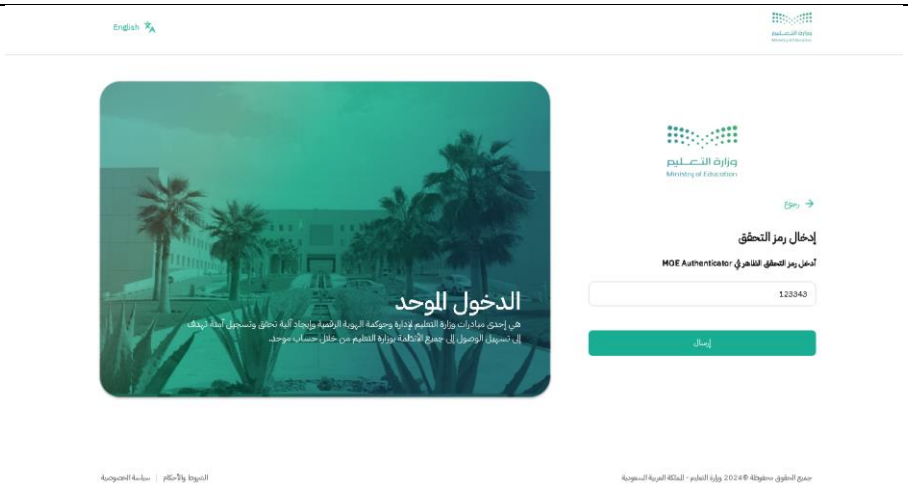
الوصف :	يصف هذا السيناريو الخطوات التي ينبغي أن يتخذها المستخدم للدخول من خلال منصة SSO كل مره يقوم باستخدام النظام فيها بعد التسجيل لأول مره.
أنواع المستخدمين / الشخصيات:	- موظفو وزارة التعليم - المديرون في التعليم / الكادر الفني - الموظفون الإداريون / الأكاديميون في التعليم - الطلاب الذين يمتلكون حسابًا علىAzure AD
الشروط :	- المستخدم لديه حساب نشط ومُسجل في قواعد بيانات الوزارة. - المستخدم لديه اسم المستخدم وكلمة المرور الخاصة به.

الخطوات التفصيلية :

1. يقوم المستخدم بإدخال الرابط الخاص بالتطبيق الذي يرغب في الدخول عليه (مثال: فارس، نور، خدماتي) واختيار خيار الدخول عن طريق نظام الدخول الموحد SSO.
2. يقوم المستخدم بإدخال اسم المستخدم (AD/Azure email) أو رقم الهوية / الإقامة المسجلة بالنظام وكذلك رمز التحقق والضغط على التالي.

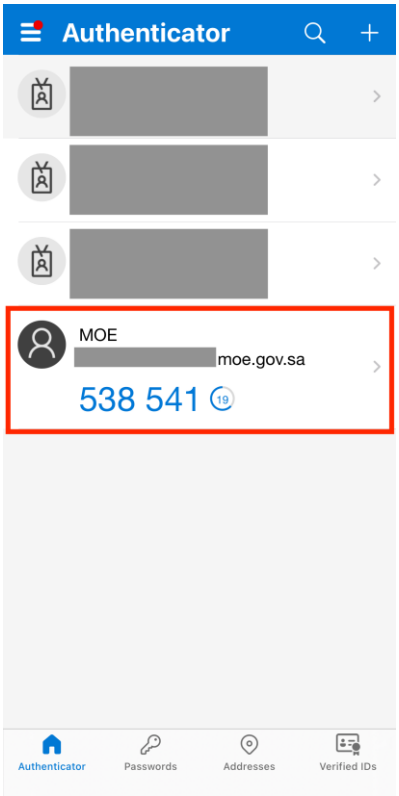


3. يقوم المستخدم بإدخال كلمة المرور الخاصة ب (AD/Azure AD Password)، الضغط على login.
4. بعد التحقق من اسم المستخدم وكلمة المرور بنجاح يتم إعادة التوجيه للصفحة الخاصة ببرنامج التوثيق.



5. قم بفتح برنامج التوثيق "Microsoft Authenticator"

6. سيظهر كود التوثيق المكون من ٦ أرقام والذي يتغير كل ٣٠ ثانية .



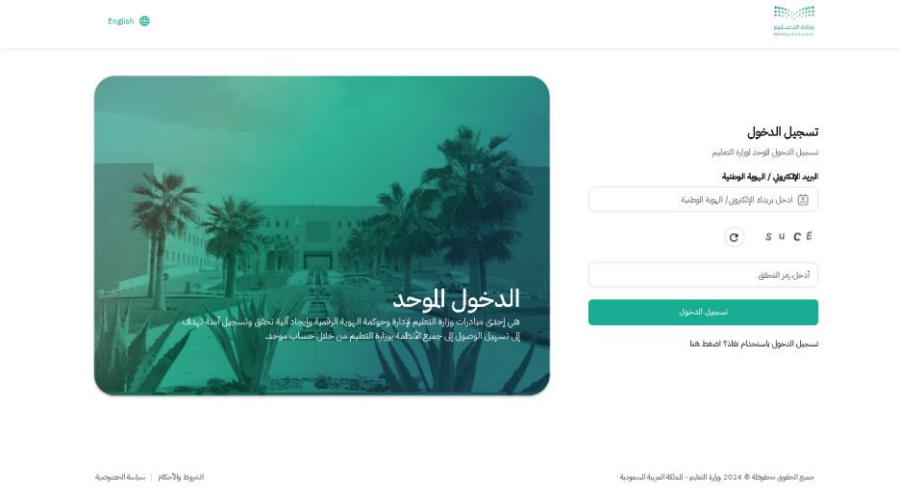
7. بمجرد ادخال الكود والضغط على إرسال سيتم تحويل الصفحة للتطبيق المطلوب .

1.4 اعاده تعريف الجهاز المستخدم لكود الحمايه – في حاله فقد / سرقه / تلف الجهاز القديم

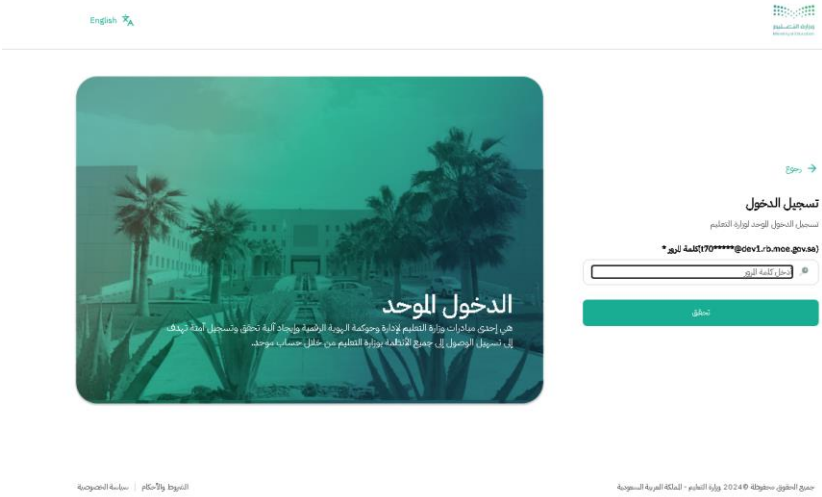
الوصف:	يصف هذا السيناريو الخطوات التي يجب أن يتبعها المستخدم في حالة فقد او تلف جهاز الموبايل المستخدم لتعريف الكود الشخصي للدخول علي ال SSO
أنواع المستخدمين / الشخصيات:	- موظفو وزارة التعليم - المديرون في التعليم / الكادر الفني - الموظفون الإداريون / الأكاديميون في التعليم - الطلاب الذين يمتلكون حسابًا علىAzure AD
الشروط:	- المستخدم لديه حساب نشط ومُسجل في قواعد بيانات الوزارة. - المستخدم لديه اسم المستخدم وكلمة المرور الخاصة به .لم يتم تعيين كلمة مرور للمستخدم الذي تم إنشاؤه بعد. - المستخدم قام بتسجيل جهاز موبايل سابق بتطبيق الموثق "Microsoft Authenticator"

الخطوات التفصيلية:

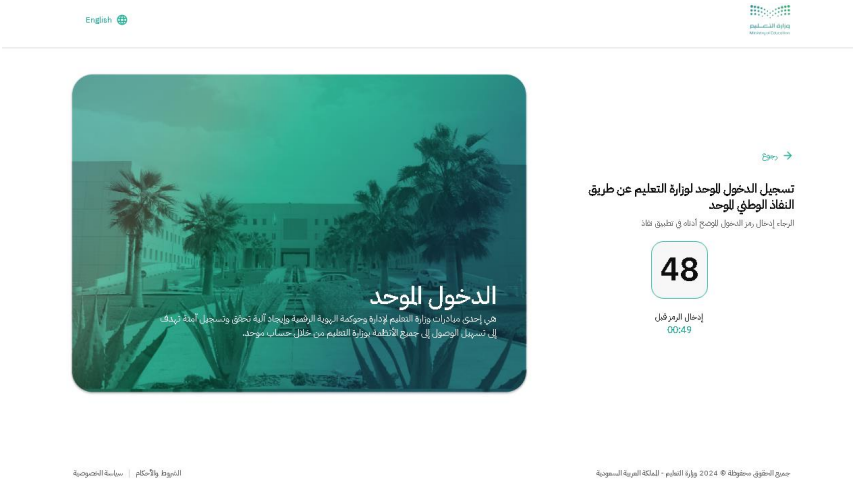
1. يقوم المستخدم بالاتصال بفريق الدعم الفني "Help Desk" (راجع الرقم 3)
2. يقوم فريق الدعم الفني بجمع البيانات الخاصه بالمستخدم والتأكد من صلاحيه المستخدم
3. بعد التأكد من صلاحيه البيانات، يقوم الفريق بحذف الاجهزه المعرفهالمرتبطه بالمستخدم من تطبيق ال "Microsoft Authenticator" ويصبح الكود السابق غير صالح للعمل.
4. يقوم المستخدم بإدخال الرابط الخاص بالتطبيق الذي يرغب في الدخول عليه (مثال: فارس، نور، خدماتي) واختيار خيار الدخول عن طريق نظام الدخول الموحد SSO .
5. يقوم المستخدم بإدخال اسم المستخدم (AD/Azure email) أو رقم الهوية / الإقامة المسجلة بالنظام وكذلك رمز التحقق والضغط على التالي.



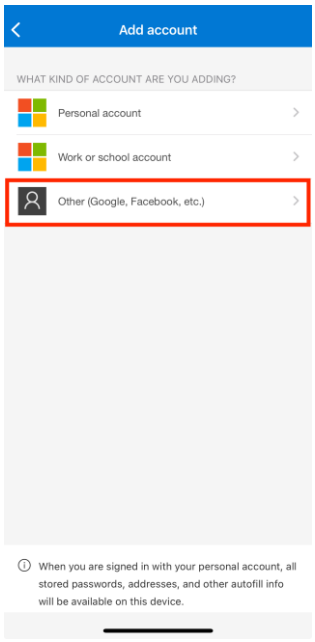
6. يقوم المستخدم بإدخال كلمة المرور الخاصة ب (AD/Azure AD Password)، ثم الضغط على login.



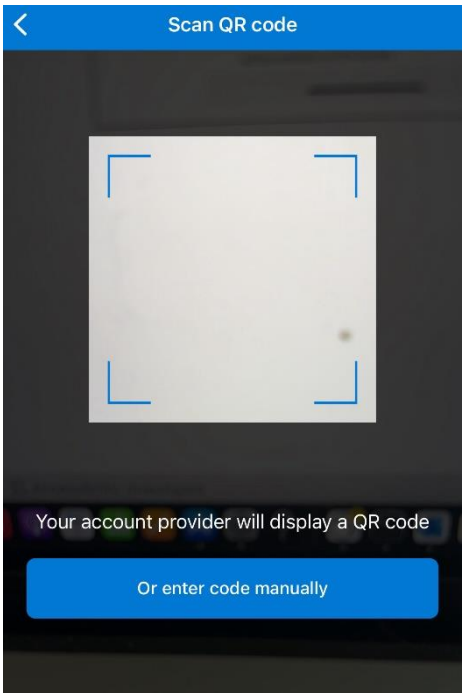
7. بعد التحقق من اسم المستخدم وكلمه المرور يتم إعادة التوجيه للصفحة الخاصة بنظام نفاذ لتأكيد الهوية.

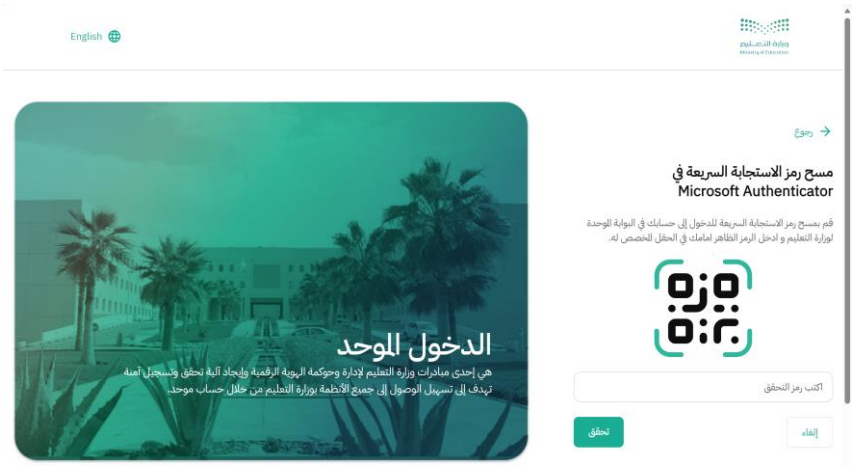


8. بعد التحقق من الهوية بنجاح يتم إعادة التوجيه للصفحة الخاصة ببرنامج التوثيق حيث تطلب هذه الخطوة تنزيل برنامج التوثيق "Microsoft Authenticator" من خلال Apple Store أو Android Google Play .
9. في الشاشة الأولى للبرنامج، يقوم المستخدم بالضغط على علامة الإضافة "+" واختيار الخيار الاخير "Other" (Google, Facebook, etc,)

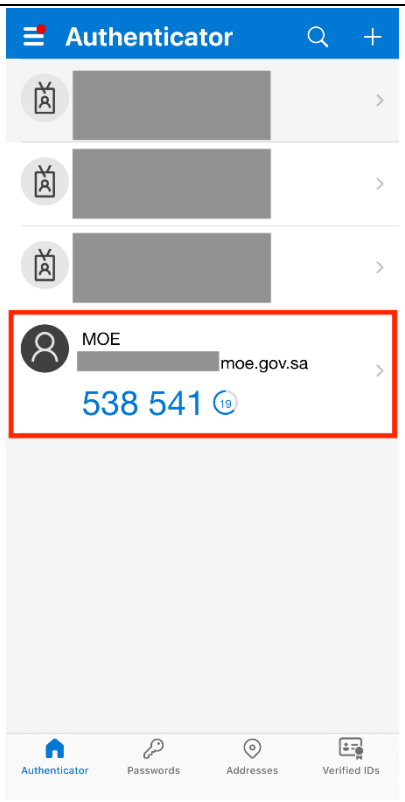


10. يقوم المستخدم بالموافقة على استخدام الكاميرا ومسح رمز الاستجابة السريع من الشاشة الخاصة بنظام الدخول الموحد.





11. بمجرد مسح رمز الاستجابة السريع، يظهر علي التطبيق الكود الخاص بالدخول والمكون من ٦ أرقام .



12. بعد إدخال الكود يتم التوجيه لصفحة الشروط والأحكام.

13. يتم توجيه المستخدم لصفحة التطبيق المطلوب .

MOE SSO LOGIN STEPS – ENGLISH GUIDE 2

2.1 Newly Created Accounts - First Time Login

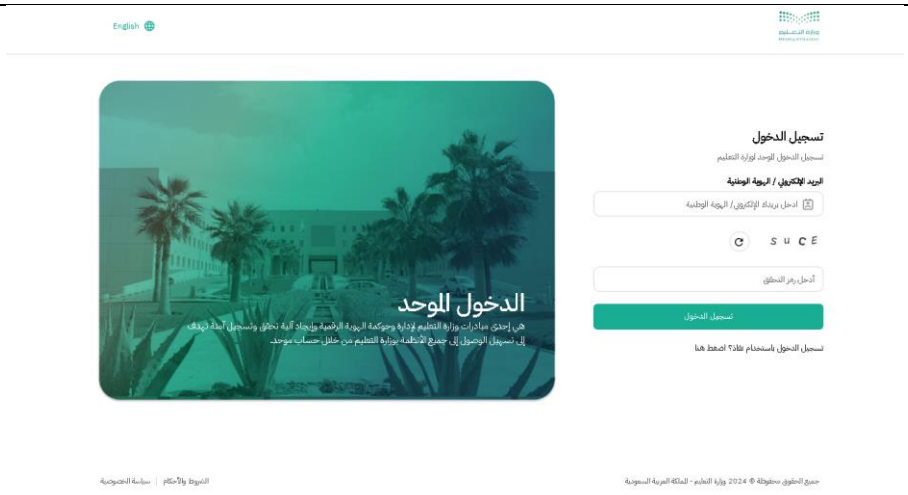
Description:	This scenario describes the steps for a user to login through the SSO platform after being created as a new user and receive SMS with the account details.
User's Types / Personas:	- MOE Staff - Education Staff Technical / Principals - Education Staff Admin / Staff - students with Azure AD account
Conditions:	- User knows his newly created email account through SMS or service desk. - User is first time to login using this account - No password has been set for the created user yet.

Detailed Steps:

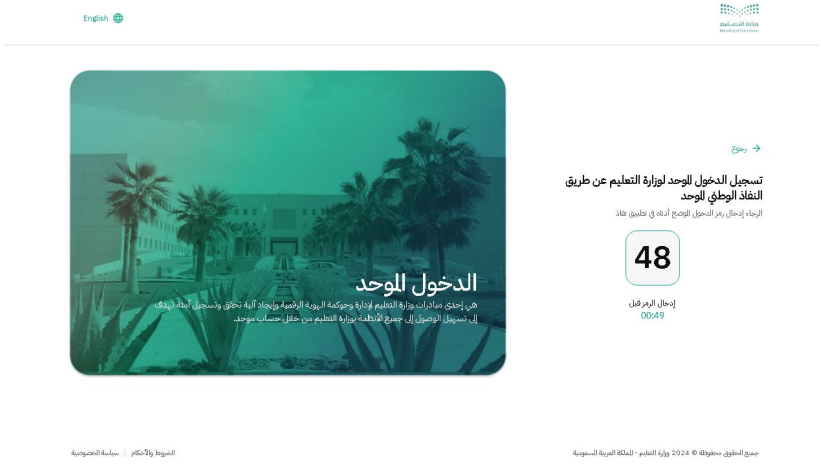
The below steps will be followed by a user which are newly created by the IAM system:

1. Once the user receives the below message from the IAM system confirming the user creation.

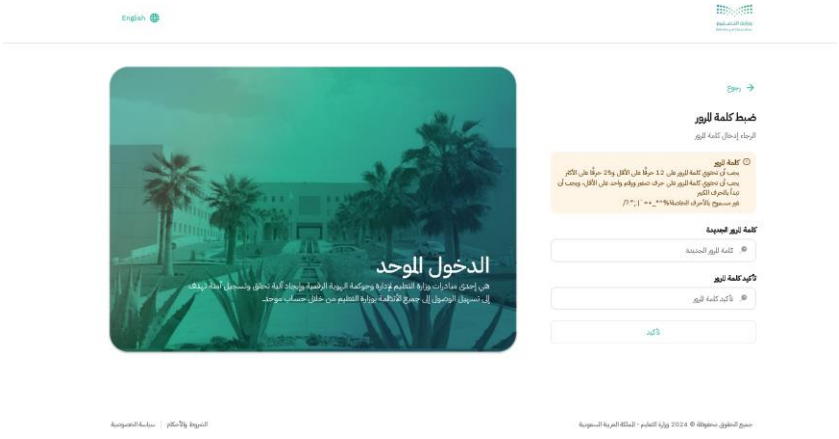
2. User Type integrated application URL (Ex: Faris, Khadamati, or Noor URL) and select the right option to login through SSO.
3. User will be redirected to the Ministry of Education (MOE) single sign on (SSO) login page for authentication.
4. User will have to enter the email address provided to the captcha and click on Next.



5. You will be redirected to Nafath application for validation, this step has to be completed within 60 seconds (one Minute) before the session is invalidated from Nafath.



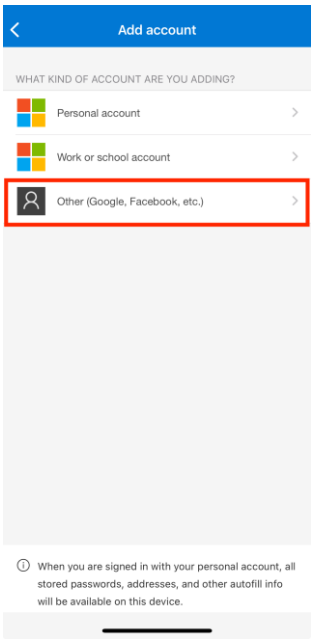
6. Reset password page will be displayed where you will be prompted to set up the new password



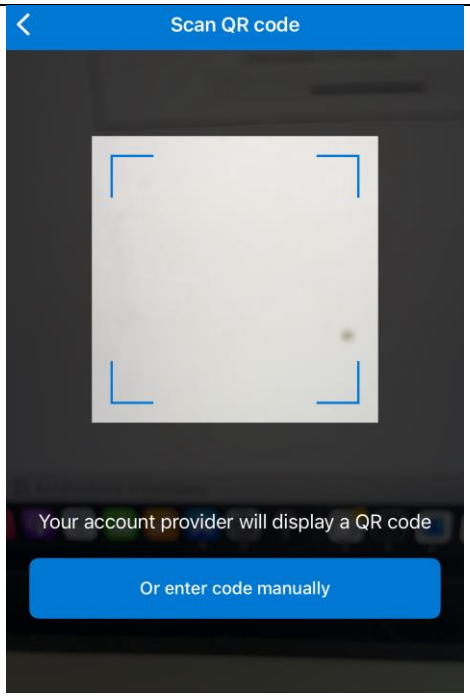
7. TOTP registration page using MOE authenticator will be displayed where you will need to download the “Microsoft Authenticator” application from Apple store or Google Play.

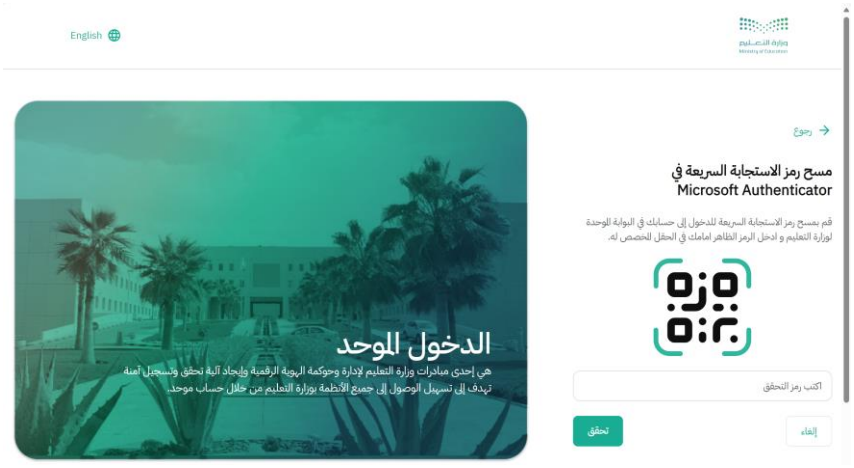
8. In the first screen of the mobile application, Click on the “+” icon

9. Select the option “Other (Google, Facebook, etc,)” in to add MOE account and scan the QR code from the screen:

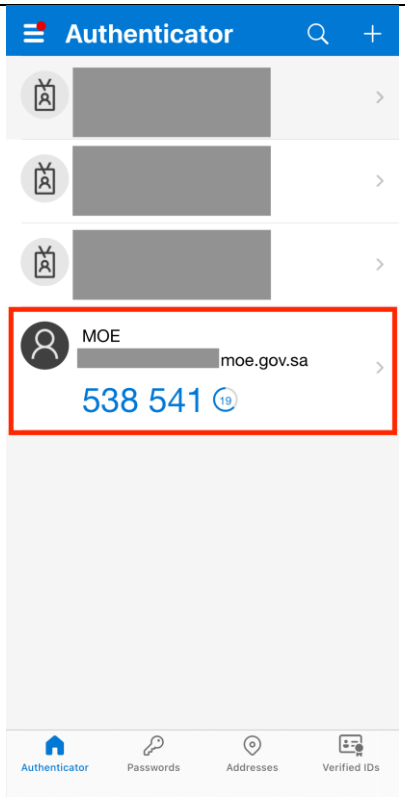


10. Allow the Camera usage and Scan the QR Code





11. TOTP “Time-based One-time Password” will appear on the screen of the mobile application under “MOE” name:



12. After a successful validation of the TOTP, End User license Agreement/Consent Form will be displayed, click “Accept” button

13. You will be redirected to integrated Application requested on first step.

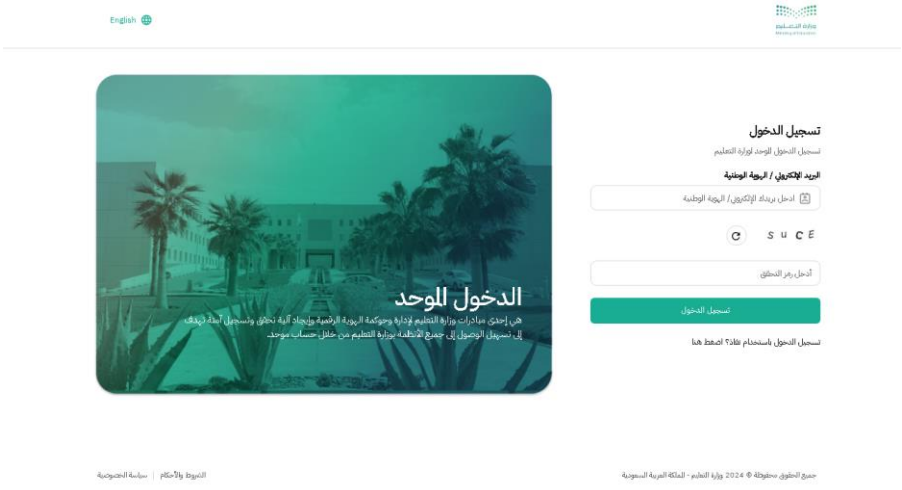
2.2 Existing User - First Time Login

Description:	This scenario describes the steps for Existing MOE Users o login through the SSO platform after for the first time using their existing accounts (Active Directory / Azure AD)
User’s Types / Personas:	- MOE Staff - Education Staff Technical / Principals - Education Staff Admin / Staff - students with Azure AD account

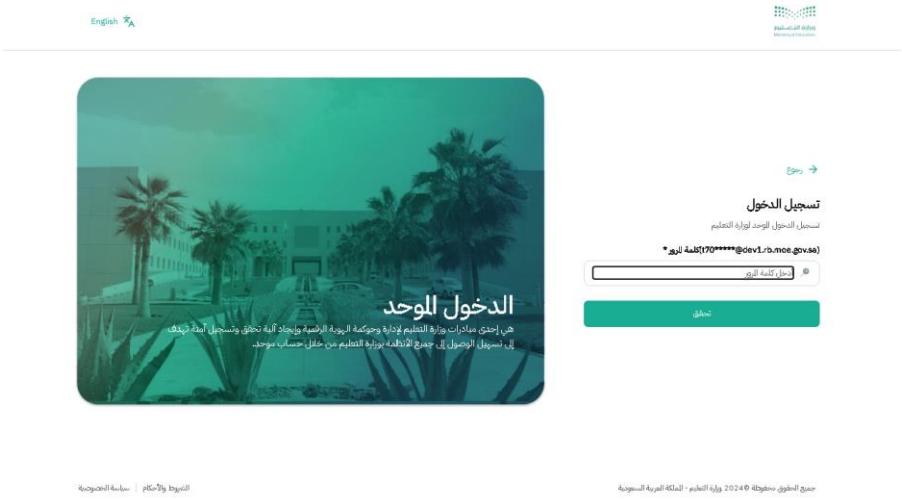
Conditions:	- User knows already exist in MOE federated repositories and has an active account. - User has his username and password handy.

Detailed Steps:

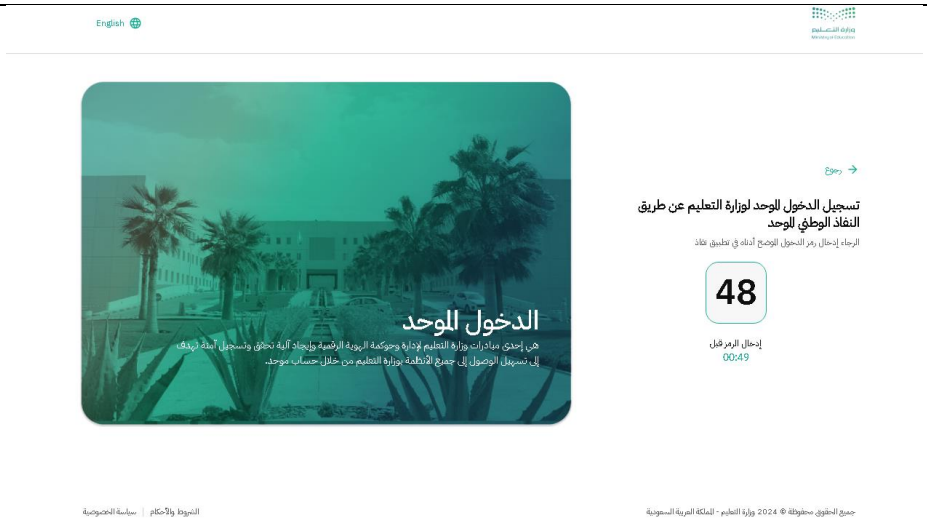
1. User Type integrated application URL (Ex: Faris, Khadamati, or Noor URL) and select the right option to login through SSO.
2. User Enter his AD/Azure email address OR registered National ID (National ID or Residency ID) along with a valid captcha and click on next



3. User Enter his (AD/Azure AD ID Password) and click the button “Login”:

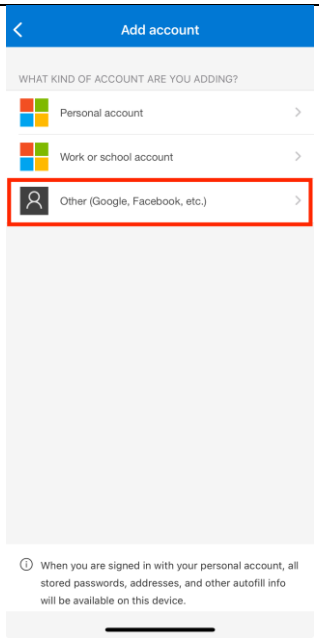


4. After successful user credential validation, user will be redirected to Nafath application for first time validation, this step has to be completed within 60 seconds or 1 minute before the session is invalidated from Nafath.

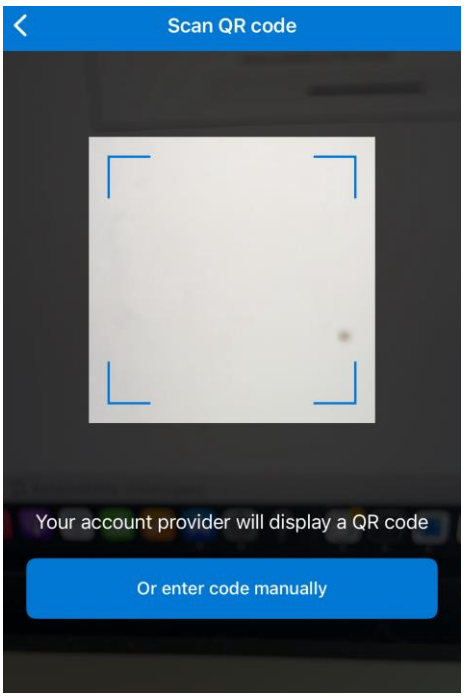


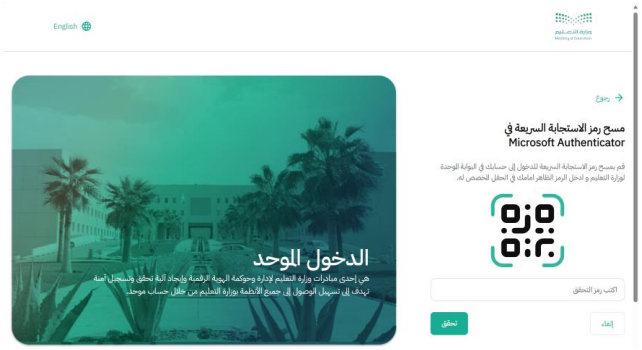
14. TOTP registration page using MOE authenticator will be displayed where you will need to download the “Microsoft Authenticator” application from Apple store or Google Play.
15. In the first screen of the mobile application, Click on the “+” icon

16. Select the option “Other (Google, Facebook, etc,)” in to add MOE account and scan the QR code from the screen:

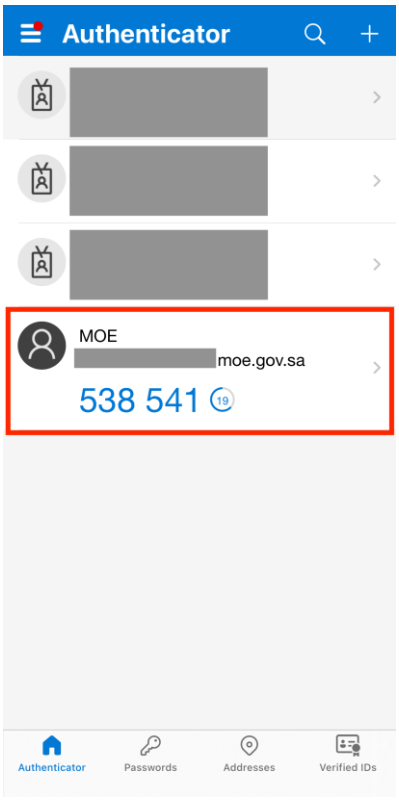


17. Allow the Camera usage and Scan the QR Code





18. TOTP “Time-based One-time Password” will appear on the screen of the mobile application under “MOE” name:



19. After a successful validation of the TOTP, End User license Agreement/Consent Form will be displayed, click “Accept” button

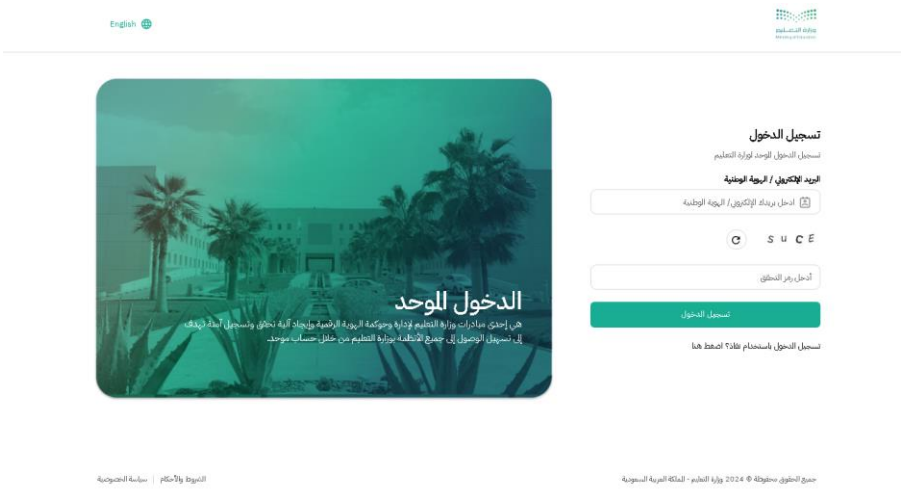
20. You will be redirected to integrated Application requested on first step.

2.3 Existing User - Normal/Regular Login

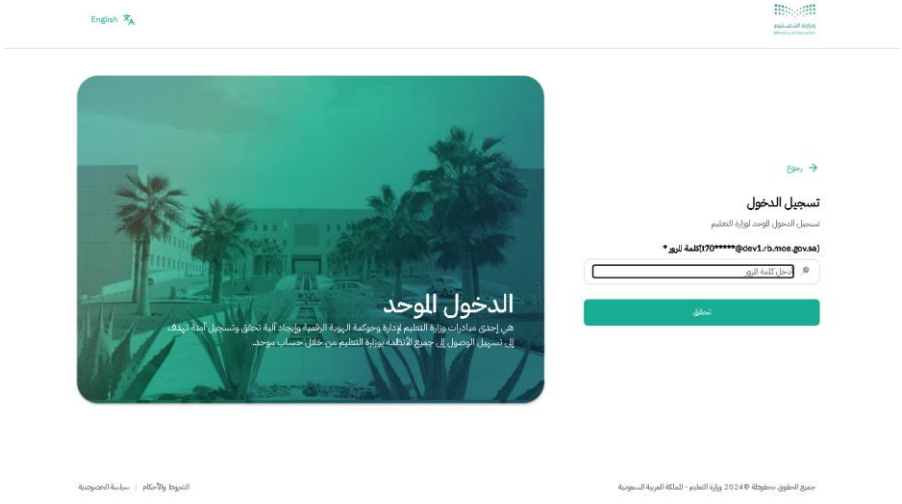
Description:	This scenario describes the steps for Existing MOE Users o login through the SSO platform after for the first time using their existing accounts (Active Directory / Azure AD)
User's Types / Personas:	- MOE Staff - Education Staff Technical / Principals - Education Staff Admin / Staff - students with Azure AD account
Conditions:	- User knows already exist in MOE federated repositories and has an active account. - User has his username and password handy. - MOE Authenticator is installed and configured with MOE TOTP

Detailed Steps:

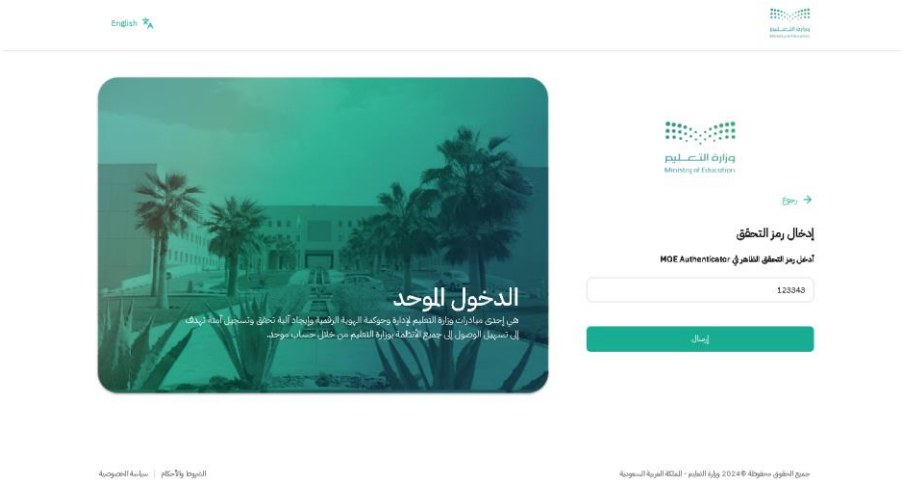
1. User Type integrated application URL (Ex: Faris, Khadamati, or Noor URL) and select the right option to login through SSO.
2. User Enter his AD/Azure email address OR registered National ID (National ID or Residency ID) along with a valid captcha and click on next



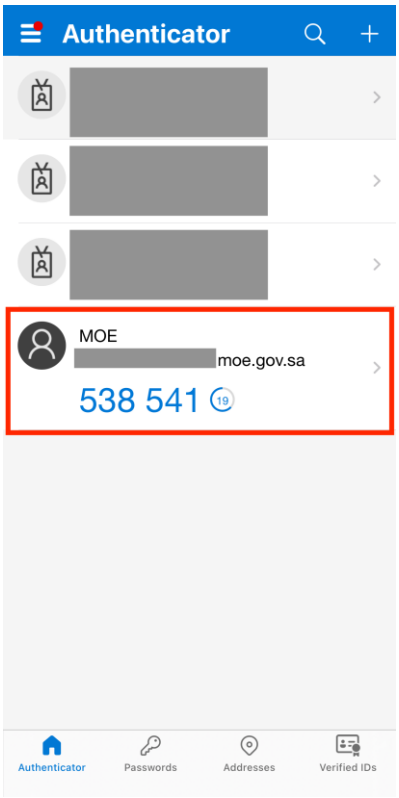
3. User Enter his (AD/Azure AD ID Password) and click the button "Login":



4. After successful user credential validation, you will be prompted to provide the TOTP code from the MOE Authenticator app. Enter the code shown in the MOE authentication (This action needs to be completed before 10 minutes):



5. Open “Microsoft Authenticator” mobile application
6. TOTP “Time-based One-time Password” will appear on the screen of the mobile application under “MOE” name:



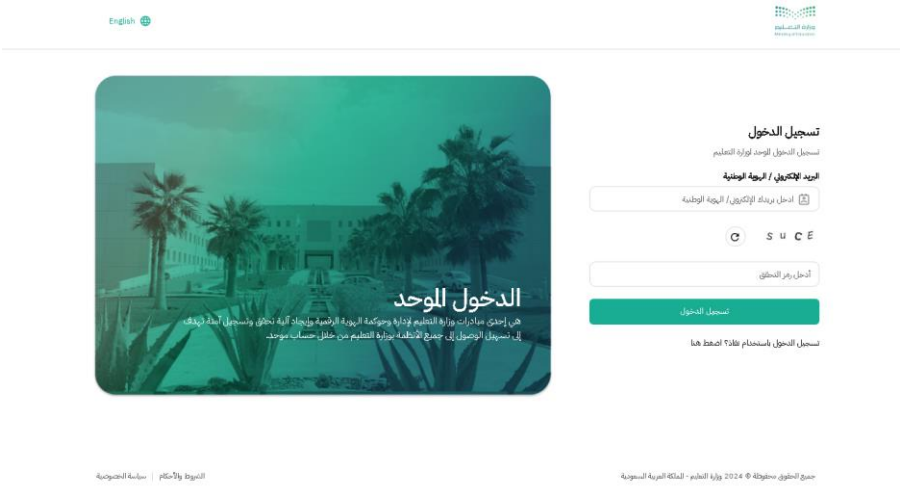
7. You will be redirected to integrated Application requested on first step

2.4 TOTP Reset – New Device registration or Device Lost/Stolen/Damaged

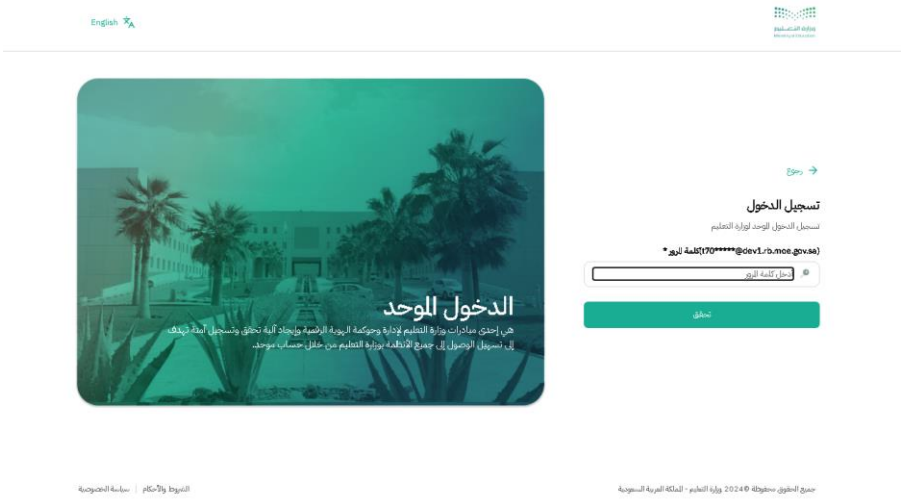
Description:	This scenario describes the steps for Existing MOE Users to perform in case of their TOTP device being stolen/damaged/lost
User's Types / Personas:	- MOE Staff - Education Staff Technical / Principals - Education Staff Admin / Staff - students with Azure AD account
Conditions:	- User knows already exist in MOE federated repositories and has an active account. - User has his username and password handy. - MOE Authenticator was installed and configured with MOE TOTP I the device which was lost/stolen/damaged

Detailed Steps:

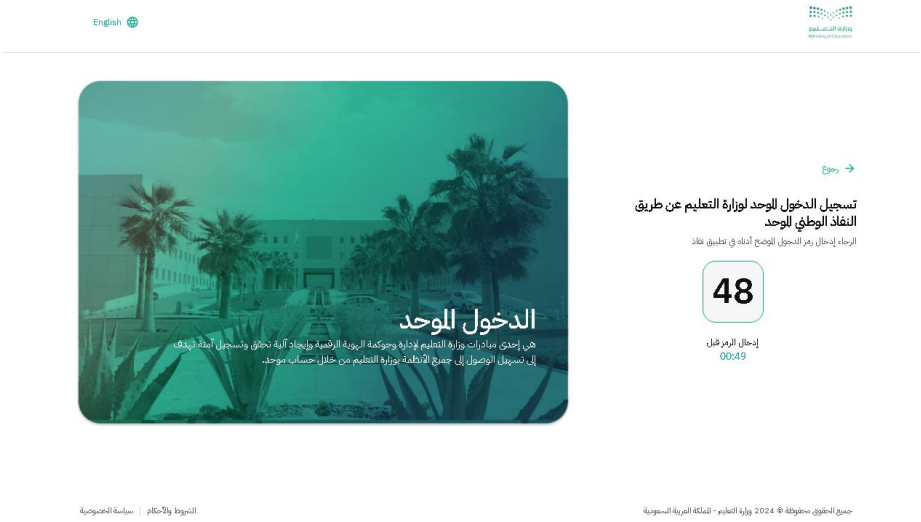
1. User needs to contact the helpdesk team by dialing the helpdesk Phone number (refer point: 3).
2. Help desk will collect the user details and verify if the user is a legitimate user.
3. Post verification helpdesk team will de-register the TOTP for the user (i.e) All the devices which have the user TOTP configured will be removed.
4. Help desk team will notify the user of the de-registration.
5. User Type integrated application URL (Ex: Faris, Khadamati, or Noor URL) and select the right option to login through SSO.
6. User Enter his AD/Azure email address OR registered National ID (National ID or Residency ID) along with a valid captcha and click on next



21. User Enter his (AD/Azure AD ID Password) and click the button “Login”:

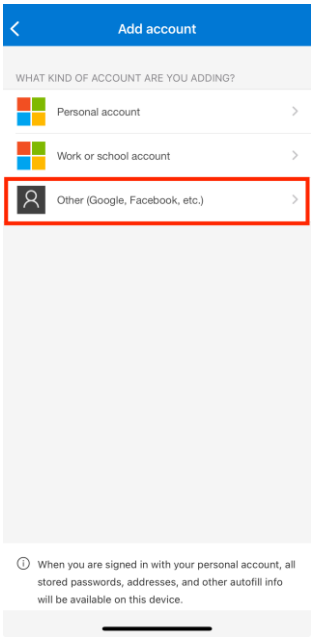


22. After successful user credential validation, user will be redirected to Nafath application for first time validation, this step has to be completed within 60 seconds or 1 minute before the session is invalidated from Nafath.

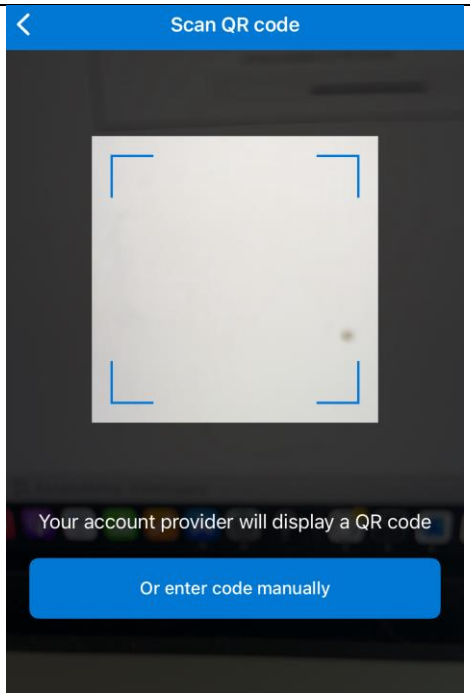


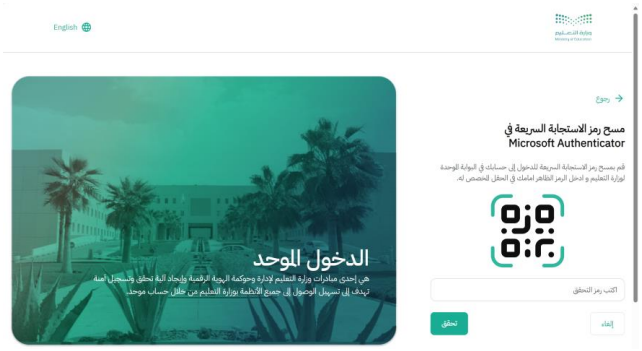
23. TOTP registration page using MOE authenticator will be displayed where you will need to download the “Microsoft Authenticator” application from Apple store or Google Play in the new device.
24. In the first screen of the mobile application, Click on the “+” icon

25. Select the option “Other (Google, Facebook, etc,)” in to add MOE account and scan the QR code from the screen:

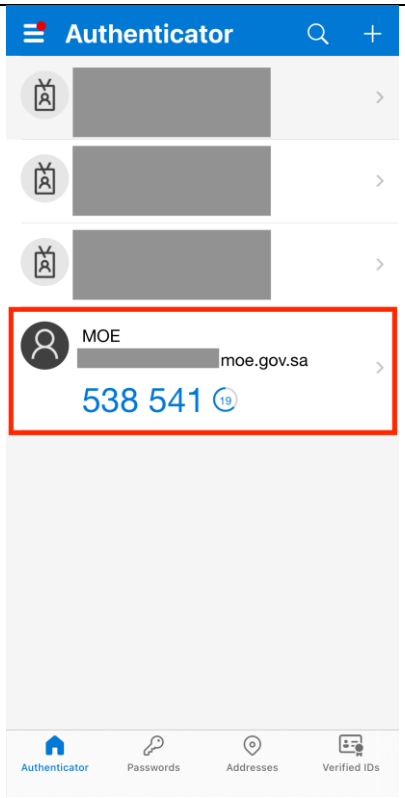


26. Allow the Camera usage and Scan the QR Code





27. TOTP “Time-based One-time Password” will appear on the screen of the mobile application under “MOE” name:



28. After a successful validation of the TOTP, End User license Agreement/Consent Form will be displayed, click “Accept” button

29. You will be redirected to integrated Application requested on first step.

3.1 تفاصيل الاتصال بدعم الفني:

عند مواجهتكم مشكلة في الدخول للنظام :

- يمكنكم التواصل مع مدير المدرسة
- أو التواصل على الهاتف 19996

3.2 Helpdesk Contact Details in English

If you encounter a problem accessing the system:

- You can contact the school principal
- Or call 19996