Instructions on Azure Multi-Factor Authentication (MFA) Enrolment

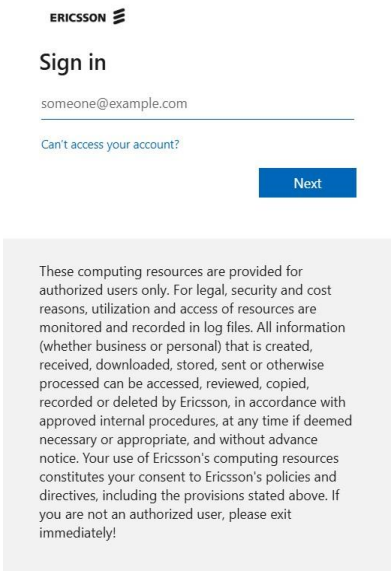
About Ericsson MFA

- To increase security, Ericsson is introducing Multi-Factor Authentication (MFA) for remote system access.
- This provides an additional security layer on top of the username and password.
- In addition to security updates, a new graphical user interface is being deployed.
- The purpose of this guide is to provide instructions for MFA enrolment.

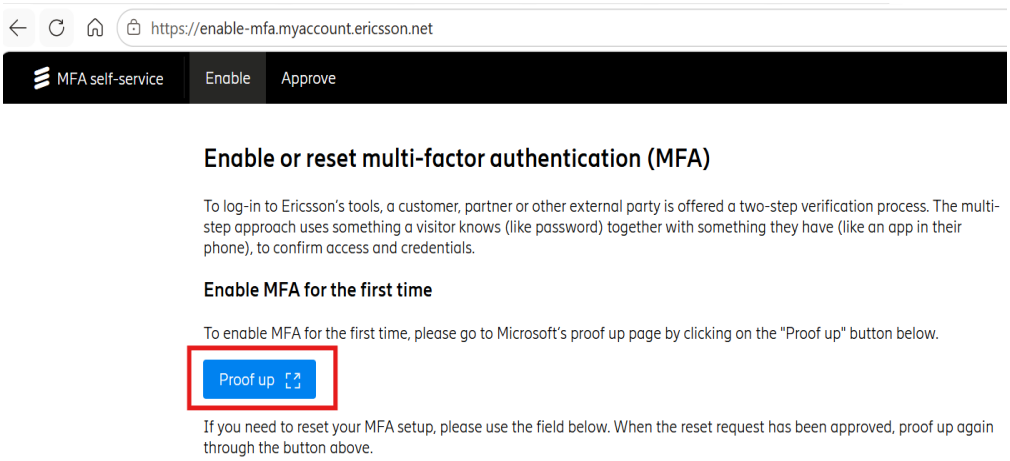
Steps to Register Multifactor Authentication (MFA)

1) Access the following link https://enable-mfa.myaccount.ericsson.net/

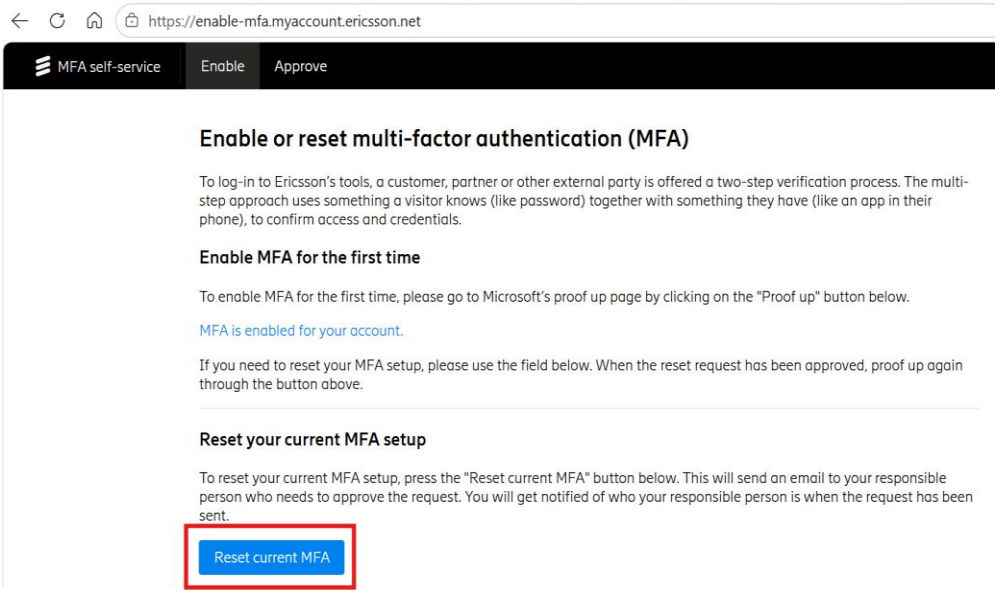
2) Enter your email address, used during ISIGNUM creation & password and click on sign-in.



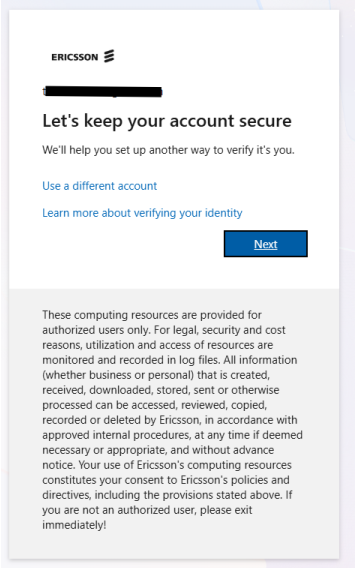
3) Click “Proof up”, you’ll be redirected to https://mysignins.microsoft.com/security-info



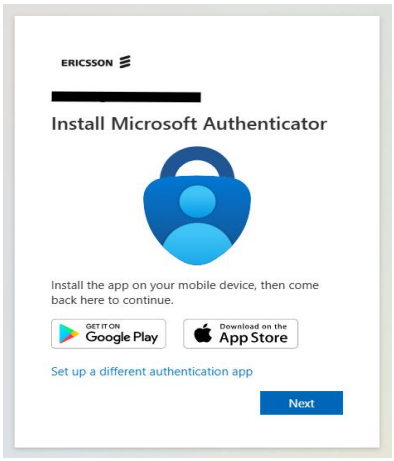
4) Click “Reset current MFA”, to reset your current MFA setup. This will populate the above “Proof up” option for MFA registration.

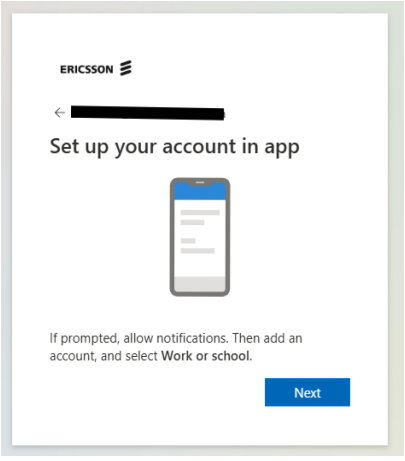


5) Once you click on “Proof up”, you will be redirected to below page for MFA registration.

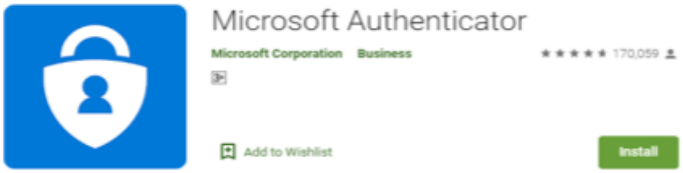


6) Please follow the MFA registration steps as listed below.





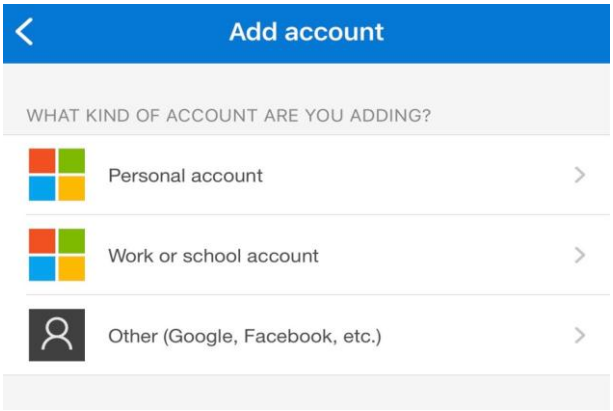
7) Install Microsoft Authenticator on your mobile phone and follow the instructions.



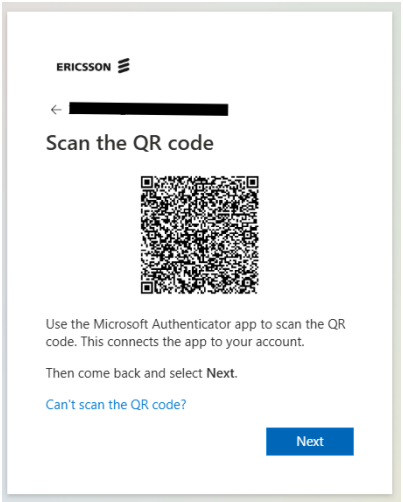
8) Open the Authenticator app and click on the "+" sign at the right top.



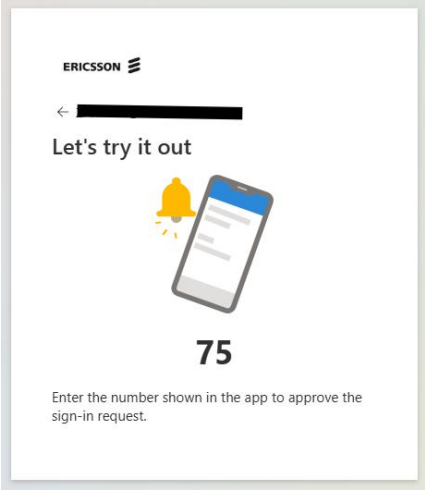
9) Select "Work or school account" and choose "Scan a QR code"



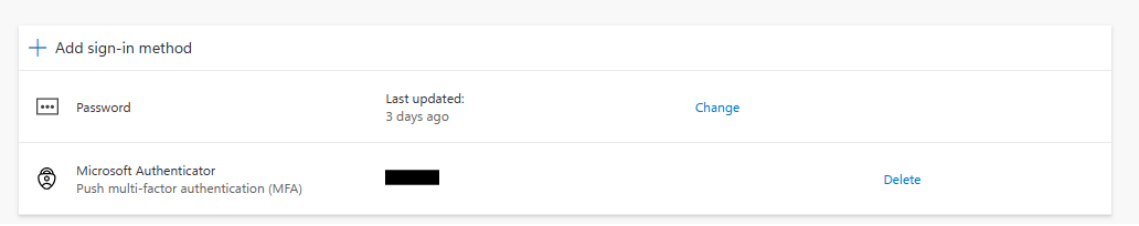
10) Scan the QR code in your laptop/desktop using the Mobile Authenticator app and click Next.



11) Users will be prompted to verify the number using their Mobile Authenticator app



12) Once validated, account is successfully added to the MS Authenticator app.



Appendix: Proof-up with Temporary Access Pass (TAP)

Instructions for XEAD users registering a YubiKey when no MFA method is currently registered.

Purpose. The TAP flow verifies your identity through a responsible person or an eligible colleague, then generates a short-lived Temporary Access Pass. Use that TAP to open Microsoft Security info and register your YubiKey.

Before you begin

- Have access to the email address used for XEAD / Ericsson sign-in.
- Have your YubiKey available. Depending on the key, it may connect through USB, Bluetooth, or NFC.
- Use the TAP only for authentication-method registration. TAP use is monitored and audited.

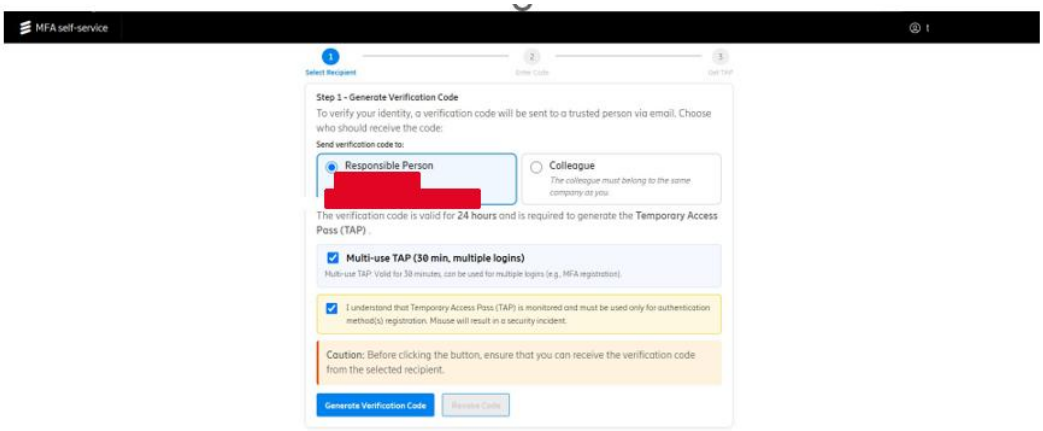
Open the self-service portal

1) Go to https://enable-mfa.myaccount.ericsson.net/ and sign in.
2) If no MFA is registered, the page displays the Temporary Access Pass section. Select Proof-up with TAP to open the TAP wizard.

Initial portal state. Users without a registered MFA method see the Temporary Access Pass section and the Proof-up with TAP button. Selecting that button opens Step 1 of the wizard shown on the next page.

Step 1 - Select a verification-code recipient

The TAP wizard opens at Select Recipient. A verification code will be sent by email to the recipient you choose.



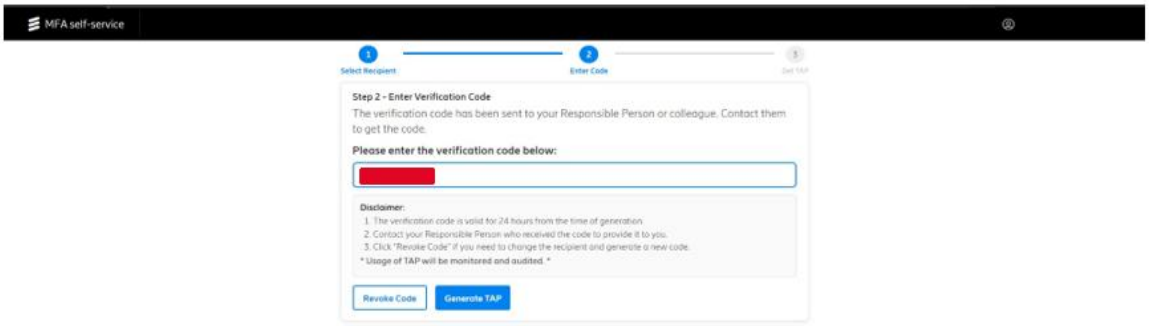
Complete the page as follows:

- Select **Responsible Person** if the code should be sent to the responsible person shown on the page.
- Alternatively, select **Colleague** and choose a colleague who belongs to the same company / organization.
- Select **Multi-use TAP (30 min, multiple logins)** when you need to use the TAP for more than one sign-in during the registration process.
- Read and accept the monitoring statement, then make sure the selected recipient can receive the code.
- Select **Generate Verification Code**.

Need to change the recipient? Select Revoke Code, choose the correct recipient, and generate a new verification code.

Step 2 - Enter the verification code

The selected responsible person or colleague receives the verification code by email. Contact that person and obtain the code.



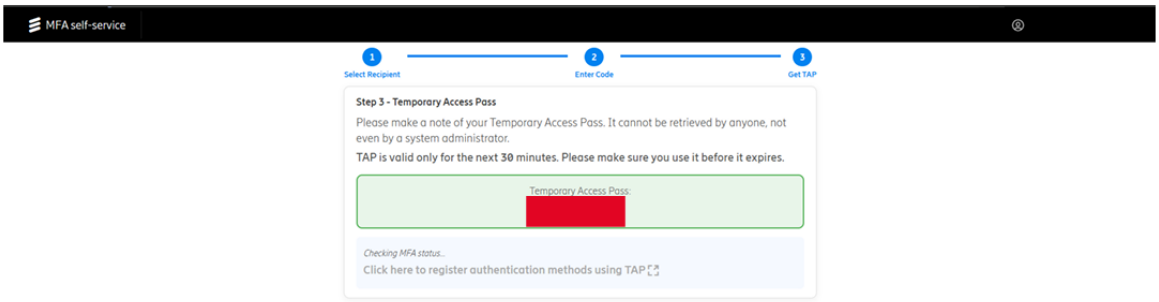
Then:

- Enter the verification code in the field exactly as provided.
- The verification code is valid for 24 hours from the time it is generated.
- Select **Generate TAP** to continue.
- If you need a different recipient, select **Revoke Code** and restart Step 1.

Security reminder. Do not forward the verification code or TAP. Obtain the code directly from the selected recipient and use it only to register your authentication method.

Step 3 - Retrieve the Temporary Access Pass

After the verification code is accepted, the wizard displays the TAP.



Complete the page as follows:

- Make a note of the TAP immediately. It cannot be retrieved later - not even by a system administrator.
- The TAP is valid for 30 minutes. Use it before it expires.
- If you selected multi-use TAP, it can be used for multiple logins during its 30-minutevalidity period.
- Select **Click here to register authentication methods using TAP**.

Important. Keep the TAP private. Do not paste it into email, chat, tickets, or screenshots.

Register the YubiKey using the TAP

Use the generated TAP to satisfy the Microsoft sign-in prompt, then add the YubiKey as a security key.

1) On the Microsoft registration page opened from the TAP wizard, enter the TAP when prompted for a temporary access pass.
2) Open Security info if it is not already displayed.
3) Select + Add sign-in method.
4) Select Security key, then choose the connection type offered for your YubiKey: USB, Bluetooth, or NFC.
5) Insert, tap, or connect the YubiKey and follow the on-screen prompts. Create or enter the security-key PIN if Microsoft requests one, then touch the key when prompted.
6) Give the key a recognizable name and complete registration.
7) Confirm that the YubiKey appears in the Security info list. Keep the original guide available if you also need to register Microsoft Authenticator.

Completion check. Sign out or close the registration page, then verify that the YubiKey is listed under Microsoft Security info. If the TAP expires before registration is complete, return to the self-service portal and generate a new TAP.

Reference

The original guide continues with the standard MFA enrolment steps, including access to Microsoft Security info and adding sign-in methods. This appendix adds the TAP-based path for users who need a temporary sign-in method to register a YubiKey.