

Instructions on Azure MFA enrollment and reset

User Instruction

Contents

1	About Ericsson MFA	2
2	Support and contact	2
3	MFA enrollment via Self-Service Portal	3
4	Resetting MFA	10



1 **About Ericsson MFA**

- To increase security, Ericsson is introducing multi-factor authentication 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 quick guide is to provide short instructions for MFA enrollment and resetting.

2 **Support and contact**

Please contact Extranet Support if you have questions or need help.

<https://www.ericsson.com/en/contact/extranet-support>

Support is available Monday-Sunday, 24 hours/day.

Support Tel: +46 10 71 33085 or 888-671-1268 from North America.




3 MFA enrollment via Self-Service Portal

3.1 Step 1 – Connect to the Self-Service Portal

Note: If you navigate directly to a MFA enforced application, you can jump to section 1.

3.1.1 Login with your email and password to <https://enable-mfa.myaccount.ericsson.net>

ERICSSON 

Sign in

[Can't access your account?](#)

[Sign-in options](#)

[Next](#)

Enterprise sign in

Welcome to Ericsson!
Enter by supplying your user ID or email address and access a whole range of information, services and products.

If you have trouble logging on due to a forgotten password, please click 'Forgot your password?'

User ID

Password

[Sign in](#)

[Password reset - External users](#)
[Password reset - Employees and consultants](#)
[Extranet support](#)



3.1.2 Initiate enrollment process by pressing "Proof up"

The screenshot shows a mobile application interface for MFA enrollment. At the top, there is a navigation bar with a hamburger menu icon on the left, the text "Enable" and "Approve" in the center, and a user profile icon on the right. Below the navigation bar, the main heading is "Enable or reset multi-factor authentication (MFA)". The text below explains that to log in to Ericsson's tools, a two-step verification process is used. It then provides instructions on how to enable MFA for the first time by clicking on a "Proof up" button, which is highlighted with a red box. Below this, there is a section for resetting the MFA setup, followed by a "Reset your current MFA setup" heading and instructions. At the bottom, a status message reads "MFA is not enabled yet for your account."

Enable or reset multi-factor authentication (MFA)

To log-in to Ericsson's tools, a customer, partner or other external party is offered a two-step verification process. The multi-step approach uses something a visitor knows (like password) together with something they have (like an app in their phone), to confirm access and credentials.

Enable MFA for the first time

To enable MFA for the first time, please go to Microsoft's proof up page by clicking on the "Proof up" button below.

[Proof up](#)

If you need to reset your MFA setup, please use the field below. When the reset request has been approved, proof up again through the button above.

Reset your current MFA setup

To reset your current MFA setup, press the "Reset current MFA" button below. This will send an email to your responsible person who needs to approve the request. You will get notified of who your responsible person is when the request has been sent.

[MFA is not enabled yet for your account.](#)

3.1.3 You will be redirected to Microsoft proof up wizard. Press "Next".

The screenshot shows a Microsoft proof up wizard screen. At the top left, the Ericsson logo is displayed. Below it, the email address "██████████@yahoo.com" is shown. The main heading is "More information required". The text below states "Your organization needs more information to keep your account secure". There are two links: "Use a different account" and "Learn more". At the bottom right, a blue "Next" button is highlighted with a red box.

ERICSSON

██████████@yahoo.com

More information required

Your organization needs more information to keep your account secure

[Use a different account](#)

[Learn more](#)

[Next](#)



3.1.4

You will be displayed this view. Proceed to Section 3.2.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

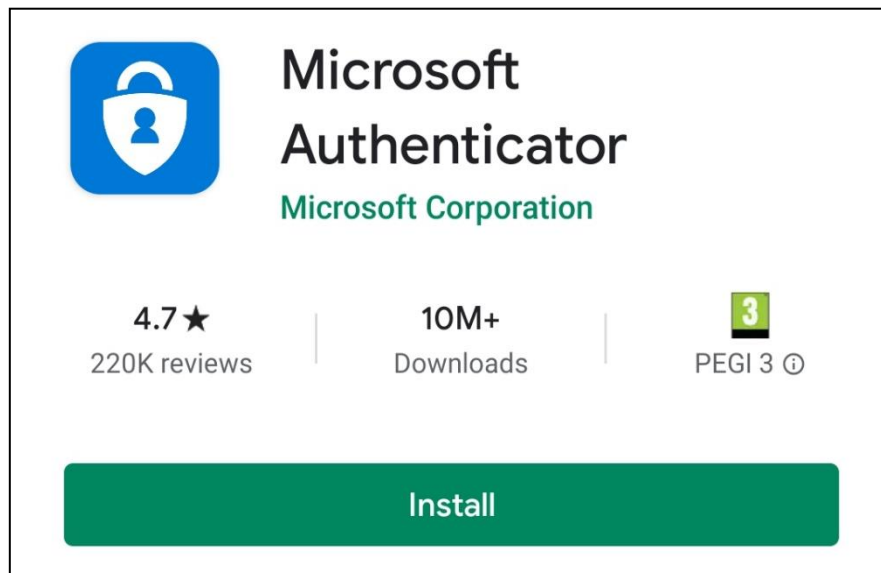
Mobile app has been configured.

3.2

Step 2 – Install and configure mobile app

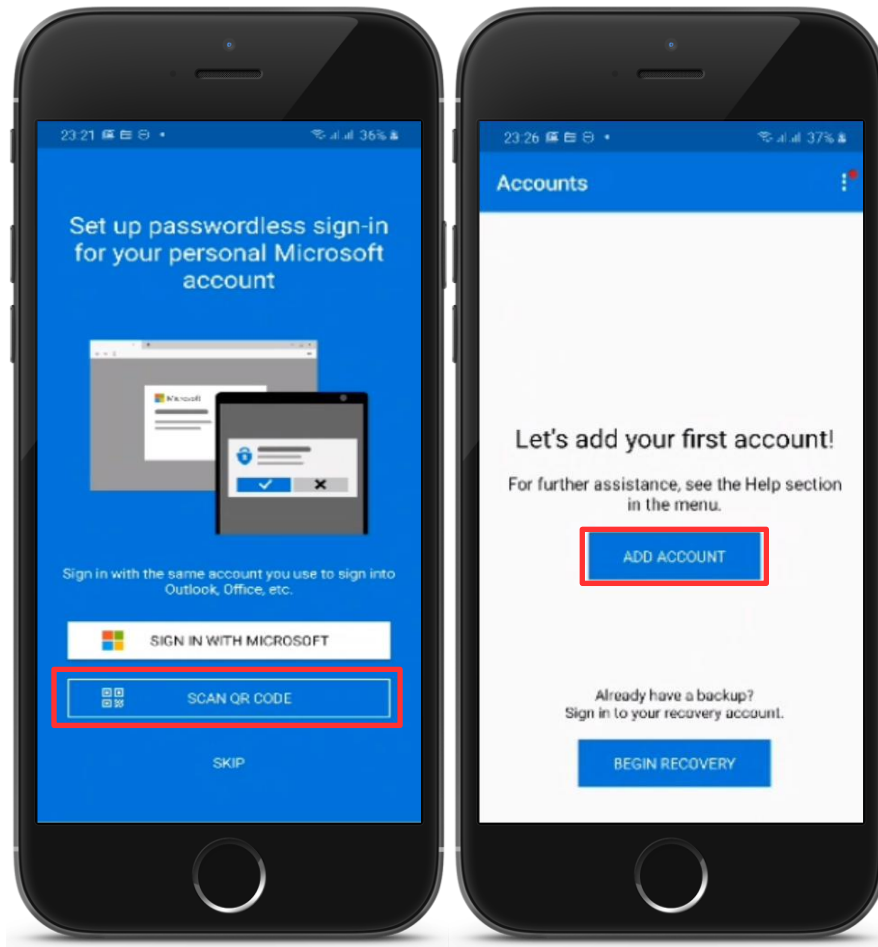
3.2.1

Download Microsoft Authenticator app on your mobile phone





3.2.2 Launch app and press "Scan QR Code" or press "Add account" and then "Work or school account".





3.2.3 Press "Set up" button on the Security verification screen from Step Error! Reference source not found.

Additional security verification

Secure your account by adding phone verification to your password. [View video to know how to secure your account](#)

Step 1: How should we contact you?

Mobile app ▼

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up Mobile app has been configured.


Next

3.2.4 Scan the QR code displayed in the browser and press "Next"

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for Windows Phone, Android or iOS.
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



If you are unable to scan the image, enter the following information in your app.
Code: 484 684 454
Url: <https://cys01eupad09.eu.phonefactor.net/pad/367266942>

If the app displays a six-digit code, choose "Next".

Next cancel



3.2.5 Wait for the message "Mobile app has been configured for notifications and verification codes"

3.3 Step 3 – Verify mobile app setup

3.3.1 Choose "Use verification code" as MFA method and press "Next"

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?

Receive notifications for verification

Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up Mobile app has been configured for notifications and verification codes.

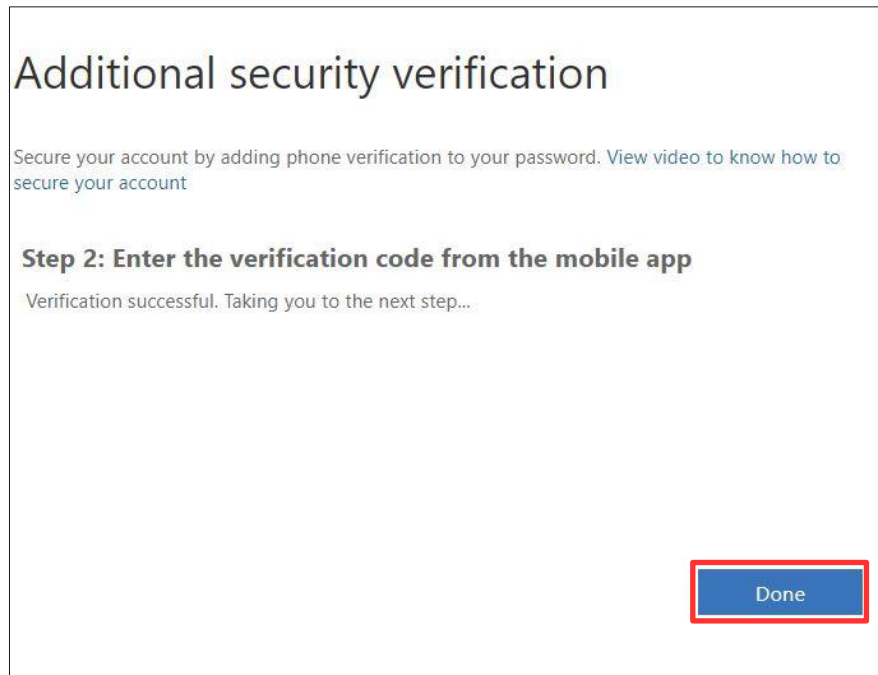
Next

3.3.2 Verify the mobile app setup by providing token generated in Authenticator app



3.3.3

Verification is successful once you see the message in the browser *“Verification successful. Taking you to the next step”*, then press *“Done”* button.





4 Resetting MFA

4.1 Login with your email and password to <https://enable-mfa.myaccount.ericsson.net>

4.2 Press on "Reset current MFA" to initiate the reset process

The screenshot shows a web interface for managing Multi-Factor Authentication (MFA). At the top, there is a navigation bar with a hamburger menu icon, the text 'Enable', the text 'Approve', and a user profile icon. The main content area is titled 'Enable or reset multi-factor authentication (MFA)'. Below the title, there is a paragraph explaining the two-step verification process. This is followed by a section titled 'Enable MFA for the first time' with instructions to go to Microsoft's proof up page. Below that, a blue link states 'MFA is enabled for your account.' Another paragraph explains how to reset the MFA setup. At the bottom of this section, a blue button labeled 'Reset current MFA' is highlighted with a red rectangular border.

4.3 A message will be sent to Ericsson responsible to approve your request. Once it is approved, you will receive email notification or you can check status on <https://enable-mfa.myaccount.ericsson.net>

4.4 Once request for resetting MFA is approved, you need to perform all steps described in MFA enrollment via Self-Service Portal section.