MOS USER SECURITY GUIDE

Guide #001

Set Up MFA On Your Account

Multi-Factor Authentication - your first line of defence

This guide explains why MFA is required at Magister Operis Systems and shows you exactly how to set it up on your Microsoft 365 account in under 5 minutes.

Jean Claude Munyakazi | IT Systems Administrator | Magister Operis Systems

munyakazi.org

🏢 COMPANY POLICY

MOS Security Policy §3.1 requires all staff to enable Multi-Factor Authentication (MFA) on their company Microsoft 365 account.

Deadline: MFA must be active within 5 business days of receiving this notice.

Accounts without MFA enabled will be blocked from signing in after the deadline.

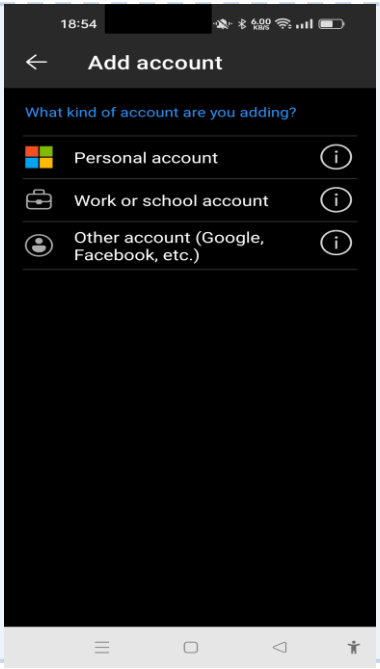
⚠ WHY THIS MATTERS

80% of account breaches happen because of stolen passwords alone. MFA means even if someone steals your password, they CANNOT access your account without your phone.

One stolen account can give attackers access to company files, emails, and client data.

STEP 1

Download Microsoft Authenticator



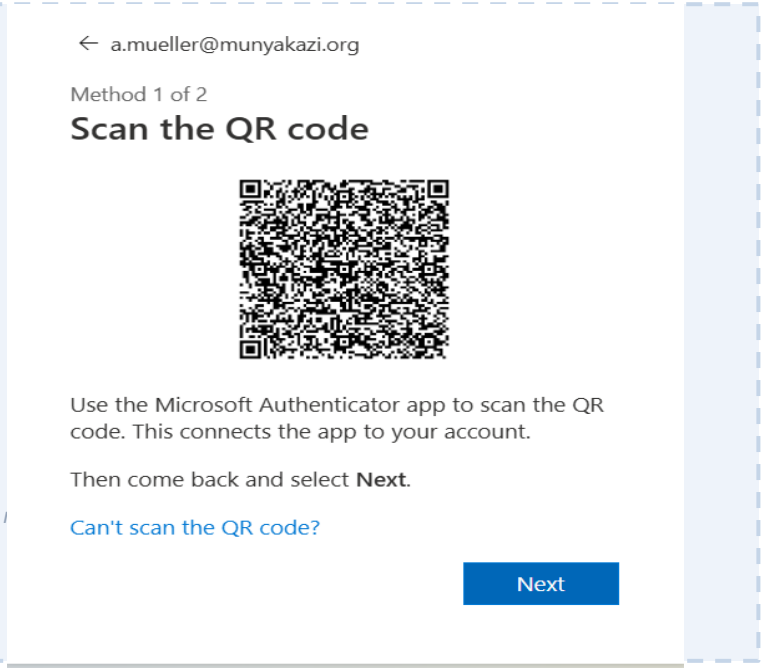
INSTRUCTIONS

1. Open the App Store (iPhone) or Google Play (Android)
2. Search for: Microsoft Authenticator
3. Install the app by Microsoft Corporation
4. Open the app - tap Add account when prompted

→ Keep the app open, you'll need it in Step 2

STEP 2

Go to Your Security Settings



INSTRUCTIONS

1. Open a browser and go to: myaccount.microsoft.com

2. Sign in with your company email

3. Click: Security info (left menu)

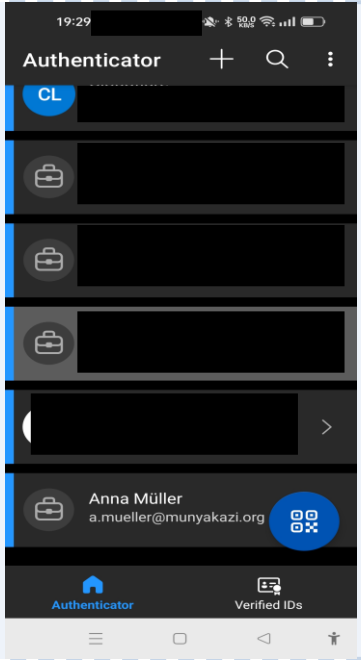
4. Click: + Add sign-in method

5. From the dropdown choose: Authenticator app

→ A QR code will appear on screen - do NOT close this page

STEP 3

Scan the QR Code



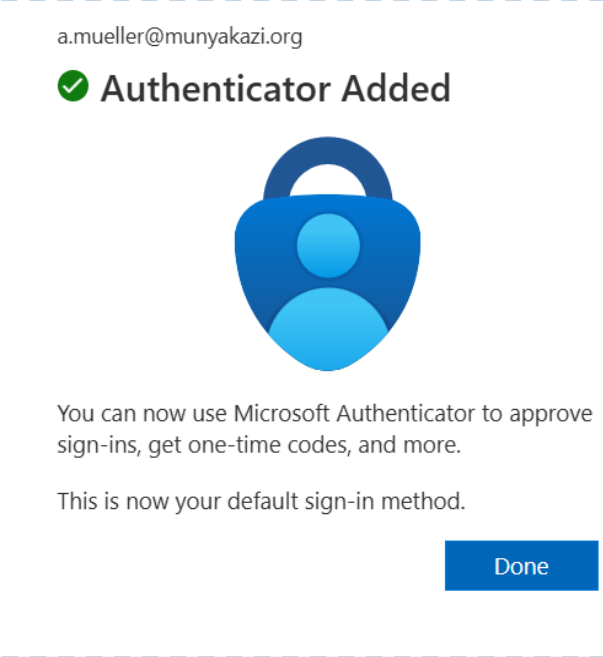
INSTRUCTIONS

1. In the Authenticator app tap the + icon
2. Choose: Work or school account
3. Choose: Scan a QR code
4. Point your phone camera at the QR code on screen
5. Your account appears in the app with a 6-digit code

→ Click Next on the browser page

STEP 4

Test and Confirm



INSTRUCTIONS

1. The browser will send a test notification to your phone

2. On your phone tap: Approve

3. Browser shows: Notification approved ✓

4. Click Next → then Done

→ MFA is now active on your account!

Next time you sign in, you will receive an approval request on your phone.

What NOT To Do

Don't share your 6-digit code

This code is personal. IT will never ask for it. If someone asks, it is a scam.

Don't skip the backup method

After setup, add a backup phone number in Security info so you can still access your account if you lose your phone.

Don't approve requests you didn't start

If your phone asks to approve a login you didn't do, tap DENY and contact IT immediately.

Don't delay past the deadline

Your account will be blocked after 5 business days without MFA. Setup takes less than 5 minutes.

Don't use personal email for MFA

Always register your company account only. Personal accounts are not covered by company security policy.

Don't use SMS as your only method

Phone-based authentication apps are more secure than SMS codes. Always prefer the Authenticator app.

Need Help? Contact IT

IT Helpdesk Chat

Teams → MOS IT Support
Channel: Incidents

Email Support

itsupport@munyakazi.org
Response within 4 hours

Urgent Security Issue

Call your manager immediately
Do NOT wait for email response

Remember: IT will NEVER ask for your password over email, chat, or phone.

✅ Quick Summary

Set Up MFA on Your Account

1. Install Microsoft Authenticator from App Store or Google Play
2. Go to myaccount.microsoft.com → Security info → Add sign-in method
3. Scan the QR code with the Authenticator app
4. Approve the test notification on your phone to confirm
5. Never approve MFA requests you did not initiate yourself
6. Contact IT if you lose your phone or cannot complete setup