M365 Administration Runbook #002

How to Enable MFA for Users in Microsoft 365

Using Entra ID (Azure Active Directory) - Security Defaults & Per-User MFA

🔐 Magister Operis Systems | ⚙ Entra ID | ⏱ 30 min | 🟢 Beginner

Jean Claude Munyakazi

IT Systems Administrator | Berlin, Germany | munyakazi.org

What You Will Learn

WHY MFA MATTERS

- 99.9% of account attacks are stopped by MFA
- Required for any serious M365 deployment
- First security task after creating user accounts
- Protects against phished passwords

METHOD 1 - SECURITY DEFAULTS

- Enables MFA for ALL users in one click
- Microsoft's recommended baseline setting
- Configured in Entra ID portal
- Best for: small organisations, first deployment

METHOD 2 - PER-USER MFA

- Enable MFA for specific users only
- Useful for testing before full rollout
- Configured in Entra ID → Users
- Best for: lab environments and demos

In this runbook we use BOTH methods - Security Defaults for the full tenant, then Per-User MFA to demonstrate individual account control.

Prerequisites

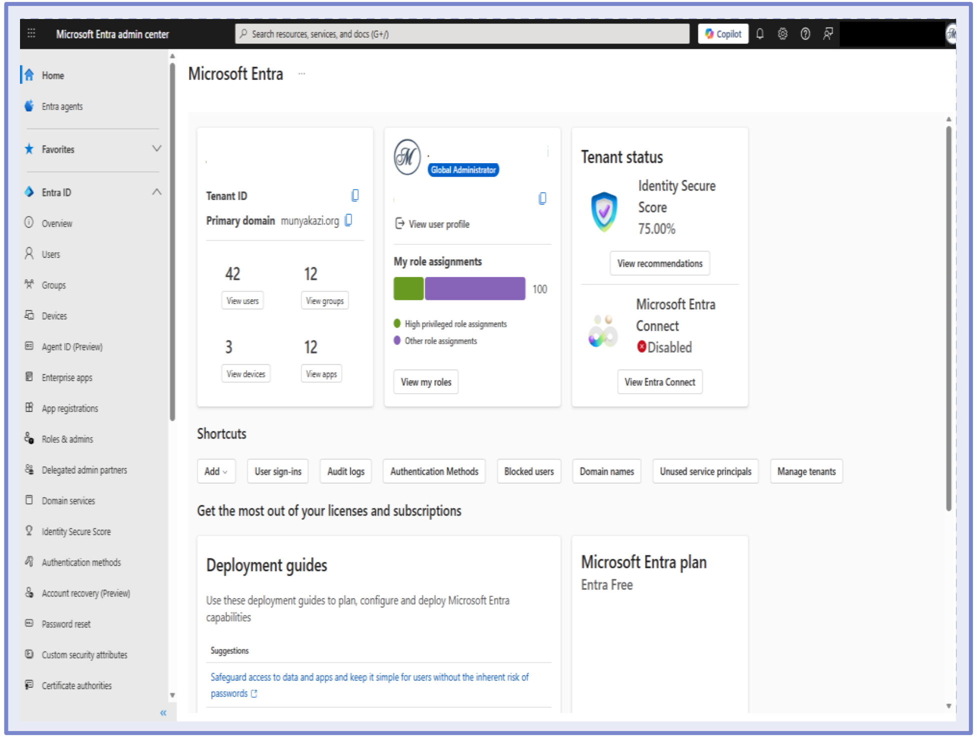
Requirement	Details
Admin Role	Global Administrator or Security Administrator
Users	At least the 23 users created in Runbook #001 must exist
Access URL	entra.microsoft.com (Entra ID portal)
Authenticator App	Microsoft Authenticator installed on a test mobile device
Important	Enabling Security Defaults will require MFA for ALL users including you
Recommendation	Test Per-User MFA on one account before enabling tenant-wide

1

Method 1 - Security Defaults

Enable MFA for the entire tenant in Entra ID

STEP 1 Open Entra ID Portal



Tenant ID

Primary domain munyakazi.org

42 View users | 12 View groups

3 View devices | 12 View apps

Tenant status

Identity Secure Score 75.00%

Microsoft Entra Connect Disabled

Get the most out of your licenses and subscriptions

Deployment guides

Use these deployment guides to plan, configure and deploy Microsoft Entra capabilities

Safeguard access to data and apps and keep it simple for users without the inherent risk of passwords

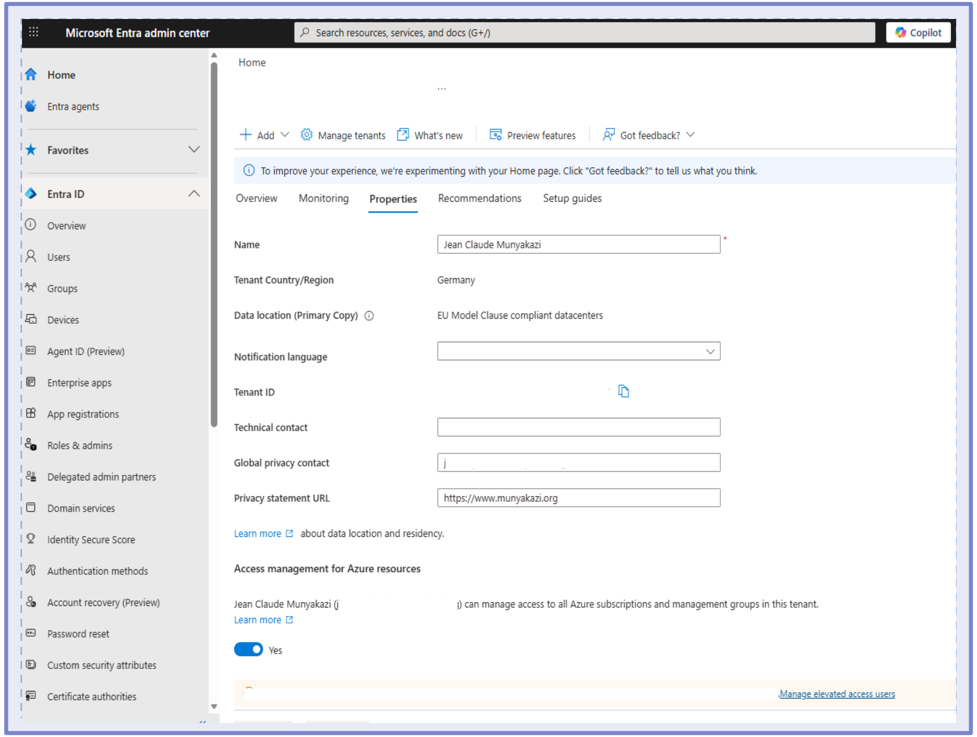
Microsoft Entra plan
Entra Free

INSTRUCTIONS

- Open a new browser tab and go to: entra.microsoft.com
- Sign in with your Global Administrator account

→ You land on the Microsoft Entra admin center overview

STEP 2 Navigate to Properties



To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

Name: Jean Claude Munyakazi *

Tenant Country/Region: Germany

Data location (Primary Copy): EU Model Clause compliant datacenters

Notification language:

Tenant ID:

Technical contact:

Global privacy contact: j

Privacy statement URL: https://www.munyakazi.org

Learn more about data location and residency.

Access management for Azure resources

Jean Claude Munyakazi (j) can manage access to all Azure subscriptions and management groups in this tenant.
Learn more

Yes

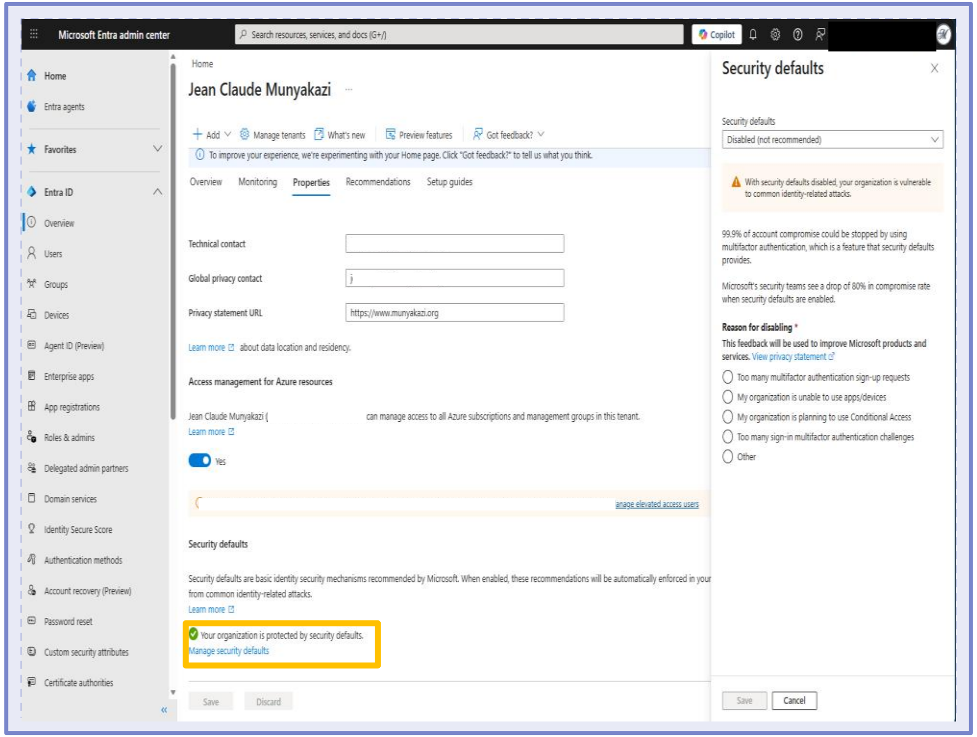
INSTRUCTIONS

- In the left menu expand: Identity
- Click: Overview
- Click the Properties tab at the top of the page

→ The tenant properties panel opens

STEP 3

Open Security Defaults



[redacted]

Home

Jean Claude Munyakazi ...

To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

Technical contact:

Global privacy contact: j

Privacy statement URL: https://www.munyakazi.org

Learn more about data location and residency.

Access management for Azure resources

Jean Claude Munyakazi (can manage access to all Azure subscriptions and management groups in this tenant.
Learn more

Yes

anage elevated access users

Security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your from common identity-related attacks.
Learn more

✓ Your organization is protected by security defaults.
Manage security defaults

Security defaults

Security defaults: Disabled (not recommended)

With security defaults disabled, your organization is vulnerable to common identity-related attacks.

99.9% of account compromise could be stopped by using multifactor authentication, which is a feature that security defaults provides.

Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled.

Reason for disabling *

This feedback will be used to improve Microsoft products and services. View privacy statement

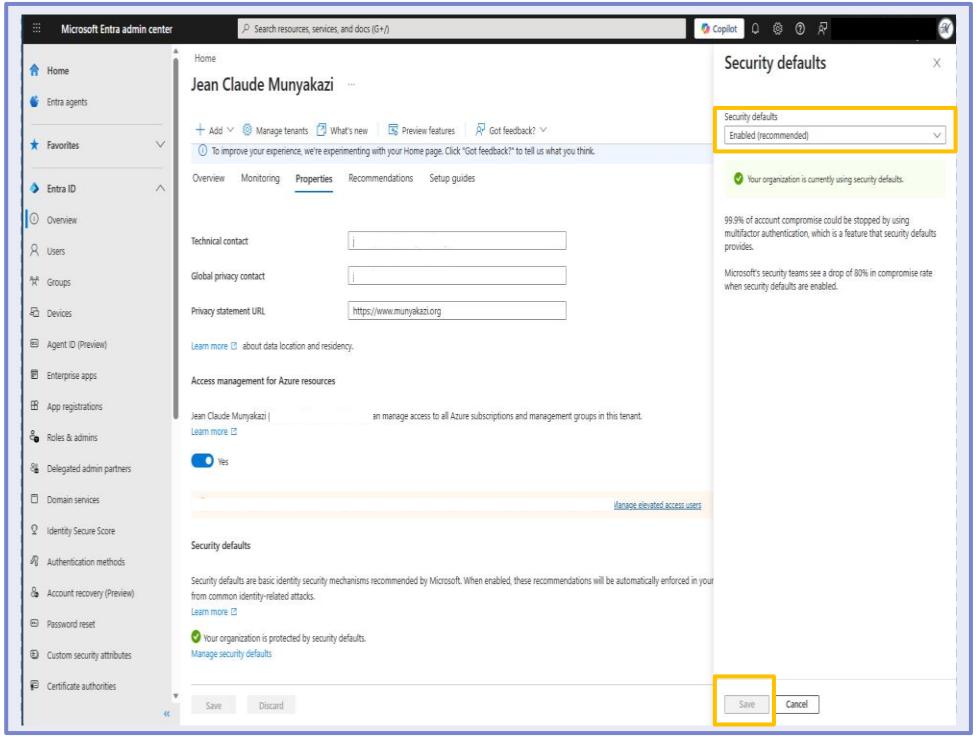
○ Too many multifactor authentication sign-up requests
○ My organization is unable to use apps/devices
○ My organization is planning to use Conditional Access
○ Too many sign-in multifactor authentication challenges
○ Other

INSTRUCTIONS

- Scroll to the bottom of the Properties page
- Click the link: Manage Security defaults

→ **A side panel slides open on the right**

STEP 4 Enable Security Defaults



Home

Jean Claude Munyakazi ...

To improve your experience, we're experimenting with your Home page. Click "Got feedback?" to tell us what you think.

Technical contact

Global privacy contact

Privacy statement URL: https://www.munyakazi.org

Learn more about data location and residency.

Access management for Azure resources

Jean Claude Munyakazi (an manage access to all Azure subscriptions and management groups in this tenant.

Learn more

Yes

Manage elevated access users

Security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your from common identity-related attacks.

Learn more

Your organization is protected by security defaults.

Manage security defaults

Security defaults

Security defaults: Enabled (recommended)

Your organization is currently using security defaults.

99.9% of account compromise could be stopped by using multifactor authentication, which is a feature that security defaults provides.

Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled.

INSTRUCTIONS

- In the Security defaults panel:
- Set the toggle to: Enabled
- A warning appears - this will require MFA for ALL users

→ Click Save to apply the setting

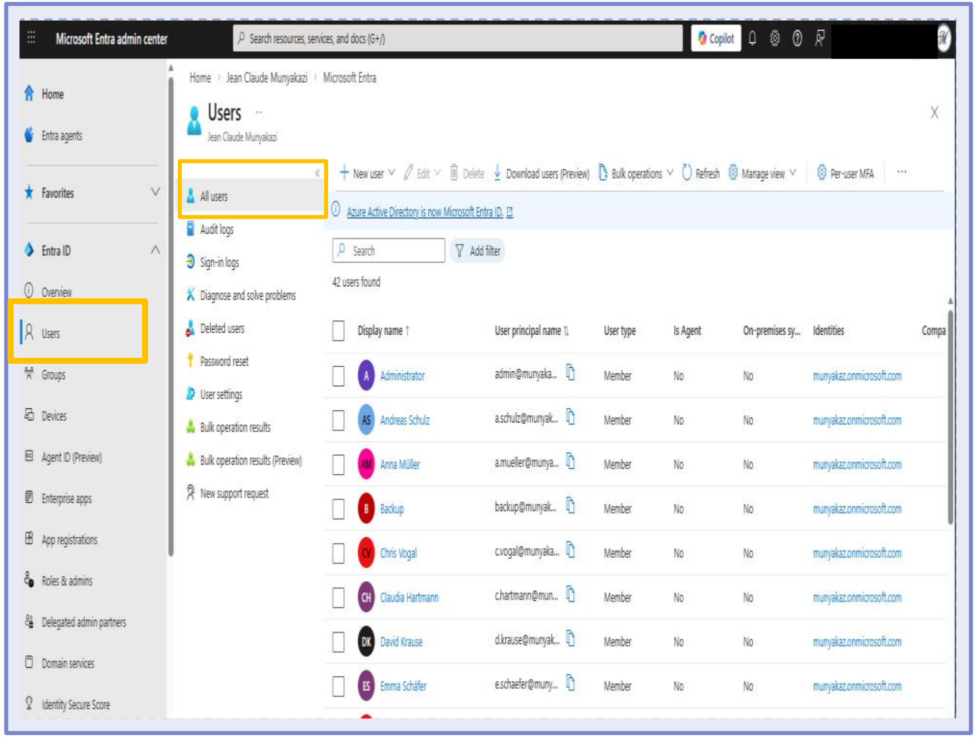
→ All users will now be prompted for MFA at next sign-in

2

Method 2 - Per-User MFA

Enable MFA for individual users (useful for testing)

STEP 1 Navigate to All Users



Azure Active Directory is now Microsoft Entra ID.

42 users found

□	Display name ↑	User principal name ⇅	User type	Is Agent	On-premises sy...	Identities	Compa
□	Administrator	admin@munyaka...	Member	No	No	munyakaz.onmicrosoft.com	
□	Andreas Schulz	a.schulz@munyak...	Member	No	No	munyakaz.onmicrosoft.com	
□	Anna Müller	a.mueller@munya...	Member	No	No	munyakaz.onmicrosoft.com	
□	Backup	backup@munyak...	Member	No	No	munyakaz.onmicrosoft.com	
□	Chris Vogal	c.vogal@munyaka...	Member	No	No	munyakaz.onmicrosoft.com	
□	Claudia Hartmann	c.hartmann@mun...	Member	No	No	munyakaz.onmicrosoft.com	
□	David Krause	d.krause@munyak...	Member	No	No	munyakaz.onmicrosoft.com	
□	Emma Schäfer	e.schaefer@muny...	Member	No	No	munyakaz.onmicrosoft.com	

INSTRUCTIONS

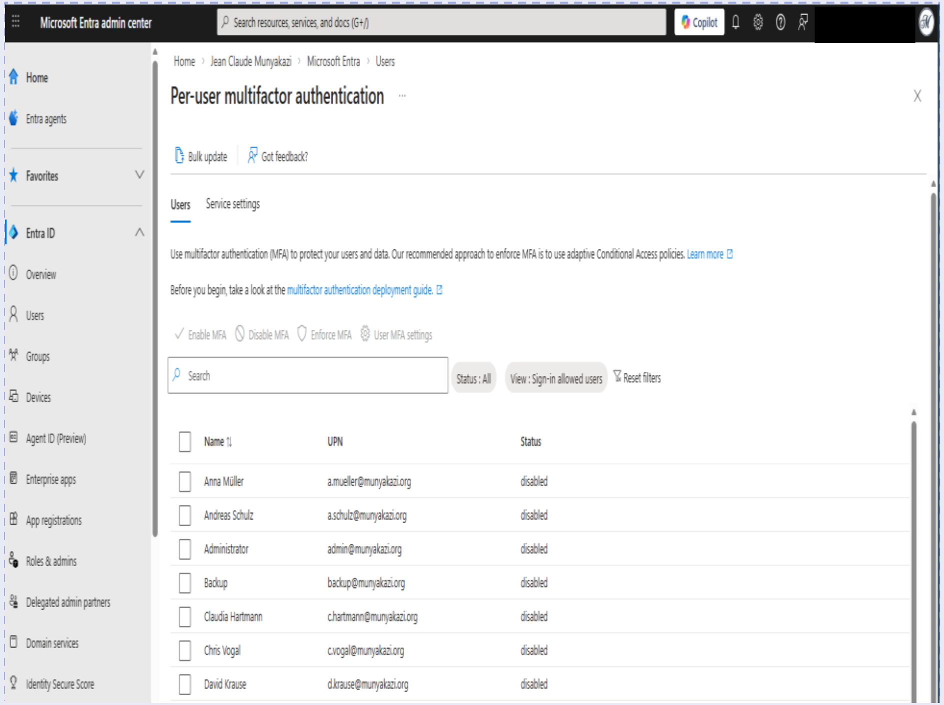
- In Entra ID left menu click: Identity → Users → All users

→ Full list of all tenant users appears

- You should see all 23 Magister Operis Systems staff here

STEP 2

Open Per-User MFA Settings



Home › Jean Claude Munyakazi › Microsoft Entra › Users

Per-user multifactor authentication ...

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more

Before you begin, take a look at the multifactor authentication deployment guide.

□	Name ↑↓	UPN	Status
□	Anna Müller	a.mueller@munyakazi.org	disabled
□	Andreas Schulz	a.schulz@munyakazi.org	disabled
□	Administrator	admin@munyakazi.org	disabled
□	Backup	backup@munyakazi.org	disabled
□	Claudia Hartmann	c.hartmann@munyakazi.org	disabled
□	Chris Vogal	c.vogal@munyakazi.org	disabled
□	David Krause	d.krause@munyakazi.org	disabled

INSTRUCTIONS

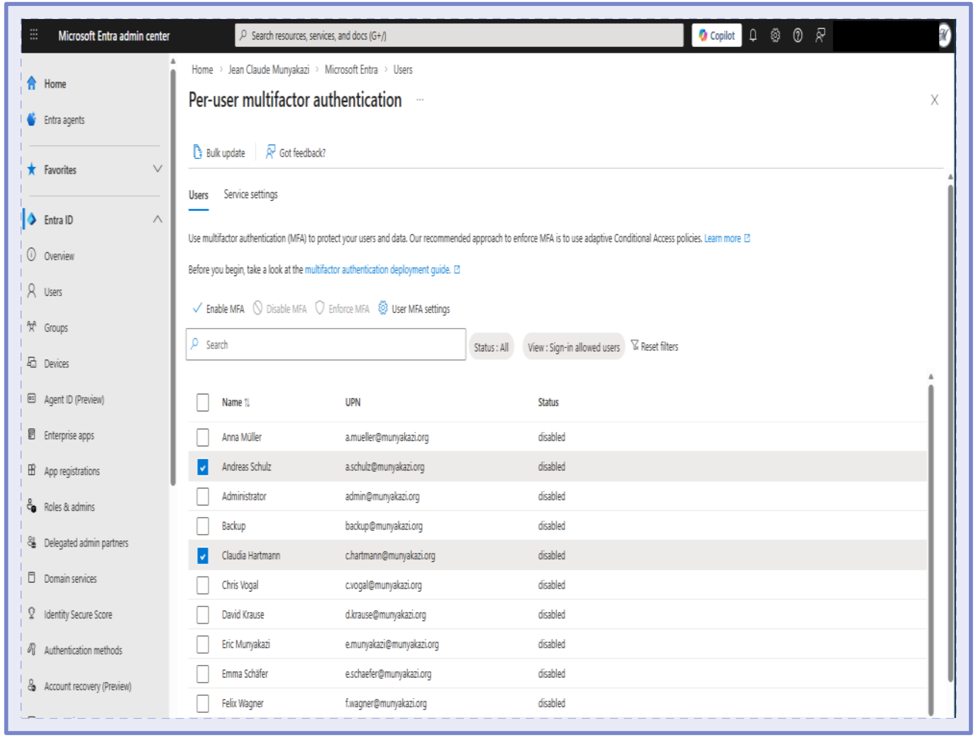
- Click the ... (More actions) menu at the top of the users list
- Select: Per-user MFA

→ **The Multi-Factor Authentication users page opens**

- (Note: this is a legacy interface - still functional)

STEP 3

Select Users to Enable



Per-user multifactor authentication

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more

Before you begin, take a look at the multifactor authentication deployment guide.

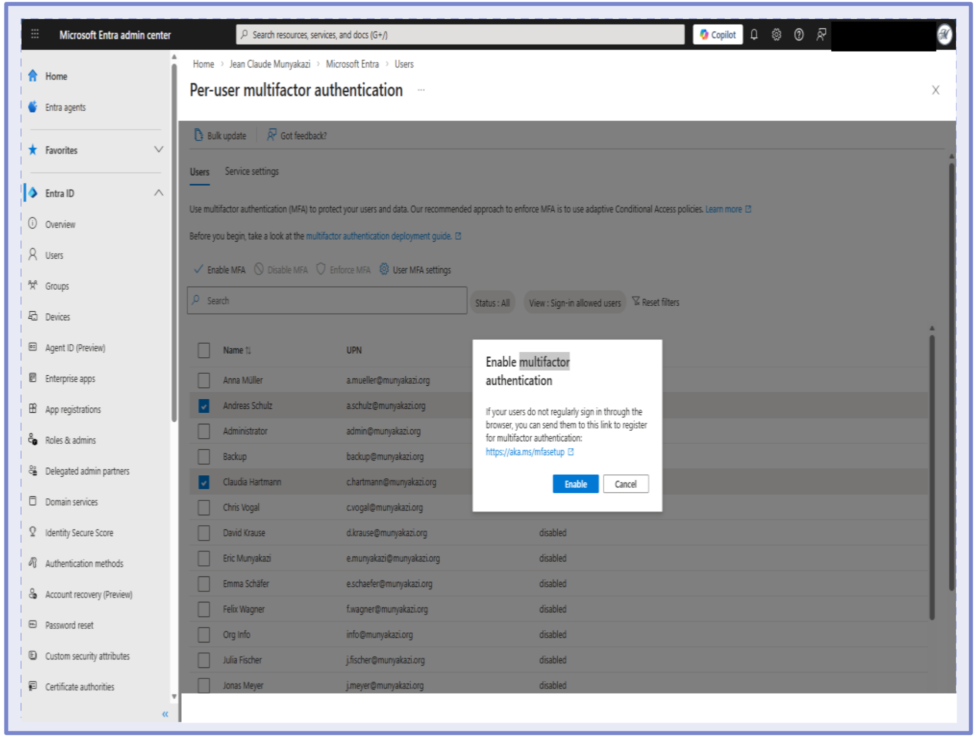
□	Name ⇅	UPN	Status
□	Anna Müller	a.mueller@munyakazi.org	disabled
☑	Andreas Schulz	a.schulz@munyakazi.org	disabled
□	Administrator	admin@munyakazi.org	disabled
□	Backup	backup@munyakazi.org	disabled
☑	Claudia Hartmann	c.hartmann@munyakazi.org	disabled
□	Chris Vogal	c.vogal@munyakazi.org	disabled
□	David Krause	d.krause@munyakazi.org	disabled
□	Eric Munyakazi	e.munyakazi@munyakazi.org	disabled
□	Emma Schäfer	e.schaefer@munyakazi.org	disabled
□	Felix Wagner	f.wagner@munyakazi.org	disabled

INSTRUCTIONS

- Tick the checkbox next to the users you want to enable
- For this demo: select Andreas Schulz and Claudia Hartmann

→ The 'quick steps' panel appears on the right side

STEP 4 Enable MFA



[redacted]

Per-user multifactor authentication

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more

Before you begin, take a look at the multifactor authentication deployment guide.

□	Name ⇅	UPN	
□	Anna Müller	a.mueller@munyakazi.org	
☑	Andreas Schulz	a.schulz@munyakazi.org	
□	Administrator	admin@munyakazi.org	
□	Backup	backup@munyakazi.org	
☑	Claudia Hartmann	c.hartmann@munyakazi.org	
□	Chris Vogal	c.vogal@munyakazi.org	
□	David Krause	d.krause@munyakazi.org	disabled
□	Eric Munyakazi	e.munyakazi@munyakazi.org	disabled
□	Emma Schäfer	e.schaefer@munyakazi.org	disabled
□	Felix Wagner	f.wagner@munyakazi.org	disabled
□	Org Info	info@munyakazi.org	disabled
□	Julia Fischer	j.fischer@munyakazi.org	disabled
□	Jonas Meyer	j.meyer@munyakazi.org	disabled

Enable multifactor authentication

If your users do not regularly sign in through the browser, you can send them to this link to register for multifactor authentication: https://aka.ms/mfasetup

Enable Cancel

INSTRUCTIONS

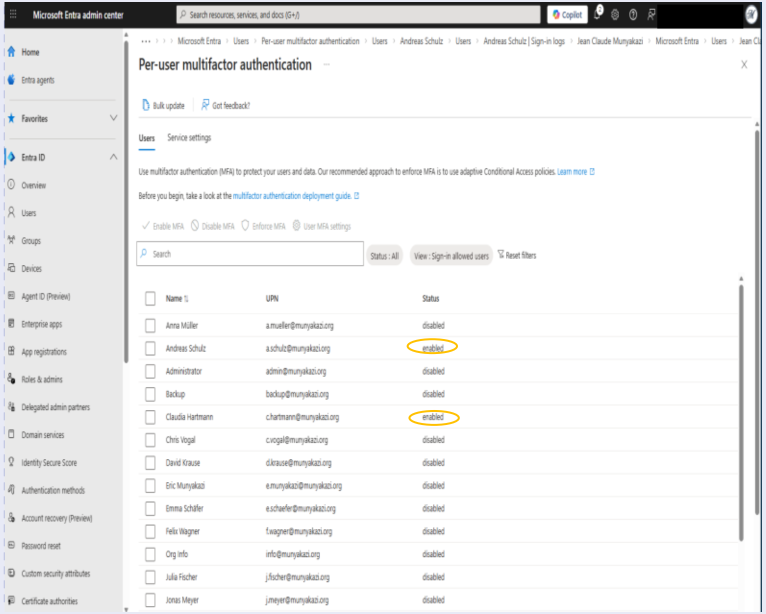
- In the quick steps panel on the right click: Enable
- A confirmation dialog appears - click enable multi-factor auth

→ MFA status for selected users changes to: Enabled

→ These users will be prompted for MFA at next sign-in

Verification Checklist

- Security Defaults shows Enabled in Entra ID → Identity → Overview → Properties
- Per-user MFA shows 'Enabled' status for select Andreas Schulz and Claudia Hartmann
- All other 21 users show MFA status as 'Not enabled' in the Per-user MFA list
- Entra ID Sign-in logs show MFA success - check Identity → Monitoring → Sign-in logs



Per-user multifactor authentication

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more

Before you begin, take a look at the multifactor authentication deployment guide.

□	Name	UPN	Status
□	Anna Müller	a.mueller@munyakazi.org	disabled
□	Andreas Schulz	a.schulz@munyakazi.org	enabled
□	Administrator	admin@munyakazi.org	disabled
□	Backup	backup@munyakazi.org	disabled
□	Claudia Hartmann	c.hartmann@munyakazi.org	enabled
□	Chris Vogal	c.vogal@munyakazi.org	disabled
□	David Krause	d.krause@munyakazi.org	disabled
□	Eric Munyakazi	e.munyakazi@munyakazi.org	disabled
□	Emma Schäfer	e.schaefer@munyakazi.org	disabled
□	Felix Wagner	f.wagner@munyakazi.org	disabled
□	Org Info	info@munyakazi.org	disabled
□	Julia Fischer	j.fischer@munyakazi.org	disabled
□	Jonas Meyer	j.meyer@munyakazi.org	disabled

Common Errors & Fixes

Error	Cause & Fix
Can't find Security Defaults	Go to: entra.microsoft.com → Identity → Overview → Properties tab → scroll to bottom
Security Defaults is greyed out	Conditional Access policies may already exist - they block Security Defaults
User not prompted for MFA	MFA may not be enforced yet - check if Security Defaults is truly Enabled and saved
Lost access to admin account	Use the emergency access (break glass) account or contact Microsoft support
Authenticator app not working	Delete the account from the app and re-register from scratch via the MFA portal
Per-user MFA option not visible	Search for 'Multi-Factor Authentication' in the Entra ID search bar at the top

What's Next

Accounts secured. Now organise them into Teams and SharePoint.

#003

Add Users to Teams & SharePoint

Assign staff to the correct Teams channels and grant SharePoint site access

20 min

#004

Set Up Conditional Access

Create security policies in Entra ID to control when and how users sign in

45 min

#005

Disable / Offboard a User

Safely remove access and block sign-in for a departing employee

20 min

All runbooks available at: munyakazi.org/m365-runbook