

# What you need to know about Microsoft Entra ID security defaults

by Elkhan Yusubov | Microsoft MVP & MCT RL



**CYBER**  
BACK TO  
SCHOOL

October 21, 2024  
8:30 PM EDT



**Elkhan Yusubov**

Speaker | Author | Architect  
Founder at #CloudMarathoner



  @ElYusubov

Elkhan is a Director of Cloud & Infrastructure, and an Architect Manager, Microsoft Azure MVP and 17+ MCT with experience in cloud solutions, enterprise healthcare systems and healthcare data, and API standards (HL7 FHIR, EDI X12).

He is an active Microsoft Tech Community Contributor, Cloud Lunch and Learn Co-organizer, Learning expert and MCT Regional Lead, and as well as a LinkedIn instructor with interests in Architecture, DevOps & Security.

He is a frequent speaker at tech meetups and has volunteered for Give Camps, Azure Data Fest, SQL Saturdays and Microsoft community events, like this one.

And please, checkout the posts at Cloud Marathoner site & LinkedIn

<https://theCloudMarathoner.com>   

# What we will cover



What is it  
and  
Why?



Enforced  
security  
defaults



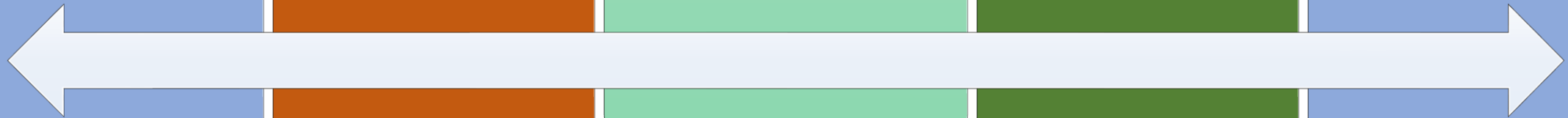
Deployment  
consideratio  
ns



Entra  
Admin  
Demo



Q&A



# What we do; where we do it

## IT Engineering Services

Agile Transformation  
Cloud Adoption &  
Infrastructure Optimization  
Cybersecurity  
Data Engineering & Analytics



Defense Health  
Agency



ICE



Intel Community



USAF



US TRANSCOM



Defense  
Information  
Systems Agency

## Customer Experience

Technology Adoption  
Release Management  
Communications Management  
Change Management



General Services  
Administration



Education



IRS

Treasury

United States<sup>®</sup>  
Census  
Bureau

## Health IT

EHR Strategy & Management  
HIPAA Compliance  
Healthcare System Integration & Testing  
Patient Experience Enhancement

## Company Info

- Established: 1999
- Legal Structure: LLC
- Headquarters: Bethesda, MD
- SDVOSB Joint Ventures
- CMMI-DEV & SVC Level 3 v2.0
- ISO 9001; ISO27001; ISO20000

### Prime Vehicles/BPAs:

- GSA MAS HACS SIN
- GSA MAS Cloud SIN
- GSA MAS IT Svcs SIN
- COBRA OTA
- CIO-SP3 Small Business
- 8(a) STARS III via MPJV
- GSA MAS HACS SB & Cloud SIN SB via MPJV

Silver  
Microsoft  
Partner

Silver Datacenter  
Silver Data Analytics  
Silver Data Platform  
Silver App Dev  
Silver App Integration

aws partner  
network  
  
Select  
Consulting  
Partner



T-Rex has donated **over \$3.5M** in support of underserved youth, veterans, and local organizations.

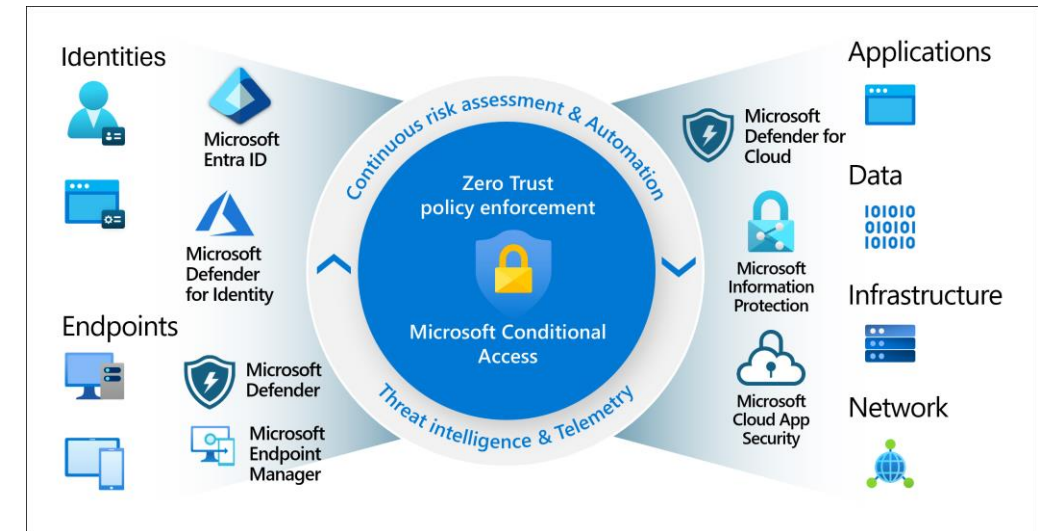
# What are the Security defaults on Entra ID?

- Security can be difficult
- Prevent common identity-related attacks
- Basic level of security
- Blocking legacy authentication protocols
- Protecting privileged activities



# Who is it for?

- Increase security posture
- Initial guidance to start securing the env.
- Relay on free tier of Microsoft Entra ID
- Need Conditional Access?





# Enabling security defaults



Microsoft Entra admin center

Search resources, services, and docs (G+/)

Home > Main Directory > Users > [redacted] > Users | User settings >

## Main Directory

+ Add Manage tenants What's new Preview features Got feedback?

Overview Monitoring **Properties** Recommendations Setup guides

Name: Main Directory

Country or region: United States

Data location: United States datacenters

Notification language: English

Tenant ID: [redacted]

Technical contact: [redacted]

Global privacy contact: [redacted]

Privacy statement URL: [redacted]

Access management for Azure resources

[redacted] can manage access to all Azure subscriptions and management groups in this tenant.

[Learn more](#)

☒ Yes

### Security defaults

Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will be automatically enforced in your organization. Administrators and users will be prompted to use multifactor authentication when logging in. [Learn more](#)

✓ Your organization is protected by security defaults. [Manage security defaults](#)

### Security defaults

Security defaults

Enabled (recommended)

Enabled (recommended)

Disabled (not recommended)

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.



# Enforced security defaults

Require	Require all users to register for Microsoft Entra multifactor authentication
Require	Require administrators to do multifactor authentication
Require	Require users to do multifactor authentication when necessary
Block	Block legacy authentication protocols
Protect	Protect privileged activities like access to the Azure portal



# Deployment considerations



Preparing your users

Authentication methods

B2B users

Disabled MFA status

Disabling security defaults

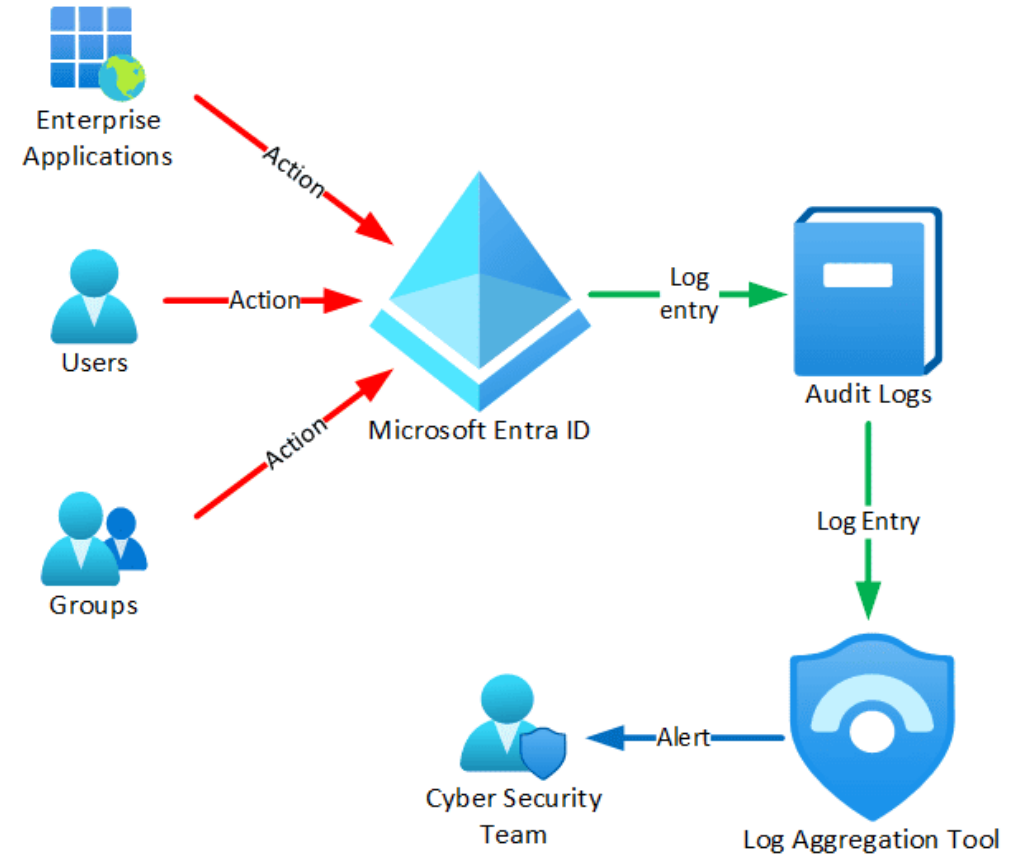
# Comparing Security Defaults to Conditional Access

	Security defaults	Conditional Access
Required licenses	None	At least Microsoft Entra ID P1
Customization	No customization (on or off)	Fully customizable
Enabled by	Microsoft or administrator	Administrator
Complexity	Simple to use	Fully customizable based on your requirements

## Demo:

# Microsoft Entra ID – Security defaults and settings

- Microsoft Entra Admin center
- User Settings
- Group settings
- Device settings



# Learning resources Microsoft Entra & Security defaults

- [Security Defaults in Microsoft Entra ID](#)
- [Improve your security posture](#)
- [Emergency access accounts](#)
- [Enable MFA](#)
- [Identity secure score](#)
- [Azure Security Benchmark \(ASB\)](#)



# Applied Skills – hands on practices



## Filter

[Clear all](#)

### Products

Find a product

- ☒ .NET
- ☒ Azure
  - ☐ Microsoft Copilot
- ☒ Microsoft Defender
- ☒ Microsoft Entra
  - ☐ Microsoft Fabric
  - ☐ Microsoft Graph
- ☒ Microsoft Power Platform
  - ☐ Microsoft Teams

### Roles

- ☐ Administrator
- ☐ AI Engineer
- ☐ App Maker
- ☐ Data Analyst
- ☐ Data Engineer

Search

Search

Applied Skills ✕

27 results

Sort by: Alphabetical (A-Z) ▾

APPLIED SKILLS

**Administer Active Directory Domain Services**

Windows • Administrator • Intermediate

Add

APPLIED SKILLS

**Build a natural language processing solution with Azure AI Language**

Azure • AI Engineer • Intermediate

Add

APPLIED SKILLS

**Build an Azure AI Vision solution**

Azure • Developer • Intermediate

Add

APPLIED SKILLS

**Build collaborative apps for Microsoft Teams**

Microsoft Teams • Developer • Intermediate

Add

APPLIED SKILLS

**Configure SIEM security operations using Microsoft Sentinel**

Azure • Security Engineer • Intermediate

Add

APPLIED SKILLS

**Configure secure access to your workloads using Azure networking**

Azure • Administrator • Intermediate

Add

APPLIED SKILLS

**Create an intelligent document processing solution with Azure AI Document Intelligence**

Azure • Developer • Intermediate

Add

APPLIED SKILLS

**Create and manage automated processes by using Power Automate**

Microsoft Power Platform • Administrator • Intermediate

Add



# What we covered



What is it  
and Why?



What  
security  
policies  
used?



Deployme  
nt  
considerat  
ions



Entra  
Admin  
demo



Q&A





# Thank you !



<https://cyberbacktoschool.com/>

**Elkhan Yusubov**  
Speaker | Author | Cloud Architect  
Founder at #cloudmarathoner

<https://theCloudMarathoner.com>   