

A decorative background featuring a network diagram with nodes and connecting lines. The nodes are represented by circles of varying sizes and colors (blue, grey, and white), and the lines are thin and grey. The network is distributed across the top-left and bottom-right corners of the image.

Identity Security

Azure Active Directory

A decorative graphic in the top-left corner consisting of a network of interconnected nodes and lines, rendered in light gray. The nodes are represented by small circles, some of which are solid and others are hollow with a dot inside. The lines are thin and connect the nodes in a complex, web-like pattern.

Hello!

I am Eng Teong Cheah

Microsoft MVP

A decorative network diagram in the top-left corner, featuring a complex web of interconnected nodes and lines. The nodes are represented by circles of varying sizes, some with concentric rings, and the lines are thin and grey. The diagram is partially cut off by the left edge of the frame.

Azure Active Directory

A decorative network diagram in the bottom-right corner, similar to the one in the top-left. It shows a cluster of nodes and connecting lines, with some nodes having concentric circles. The diagram is also partially cut off by the right edge of the frame.

Azure Active Directory(AD)

Microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources in:

- ◎ External resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications.
- ◎ Internal resources, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization.

Azure AD vs Active Directory

Azure AD

- ◎ Cloud
- ◎ Designed for HTTP & HTTPS
- ◎ Queried via REST API's
- ◎ Uses SAML, WS-Federation, or OpenID for authentication
- ◎ Uses OAuth for authentication

Includes federation services

Flat Structure

Active Directory

- ◎ On-Premises
- ◎ Query via LDAP
- ◎ Used Kerberos for Authentication
- ◎ No Federated Services
- ◎ Organizational Units(OU;s)
- ◎ Group Policy (GPO's)

Roles for Azure AD

Global Administrator

Users with this role have access to all administrative features in Azure Active Directory

Directory Reader

Makes purchases, manage subscriptions, manages support tickets, and monitors service health

Security Administrator

Users with this role have permissions to manage security-related features in the Microsoft 365 Security Center, Security Center, Azure Active Directory Identity Protection, Azure Information Protection and Office 365 Security & Compliance Center.

Global Reader

Users in this role can read settings and administrative information across Microsoft 365 services but can't take management actions.



Azure AD Domain Services (Azure AD DS)










Provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos / NTLM authentication that is fully compatible with Windows Server Active Directory.

Azure AD Users

All users must have an account

The account is used for authentication and authorization

Types of users: Azure AD, Active Directory, Guest, B2C, and B2B

Users - All users microsoft - Azure Active Directory					
<div>Search (Ctrl+/) «</div> <div><div>+ New user</div><div>+ New guest user</div><div>Reset password</div><div>Delete user</div><div>Multi-Factor Authentication</div><div>Refresh</div><div>Columns</div></div>					
NAME		USER NAME		USER TYPE	SOURCE
	Retail Crisis Notifications		@microsoft.com	Member	Windows Server AD
	"Planning & Launch Services OEM Inquiries		@microsoft.com		Windows Server AD
	' Bert		@hotmail.com	Guest	Azure Active Directory
	 @fi.pwc.com		@fi.pwc.com	Guest	Azure Active Directory

Azure AD Groups

Group Types

- Security groups
- Office 365 groups

Assignment Types

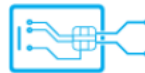
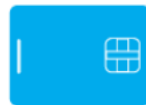
- Assigned
- Dynamic User
- Dynamic Device (Security groups only)

Users and groups - All groups

<input type="text" value="Search (Ctrl+/)"/>		<input type="text" value="Search groups"/>	
Overview			
MANAGE			
All users			
All groups			
NAME	GROUP TYPE	MEMBERSHIP TYPE	
GR Group1	Security	Assigned	
GR Group2	Security	Assigned	
GR Group23	Security	Assigned	

Azure MFA Concepts

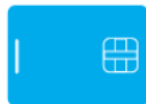
Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan.



Azure MFA Concepts

Authentication methods include:

- ◎ Something you know (typically a password)
- ◎ Something you have (a trusted device that is not easily duplicated, like phone)
- ◎ Something you are (biometrics)



Enabling MFA

Select the users that you want to modify and enable for MFA

User states can be Enabled, Enforced, or Disabled

On first-time sign-in, after MFA has been enabled, users are prompted to configure their MFA settings

Azure MFA is included free of charge for global administrator security

contoso

admin@cms

multi-factor authentication

users

service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users. Before you begin, take a look at the [multi-factor auth deployment guide](#).

View:

Sign-in allowed users

 Multi-Factor Auth status:

Any

bulk update

<input type="checkbox"/>	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
<input checked="" type="checkbox"/>	Adam Barr	AdamB@contoso.com	Disabled
<input checked="" type="checkbox"/>	Alice Ciccu	AliceC@contoso.com	Disabled
<input type="checkbox"/>	Amy Rusko	AmyR@contoso.com	Disabled
<input type="checkbox"/>	Ann Beebe	AnnB@contoso.com	Disabled
<input checked="" type="checkbox"/>	Ben Smith	BenS@contoso.com	Disabled

3 selected

quick steps

Enable

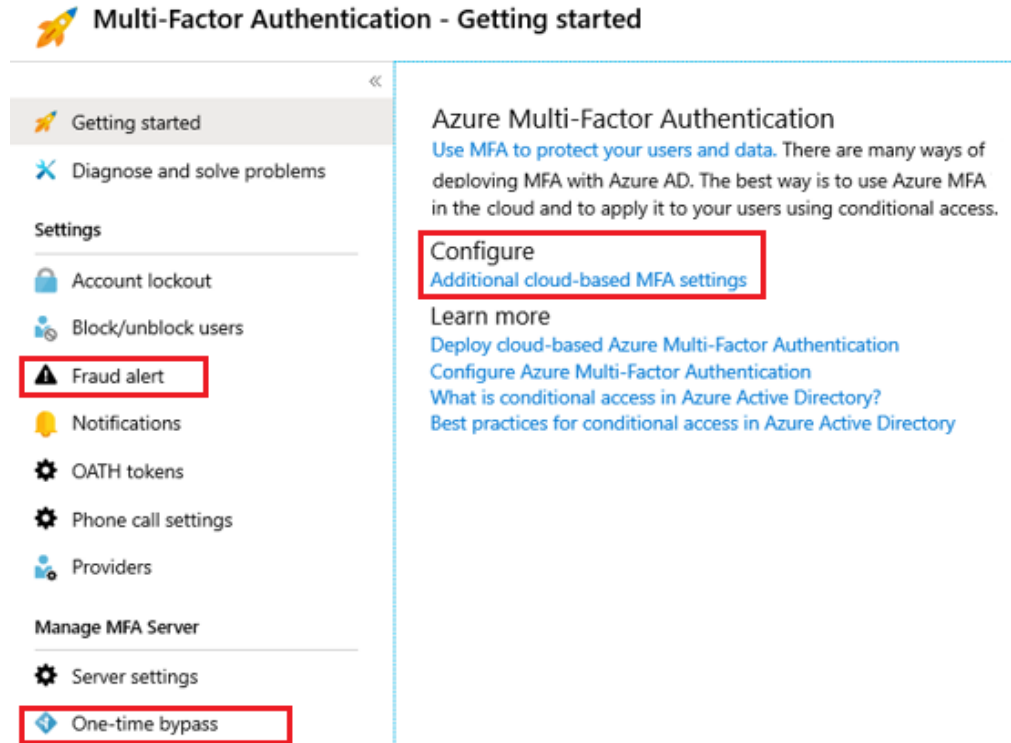
Manage user settings


MFA Settings

Trusted IPs – Allows federated users or IP address ranges to bypass two-step authentication


One-time Bypass – Allows a user to authenticate a single time without performing two-step verification


Fraud Alerts – Users can report fraudulent attempts to access their resources




 **Multi-Factor Authentication - Getting started**


«


 Getting started


 Diagnose and solve problems


Settings


 Account lockout


 Block/unblock users

 **Fraud alert**


 Notifications


 OATH tokens

 Phone call settings

 Providers

Manage MFA Server

 Server settings

 **One-time bypass**

Azure Multi-Factor Authentication

[Use MFA to protect your users and data.](#) There are many ways of deploying MFA with Azure AD. The best way is to use Azure MFA in the cloud and to apply it to your users using conditional access.

Configure

[Additional cloud-based MFA settings](#)

Learn more

[Deploy cloud-based Azure Multi-Factor Authentication](#)

[Configure Azure Multi-Factor Authentication](#)

[What is conditional access in Azure Active Directory?](#)

[Best practices for conditional access in Azure Active Directory](#)

Demonstrations

Role-Based Access Control



Thanks!

Any questions?

You can find me at:
[@walkercet](#)

References

© <https://docs.microsoft.com/en-us/>