Identity Security
Azure Active Directory

Hello!

I am Eng Teong Cheah

Microsoft MVP

Azure Active Directory

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

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.

Directory Reader

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

Global Reader

Useers 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)

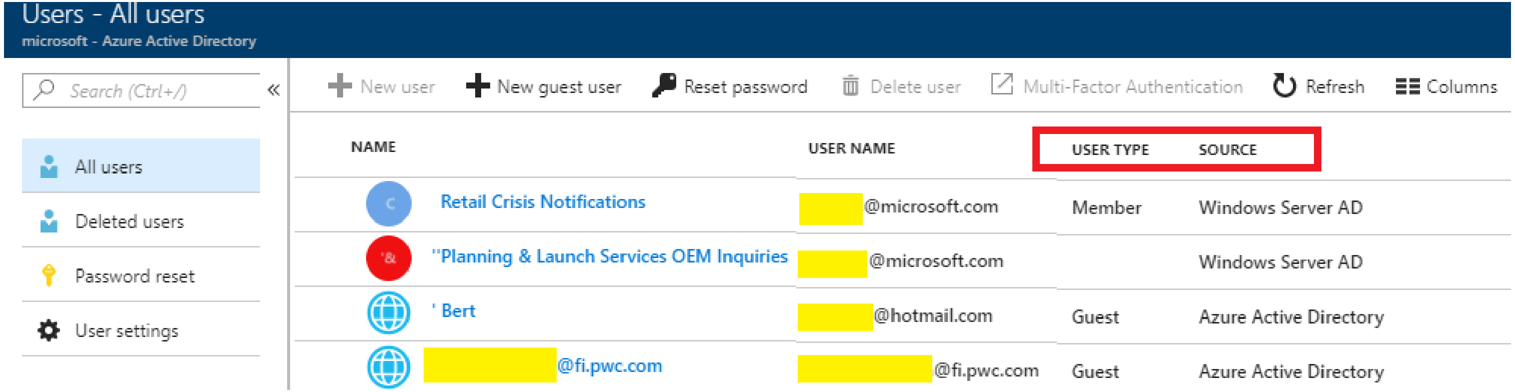
Provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos / NTLM authentication that is fully compatible with Windows Server Active Directory.

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

NAME	USER NAME	USER TYPE	SOURCE
Retail Crisis Notifications	[redacted]@microsoft.com	Member	Windows Server AD
"Planning & Launch Services OEM Inquiries	[redacted]@microsoft.com		Windows Server AD
' Bert	[redacted]@hotmail.com	Guest	Azure Active Directory
[redacted]@fi.pwc.com	[redacted]@fi.pwc.com	Guest	Azure Active Directory

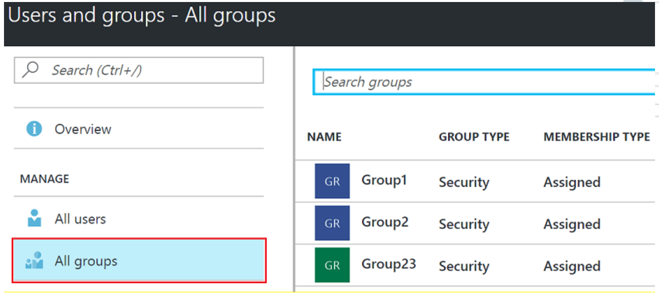
Azure AD Groups

Group Types

- Security groups
- Office 365 groups

Assignment Types

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



Users and groups - All groups

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)

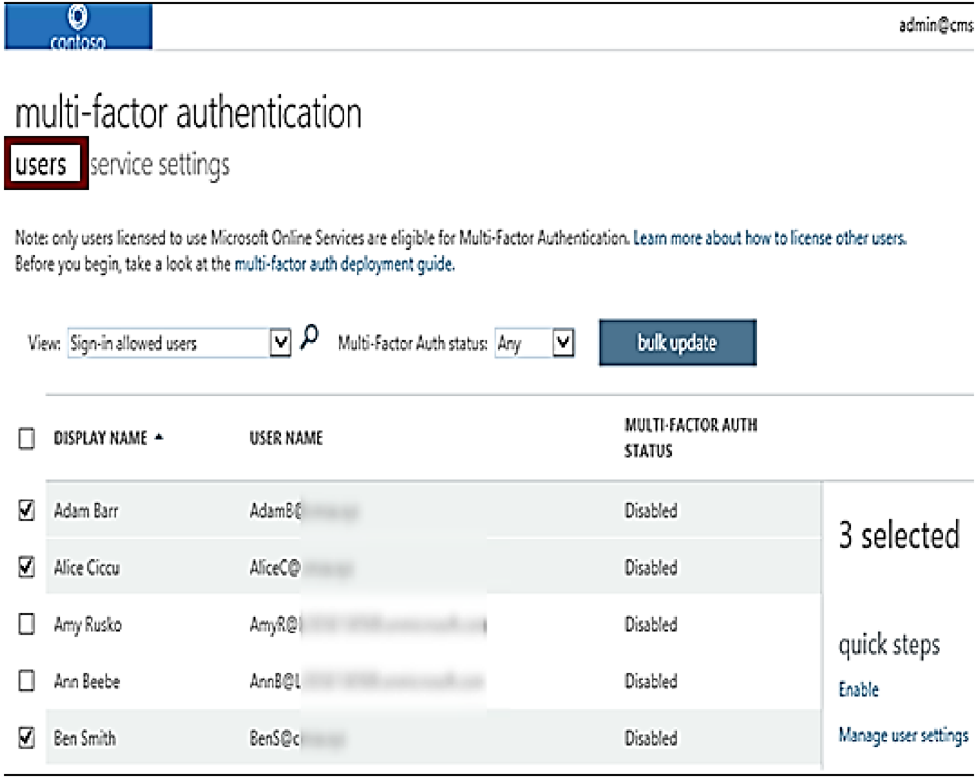
Enabling MFA

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



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

□	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
☑	Adam Barr	AdamB@[redacted]	Disabled
☑	Alice Ciccu	AliceC@[redacted]	Disabled
□	Amy Rusko	AmyR@[redacted]	Disabled
□	Ann Beebe	AnnB@[redacted]	Disabled
☑	Ben Smith	BenS@[redacted]	Disabled

3 selected

quick steps

Enable

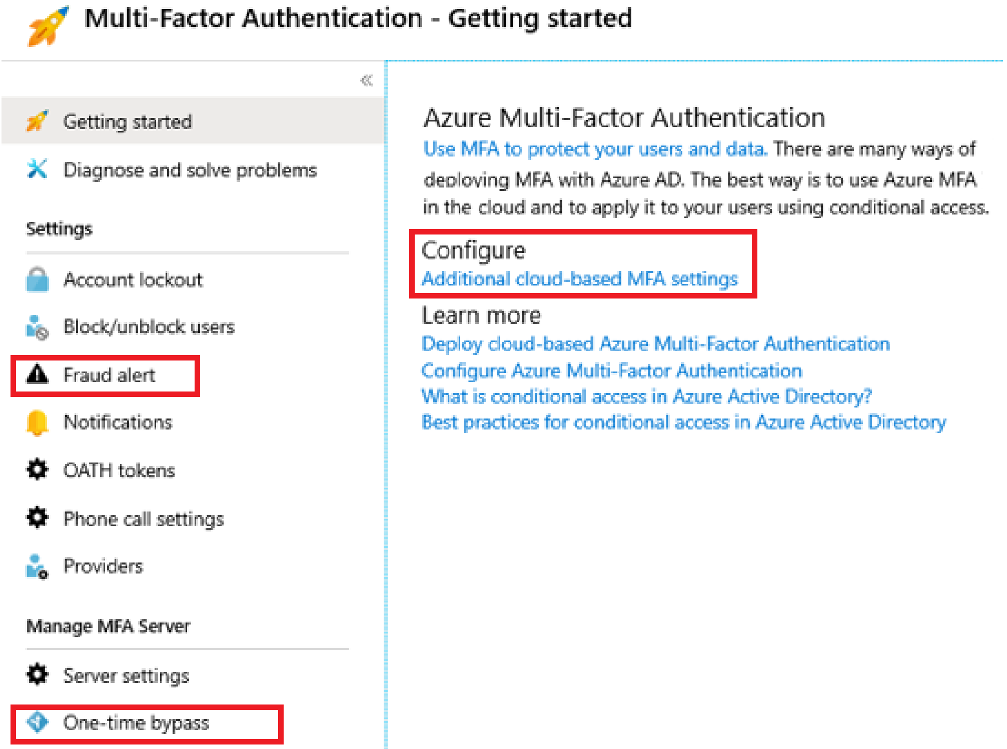
Manage user settings

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 fraudlent attempts to access their resources



Multi-Factor Authentication - Getting started

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

Demostrations

Role-Based Access Control

Thanks!

Any questions?

You can find me at:

@walkercet

References

- https://docs.microsoft.com/en-us/