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 Object(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)

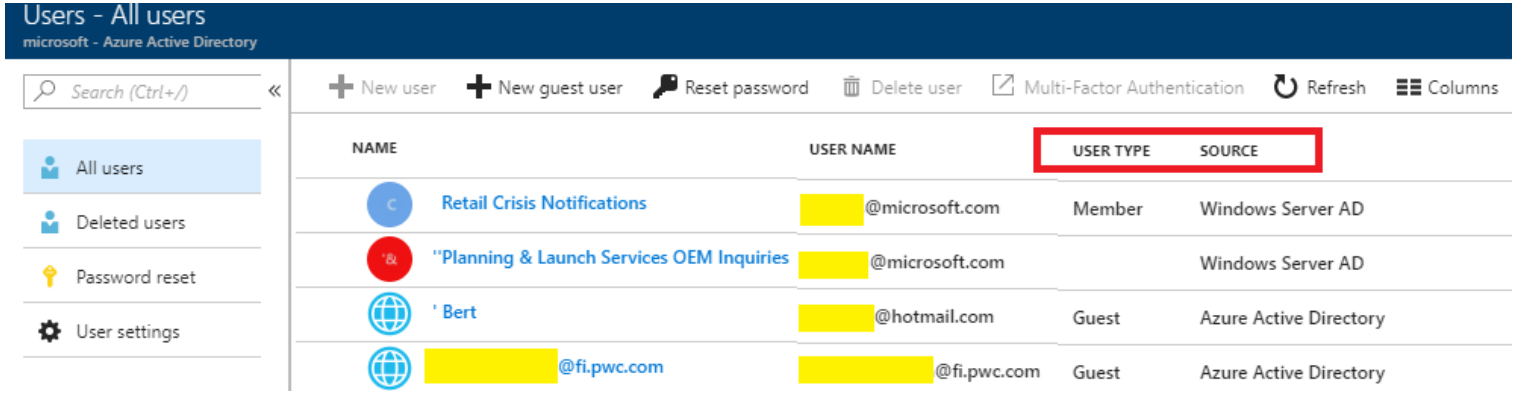
Provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos / NTLM authentication that is fully compatible with Windows Server Active Directory.

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



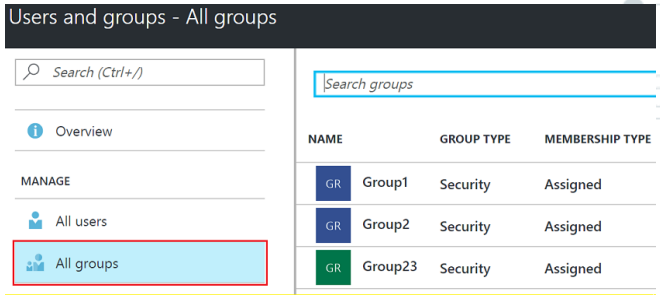
Azure AD Groups

Group Types

- Security groups
- Office 365 groups

Assignment Types

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



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)

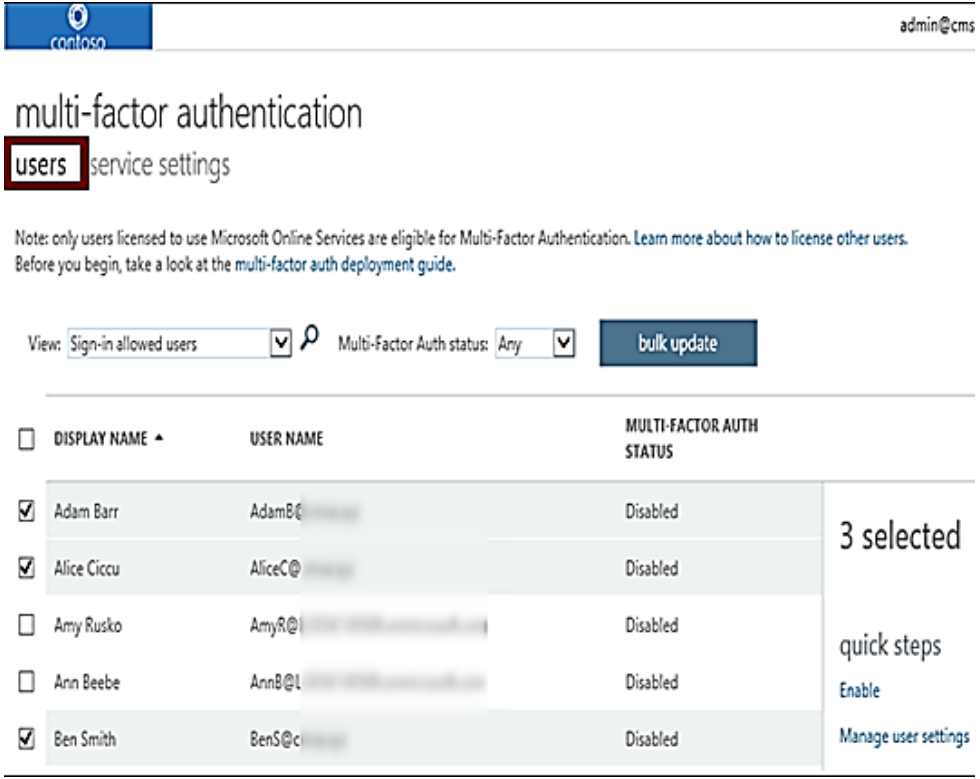
Enabling MFA

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

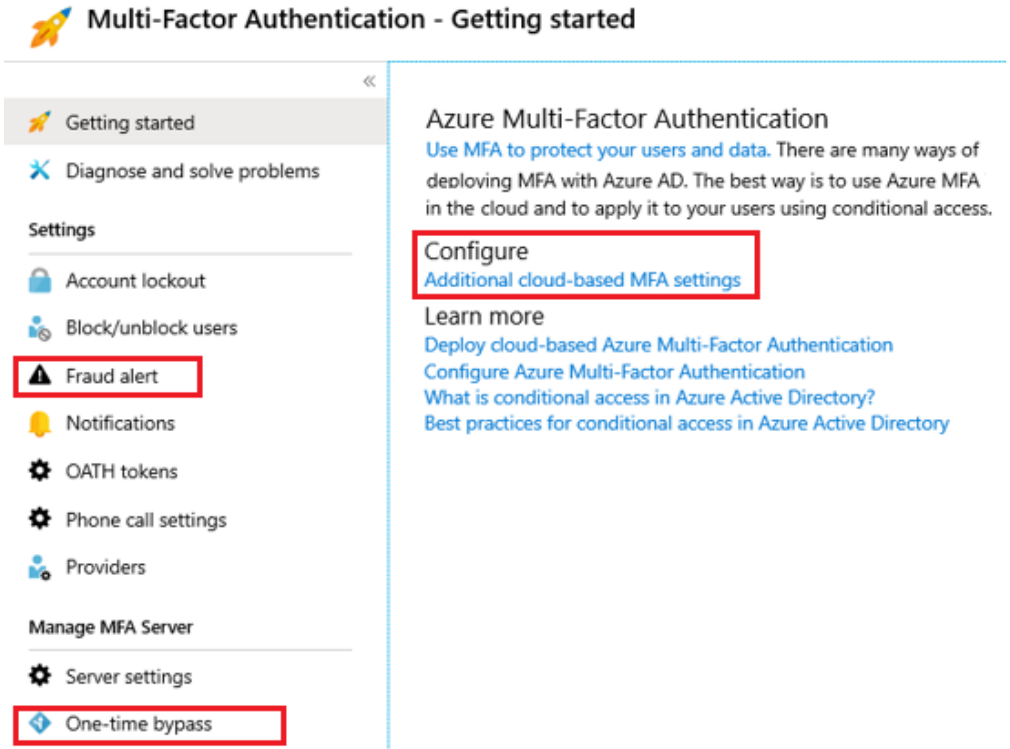


MFA Settings

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



Demostrations

Role-Based Access Control

Thanks!

Any questions?

You can find me at:

@walkercet

References

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