Module 18:

Azure Active Directory

What is Active Directory ?

- Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management. Starting with Windows Server 2008, however, Active Directory became an umbrella title for a broad range of directory-based identity-related services.

- It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software.

Active Directory - Example

- When a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user.

- Also, it allows management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services

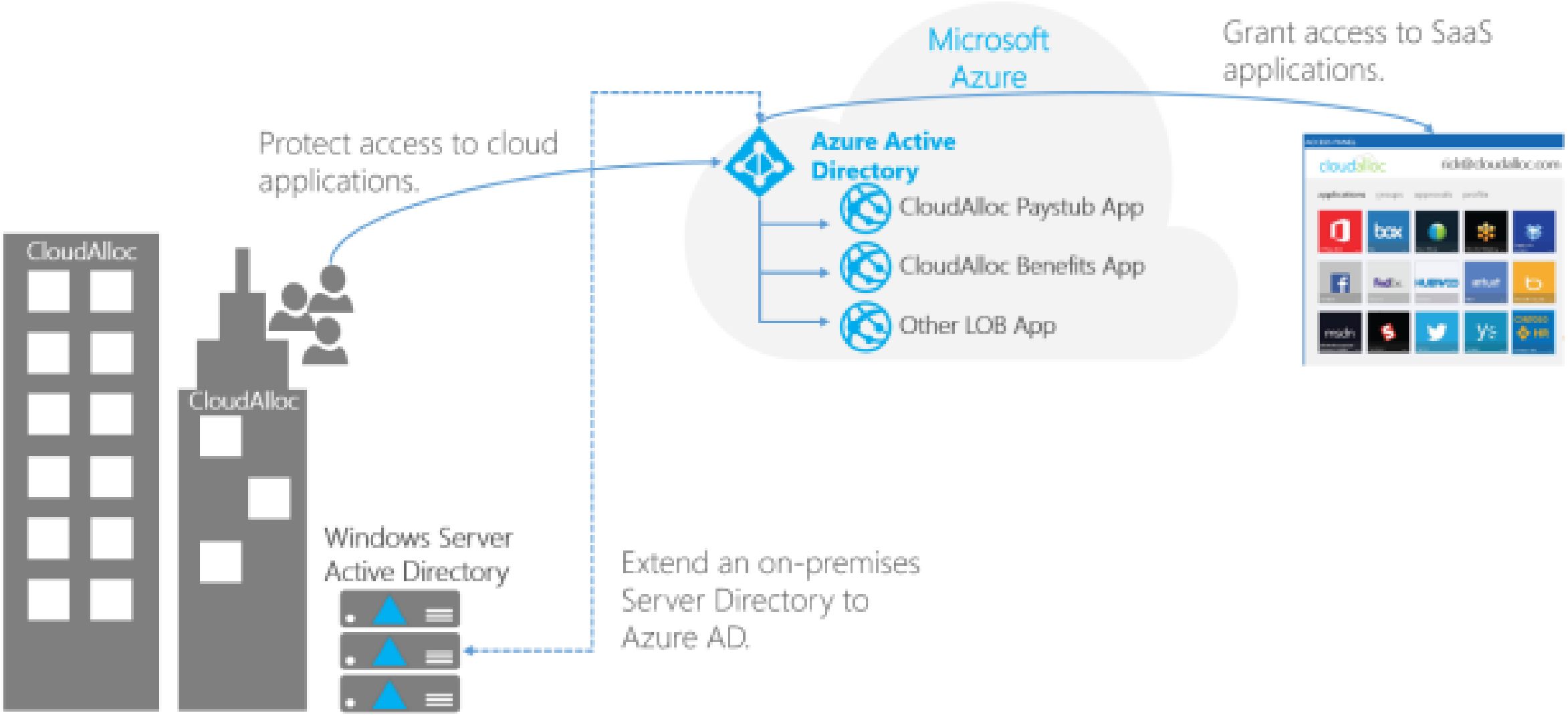
What is Azure Active Directory ?

- Azure Active Directory (aka Azure AD) is a fully managed multi-tenant service from Microsoft that offers identity and access capabilities for applications running in Microsoft Azure **and** for applications running in an on-premises environment.

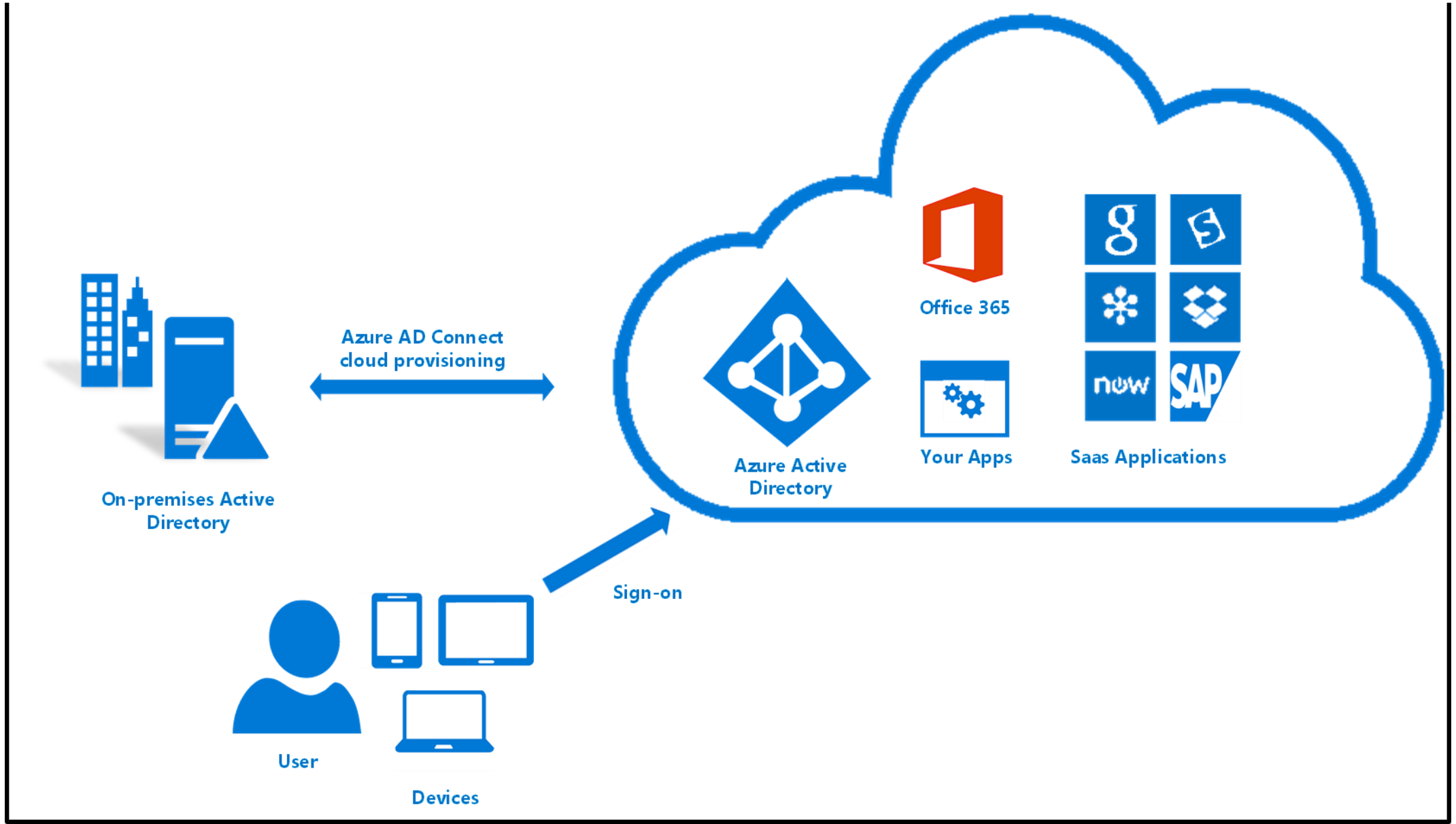
- It is a cloud service that provides administrators with the ability to manage end user identities and access privileges.

- The service gives administrators the freedom to choose which information will stay in the cloud, who can manage or use the information, what services or applications can access the information and which end users can have access.

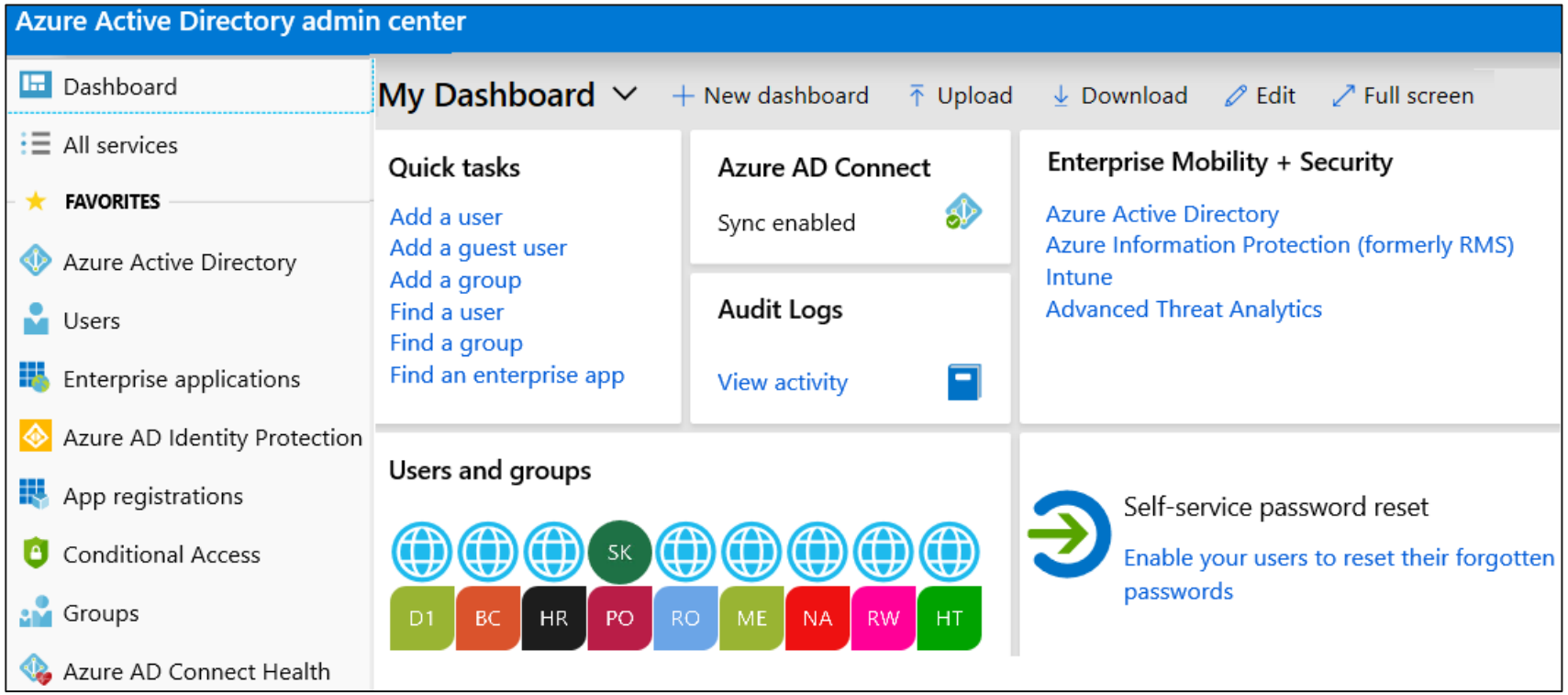
Azure Active Directory



Azure Active Directory



Azure Active Directory

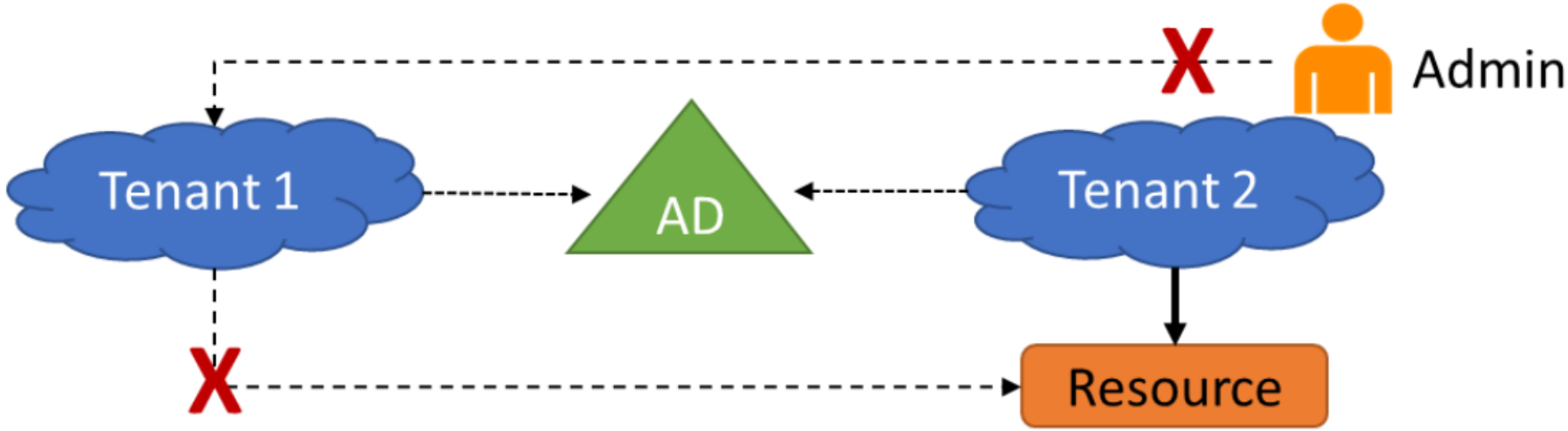


- A full suite of identity management capabilities including multi-factor authentication, device registration, self-service password management, privileged account management, RBAC, monitoring, auditing, and alerting

Azure Active Directory Editions

Feature	Free	Office 365 Apps	Premium P1	Premium P2
Directory Objects	500,000 objects	No object limit	No object limit	No object limit
Single Sign-On	Up to 10 apps	Up to 10 apps	Unlimited	Unlimited
Core Identity and Access	X	X	X	X
B2B Collaboration	X	X	X	X
Identity & Access for O365		X	X	X
Premium Features			X	X
Hybrid Identities			X	X
Advanced Group Access			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

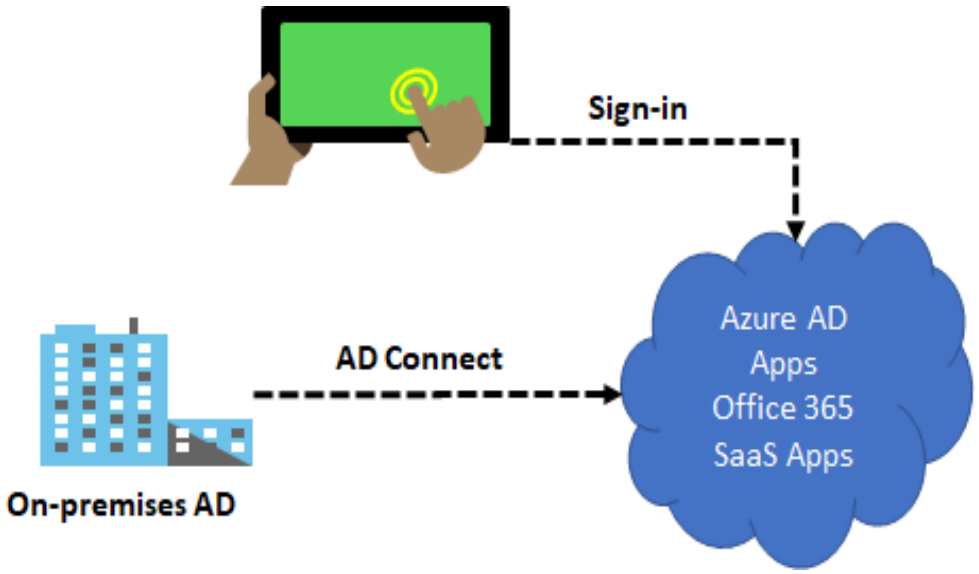
Azure AD Directories (Tenants)



- A tenant is a dedicated instance of an Azure AD directory
- You can have multiple tenants for:
  - Resource independence
  - Administrative independence
  - Synchronization independence

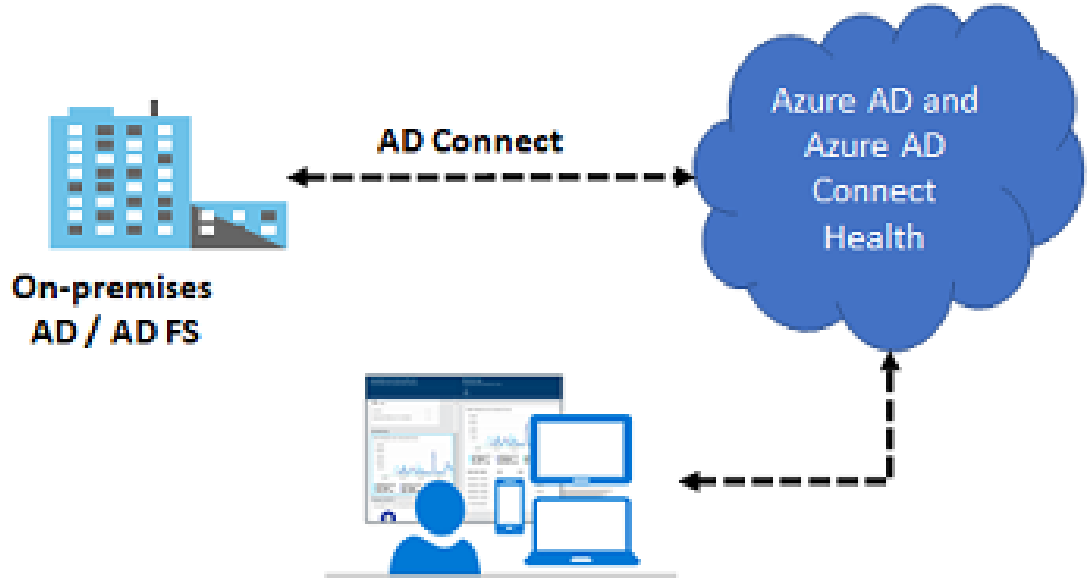
Azure AD Connect

- Integrate your on-premises directories with Azure Active Directory
- Provides a common identity for your users for Office 365, Azure, and SaaS applications integrated with Azure AD
- There are several authentication options
- Enables hybrid identity



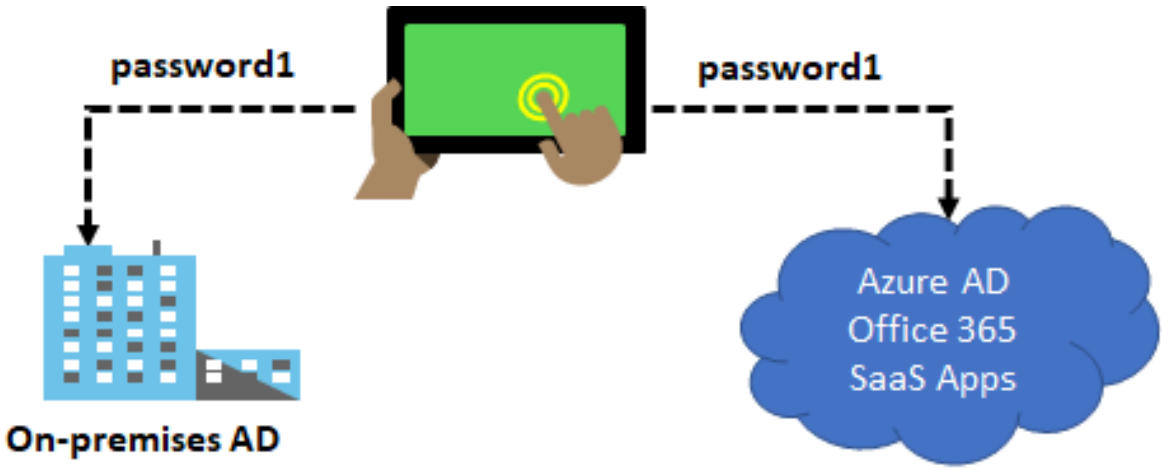
Azure AD Connect Health

- Monitor and gain insights into AD FS servers, Azure AD Connect, and AD domain controllers
- Monitor and gain insights into the synchronizations that occur between your on-premises AD DS and Azure AD
- Monitor and gain insights into your on-premises identity infrastructure that is used to access Office 365 or other Azure AD applications



Password Hash Synchronization

- Password hash synchronizes user passwords from on-premises Active Directory to cloud-based Azure AD
- Sign in to Azure AD services using the on-premises password
- Improve the productivity of your users and reduce your helpdesk costs

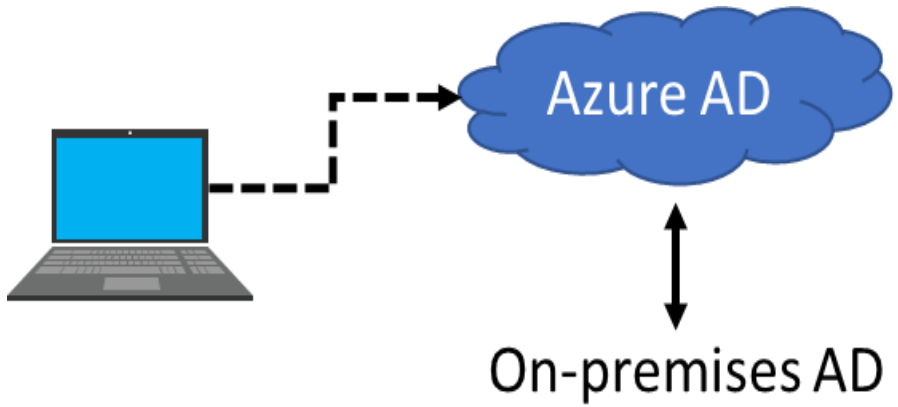


Device Management

- Azure AD enables SSO to devices from anywhere (BYOD)
- Registering a device
  - Enable a registered device to authenticate when the user signs-in
  - Disable the device, as needed
- Joining a device
  - Extends a registered device - all the benefits of registration
  - Changes the local state of device
  - Sign-in using an organizational work or school account instead of a personal account

Azure AD Joined Devices

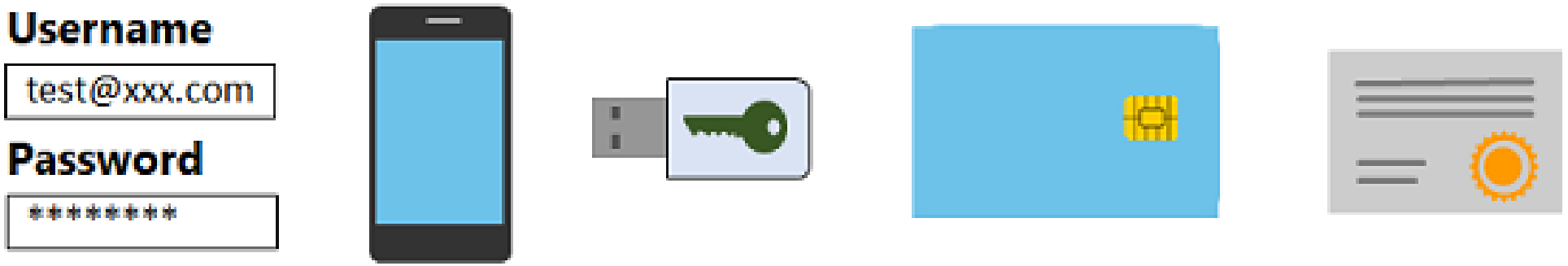
- Single-Sign-On (SSO) to your Azure managed SaaS apps and services
- Enterprise compliant roaming of user settings across joined devices
- Access to Windows Store for Business
- Windows Hello support
- Restriction of access to apps from only compliant devices
- Seamless access to on-premise resources



Multi-Factor Authentication (MFA) Overview

- Azure Multi-Factor Authentication (MFA) helps safeguard access to data and applications while maintaining simplicity for users. It provides additional security by requiring a second form of authentication and delivers strong authentication via a range of easy to use authentication methods. Users may or may not be challenged for MFA based on configuration decisions that an administrator makes.

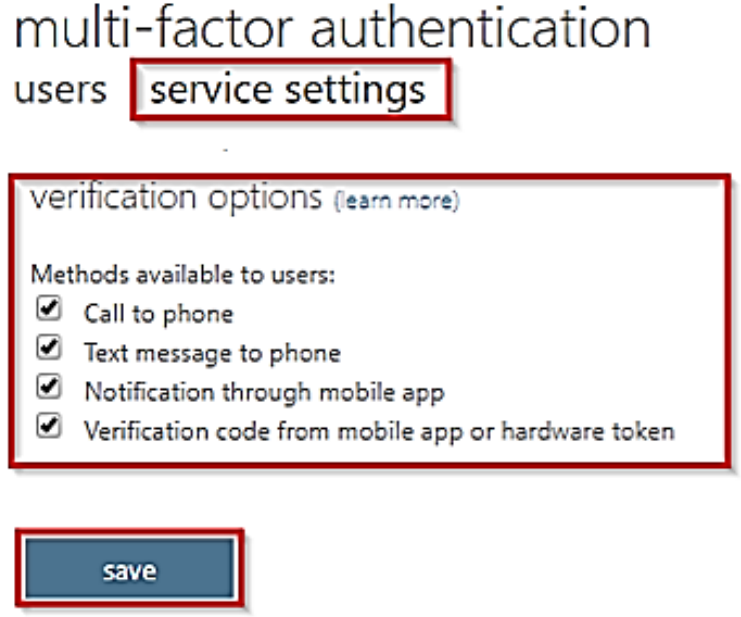
Azure MFA Concepts



- The security of MFA two-step verification lies in its layered approach
- Authentication methods include:
  - Something you know (typically a password)
  - Something you have (a trusted device that is not easily duplicated, like a phone)
  - Something you are (biometrics)

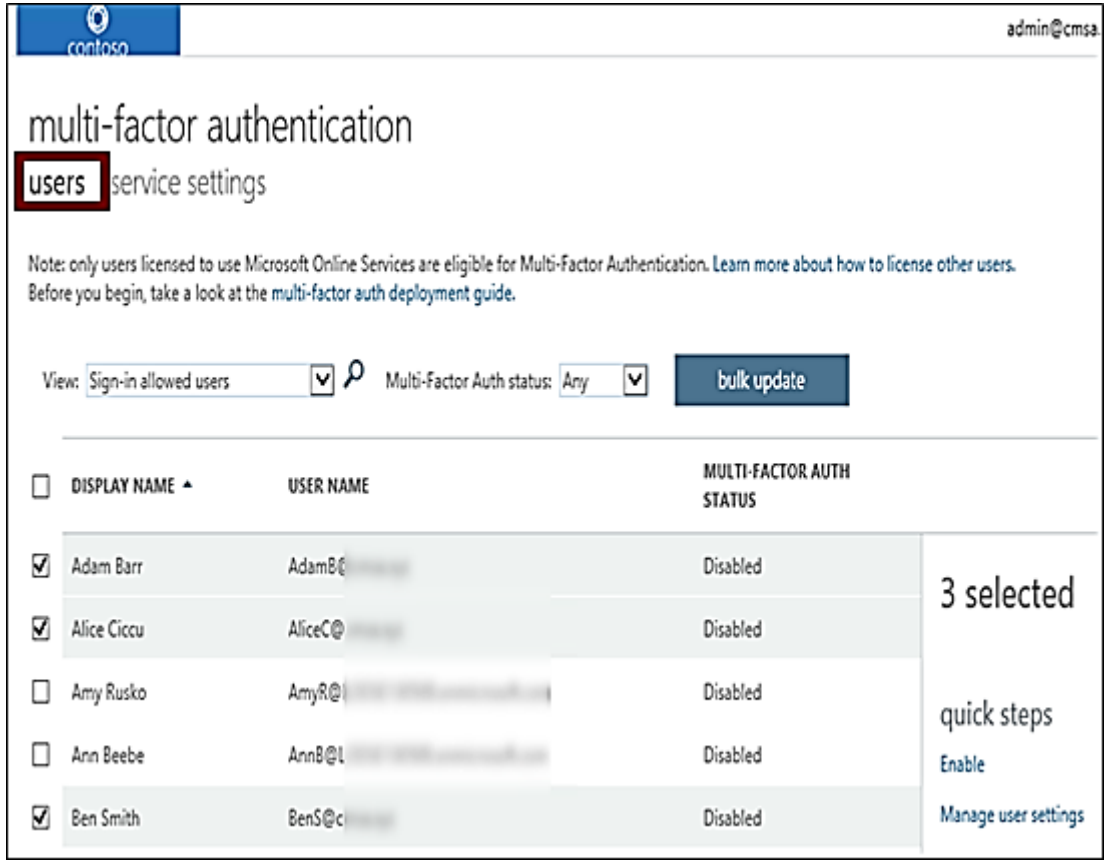
MFA Authentication Options

- **Phone Call** - automated
- **Text Message** - A six-digit code is sent to the user's cell phone
- **Mobile App Notification** – push notification
- **Mobile app verification code** - A six-digit code is sent to the user mobile app

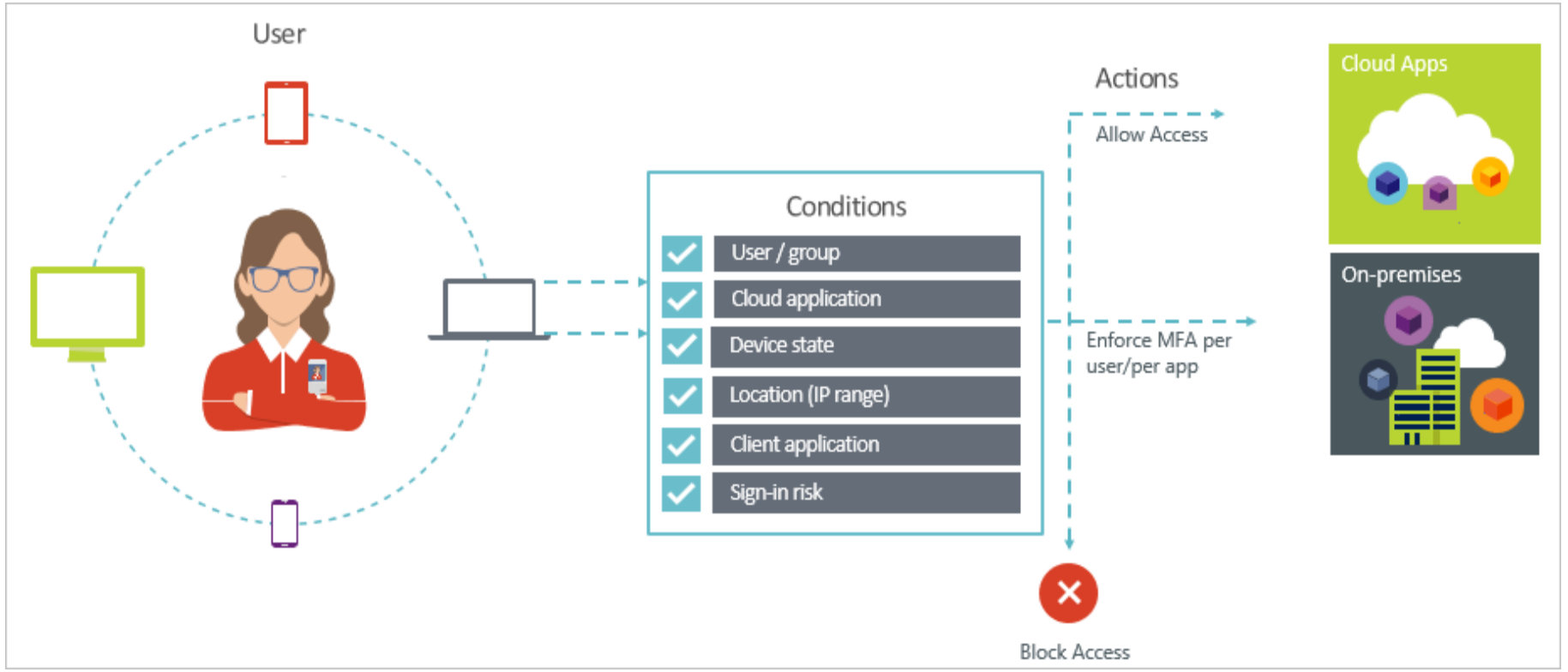


Enabling MFA

- Select the users that you want to modify and enable for MFA
- Can also bulk enable groups of users with PowerShell
- 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



Requiring MFA



Conditions – "When this happens"

Access controls – "Then do this"

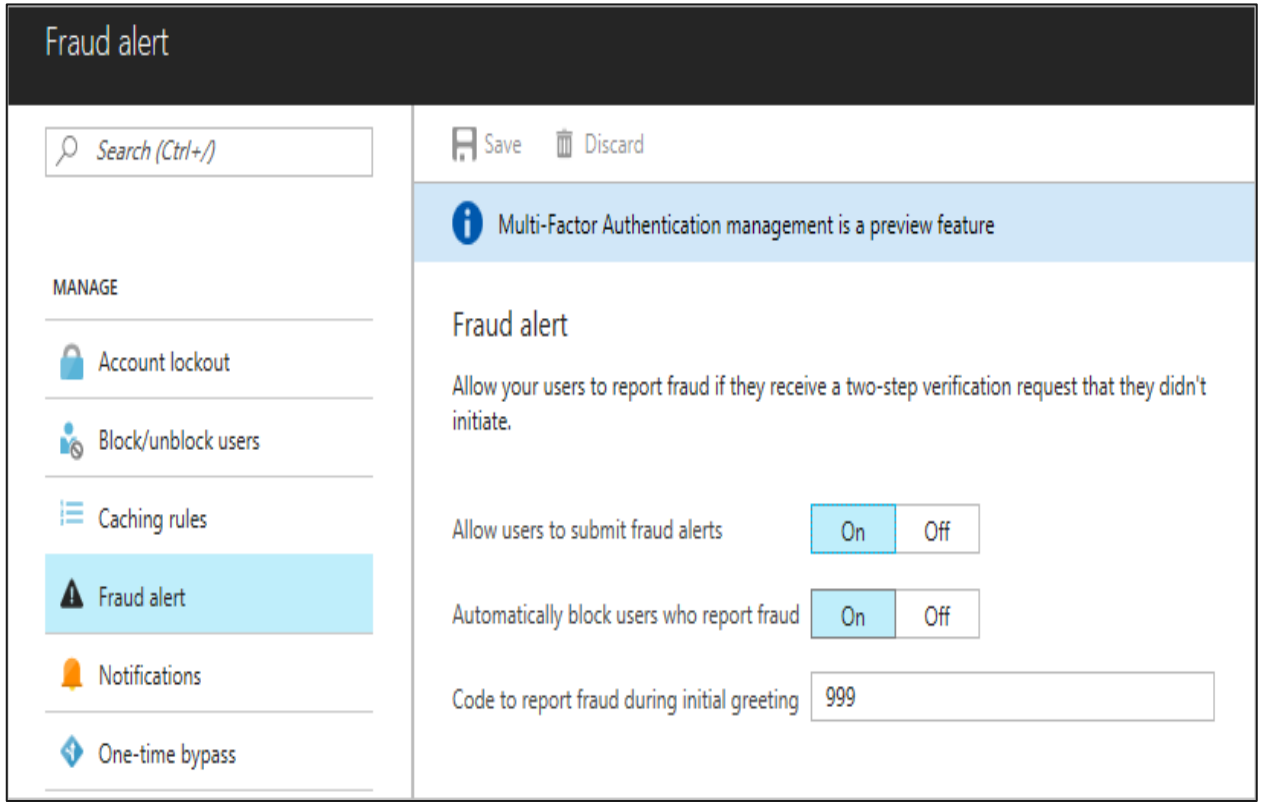
- Lets you enforce controls on access to apps based on specific conditions
- The combination of your conditions with your access controls represents a conditional access policy

Trusted IPs

- Allows federated users or IP address ranges to bypass two-step authentication
- For **managed tenants**, you can specify IP ranges that can skip MFA
- For **federated tenants**, you can specify IP ranges and you can also exempt AD FS claims users

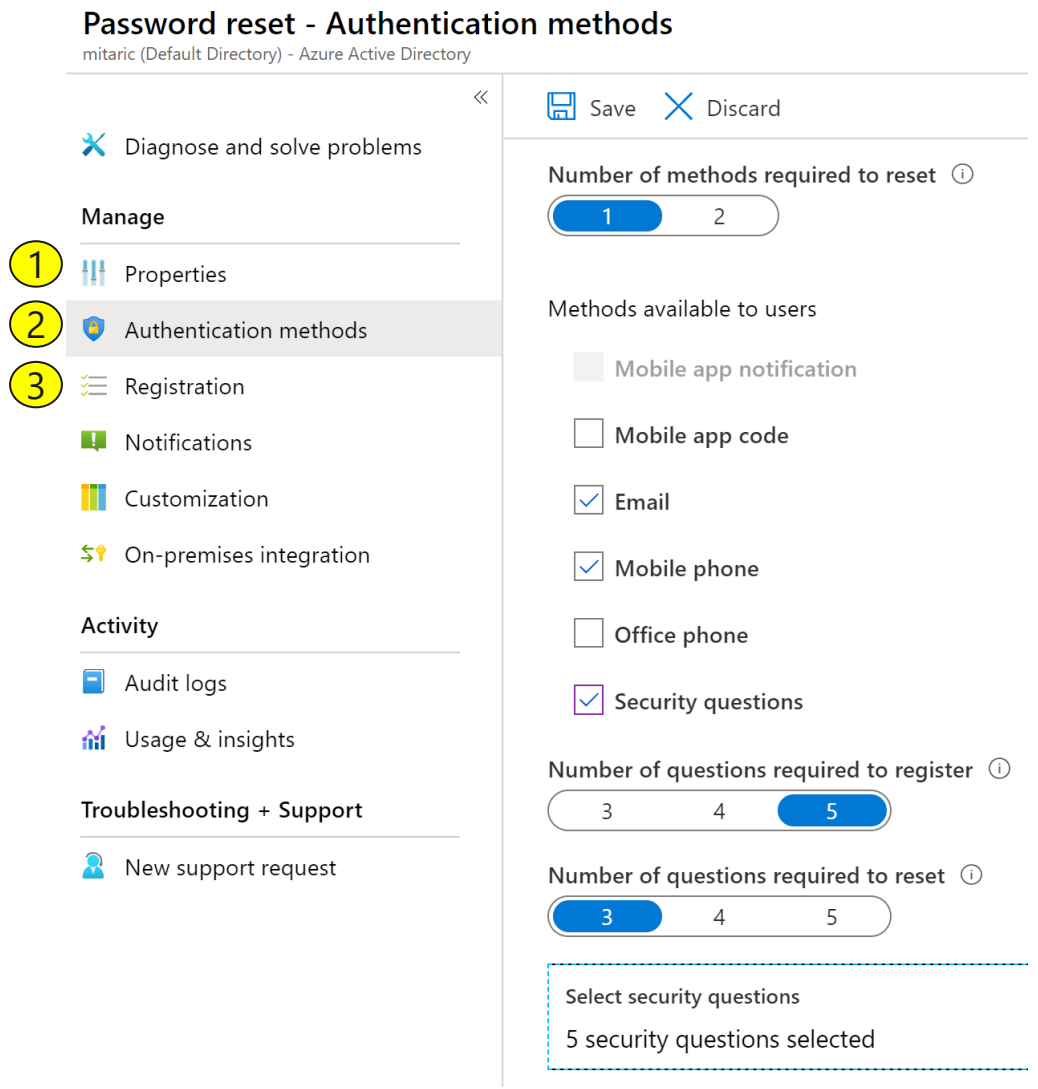
Fraud Alerts

- Users can report fraudulent attempts to access their resources
- Report fraud attempts by using the mobile app or through their phone
- Block user when fraud is reported

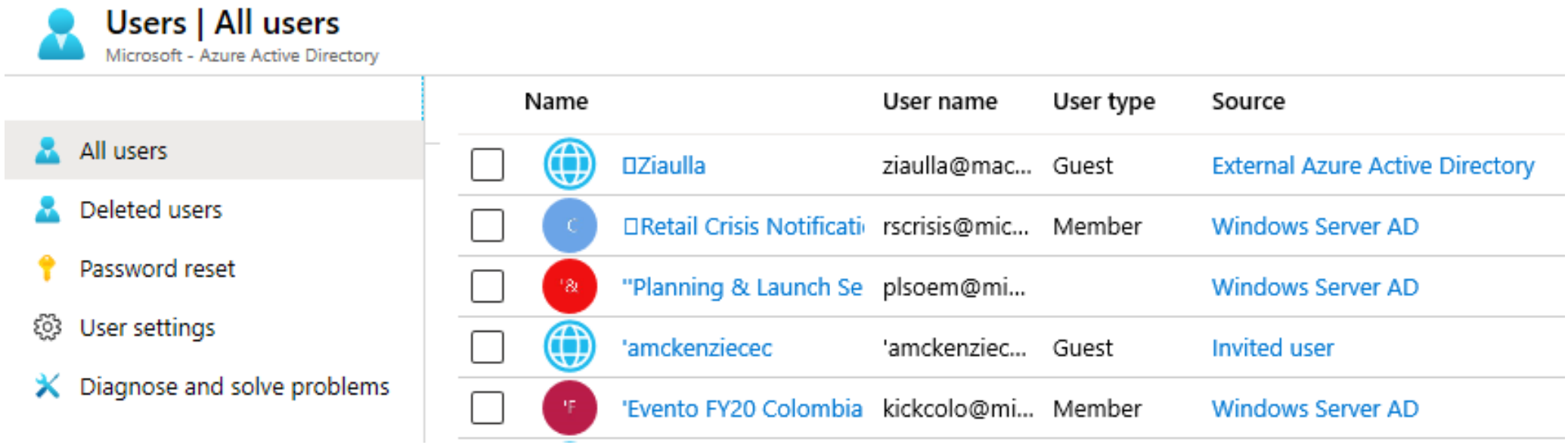


Self-Service Password Reset

1. Determine who can use self-service password reset
2. Choose the number of authentication methods required and the methods available (email, phone, questions)
3. You can require users to register for SSPR (same process as MFA)

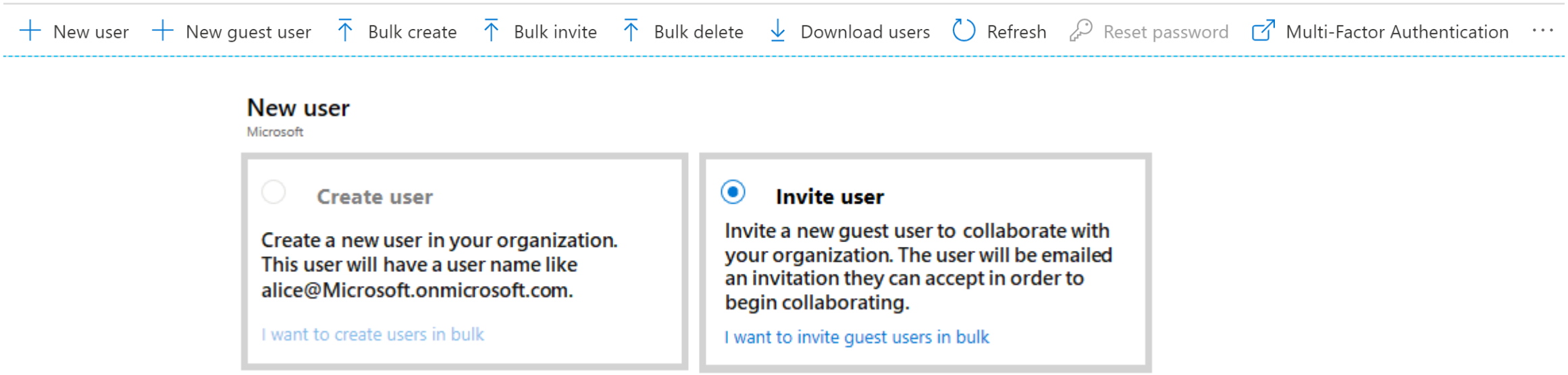


User Accounts



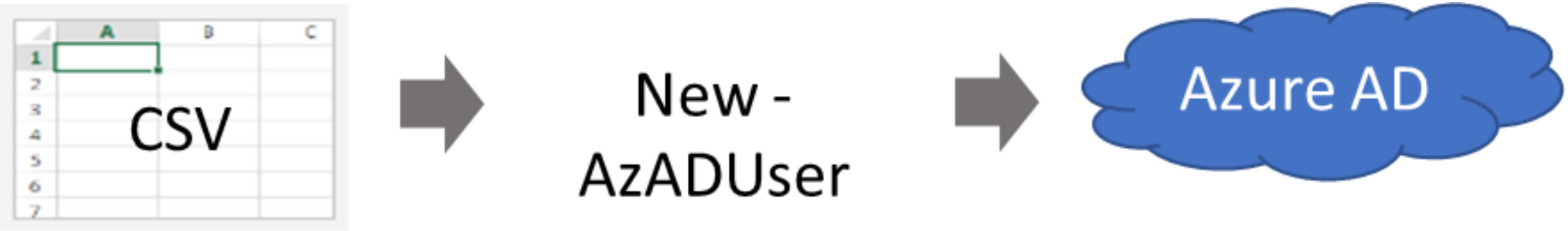
- All users must have an account
- The account is used for authentication and authorization
- Identity Sources: Cloud, Directory-synchronized, and Guest

Managing User Accounts



- Must be Global Administrator to manage users
- User profile (picture, job, contact info) is optional
- Deleted users can be restored for 30 days
- Sign in and audit log information is available

Bulk User Accounts



- Create the comma-separated values (CSV) file with the list of all the users and their properties
- Loop through the file processing each user
- Consider error handling, duplicate users, initial password settings, empty properties, and when the account is enabled

✔ Bulk invite Azure AD B2B collaboration users is in Preview

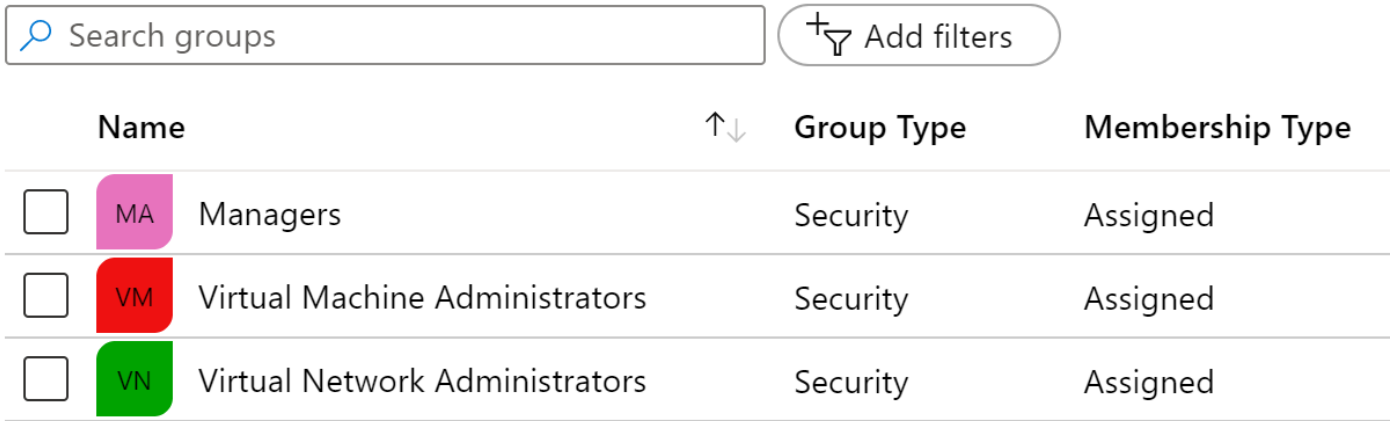
Group Accounts

Group Types

- Security groups
- Office 365 groups

Assignment Types

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

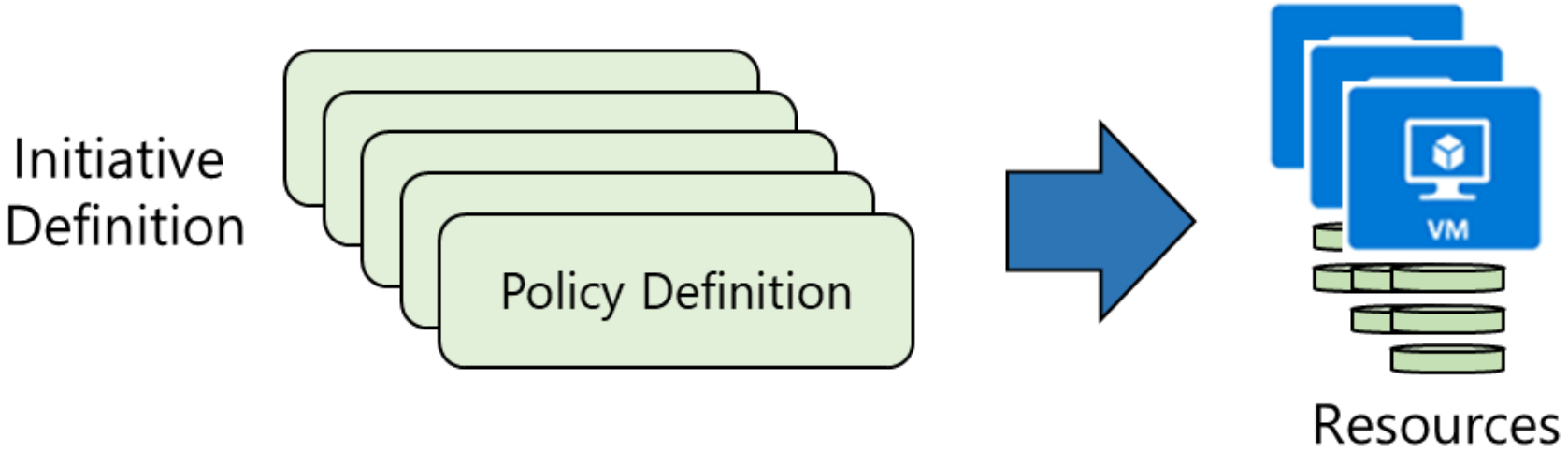


Azure Policy

- Azure Policy is a service in Azure that you use to create, assign and, manage policies
- Azure Policy runs evaluations and scans for non-compliant resources
- Advantages:
  - Enforcement and compliance
  - Apply policies at scale
  - Remediation

Usage Cases
Allowed resource types - Specify the resource types that your organization can deploy.
Allowed virtual machine SKUs – Specify a set of virtual machine SKUs that your organization can deploy.
Allowed locations – Restrict the locations your organization can specify when deploying resources.
Require tag and its value - Enforces a required tag and its value.
Azure Backup should be enabled for Virtual Machines – Audit if Azure Backup service is enabled for all Virtual machines.

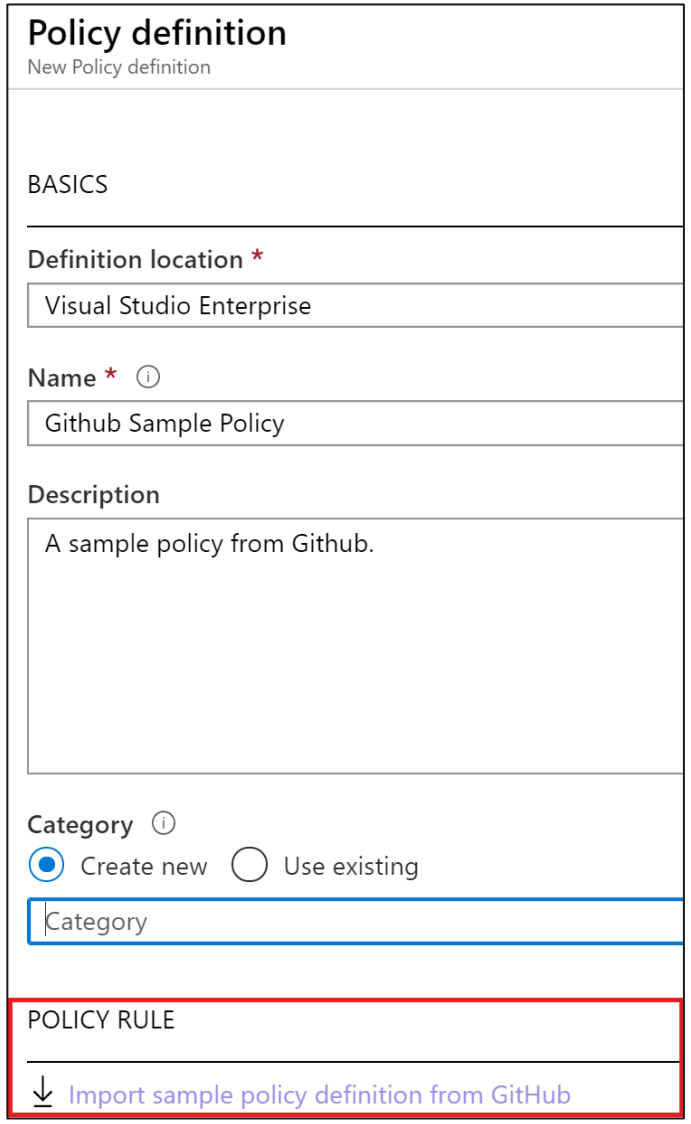
Implementing Azure Policy



1. Browse Policy Definitions
2. Create Initiative Definitions
3. Scope the Initiative Definition
4. View Policy evaluation results

Policy Definitions

- Many policy definitions are available
- You can import policies from GitHub
- Policy Definitions have a specific JSON format
- You can create custom policy definitions

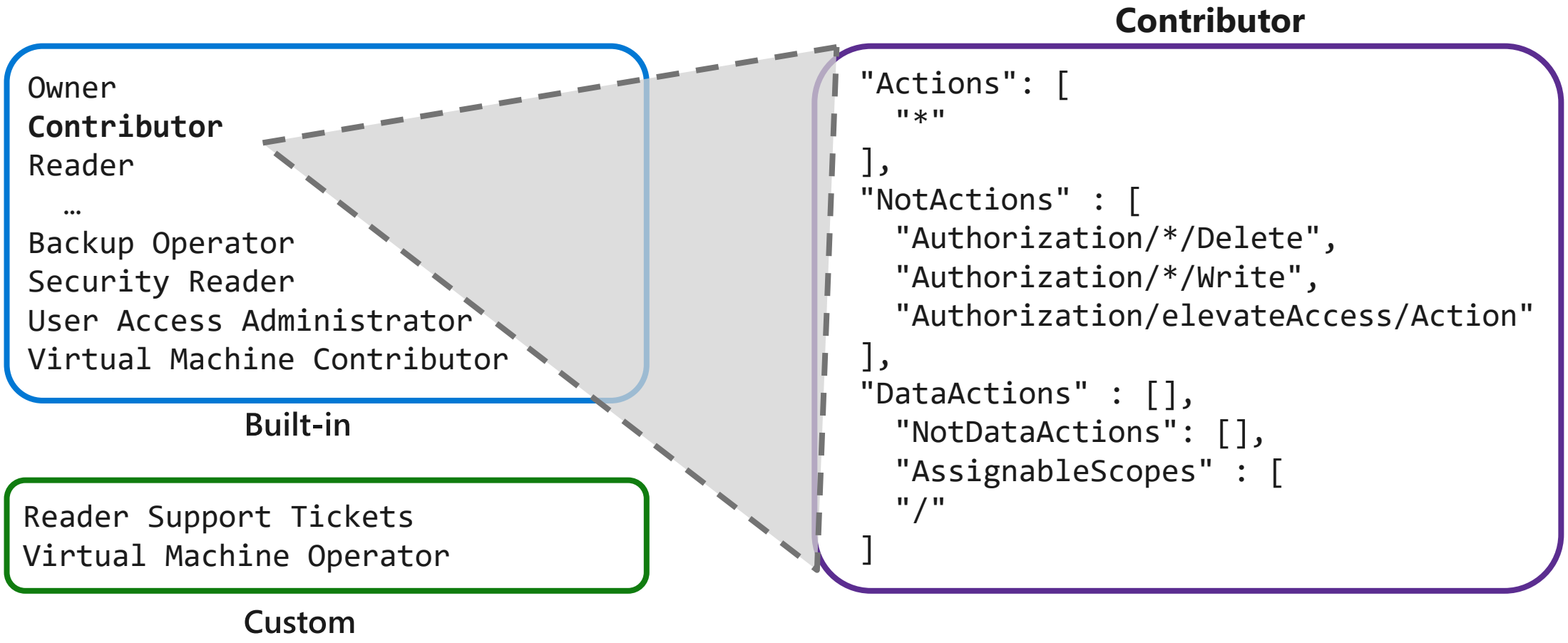


Role-Based Access Control

- Provides fine-grained access management of resources in Azure
  - Built on Azure Resource Manager
  - Segregate duties within your team
  - Grant only the amount of access to users that they need to perform their jobs
- Concepts
  - **Security principal**. Object that represents something that is requesting access to resources
  - **Role definition.** Collection of permissions that lists the operations that can be performed
  - **Scope.** Boundary for the level of access that is requested
  - **Assignment.** Attaching a role definition to a security principal at a particular scope
    - Users can grant access described in a role definition by creating an assignment
    - Deny assignments are currently read-only and can only be set by Azure

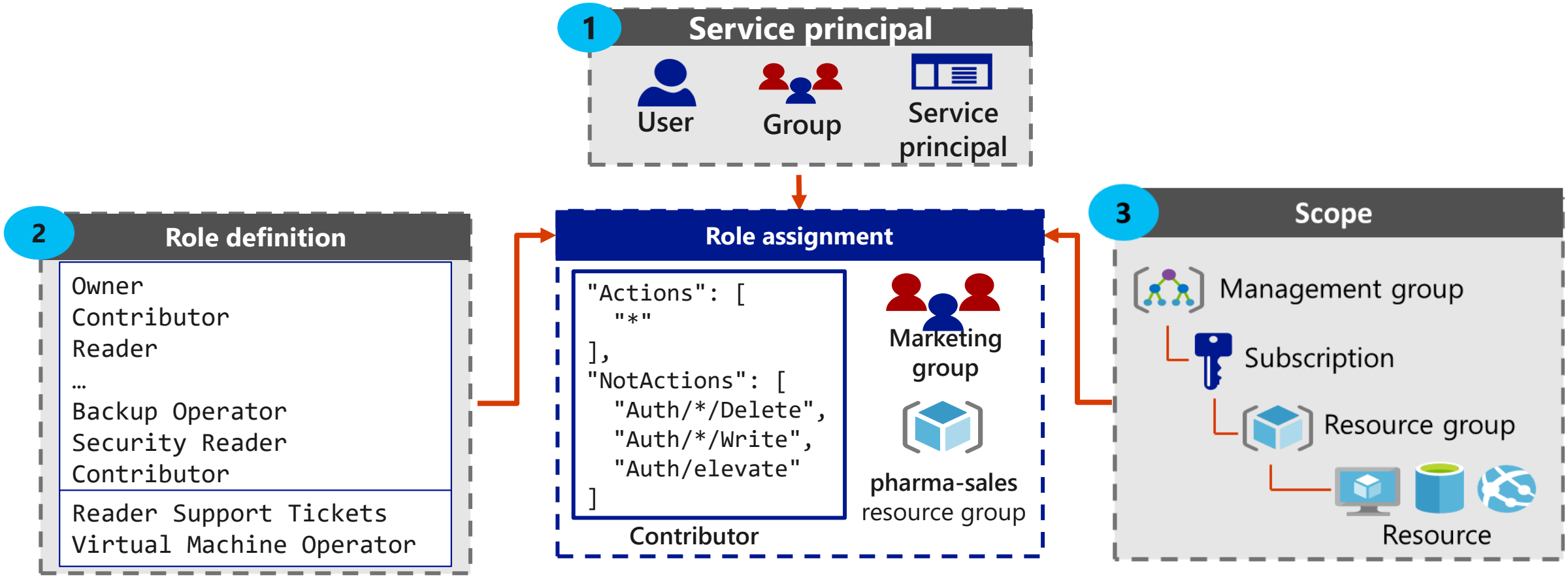
Role Definition

Collection of permissions that lists the operations that can be performed



Role Assignment

Process of binding a role definition to a user, group, or service principal at a scope for the purpose of granting access

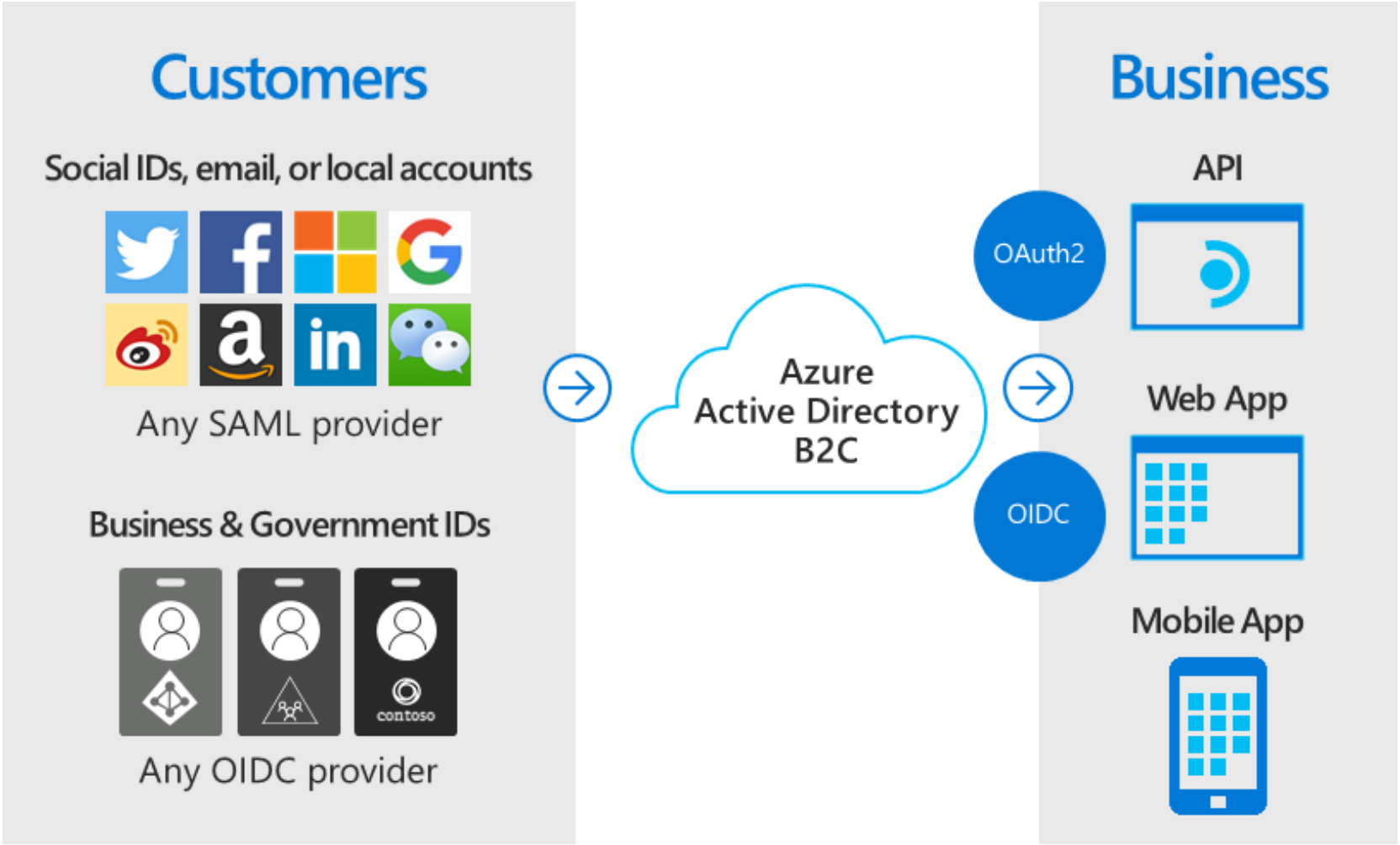


Azure RBAC Roles

RBAC role in Azure	Permissions	Notes
Owner	Has full access to all resources and can delegate access to others.	The Service Administrator and Co-Administrators are assigned the Owner role at the subscription scope. This applies to all resource types.
Contributor	Creates and manages all types of Azure resources but cannot grant access to others.	This applies to all resource types.
Reader	Views Azure resources.	This applies to all resource types.
User Access Administrator	Manages user access to Azure resources.	This applies to managing access, rather than to managing resources.

Azure Active Directory B2C

- Identity and access management for your customer-facing apps

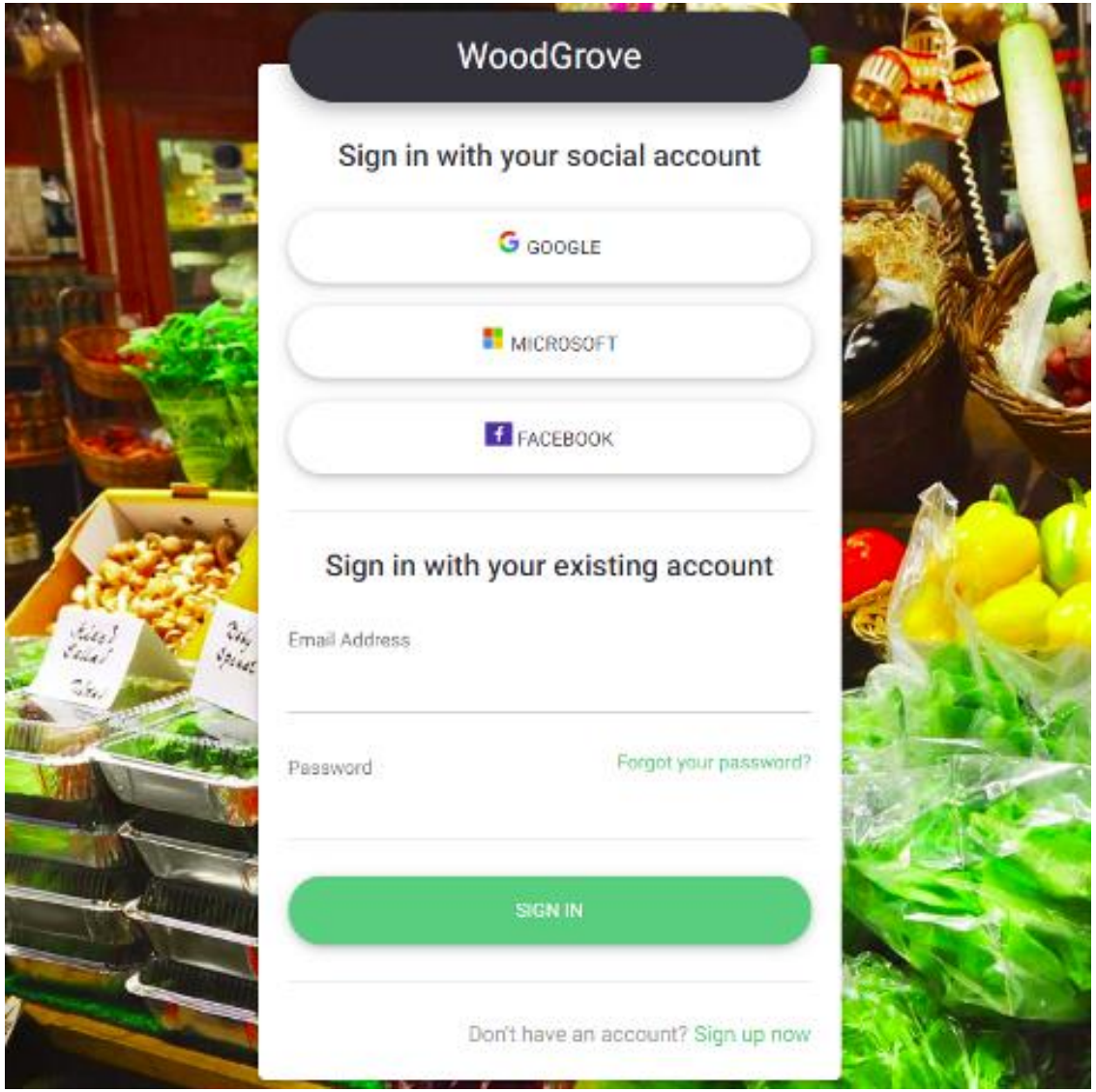


Azure Active Directory B2C

- Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.

- Manage customer, consumer and citizen access to your web, desktop, mobile or single-page applications. Built on the Azure Active Directory (Azure AD) identity platform, which supports more than 1 billion identities worldwide, this business-to-consumer (B2C) cloud identity service gives you the scalability and availability you need.

Azure Active Directory B2C - Custom-branded identity solution

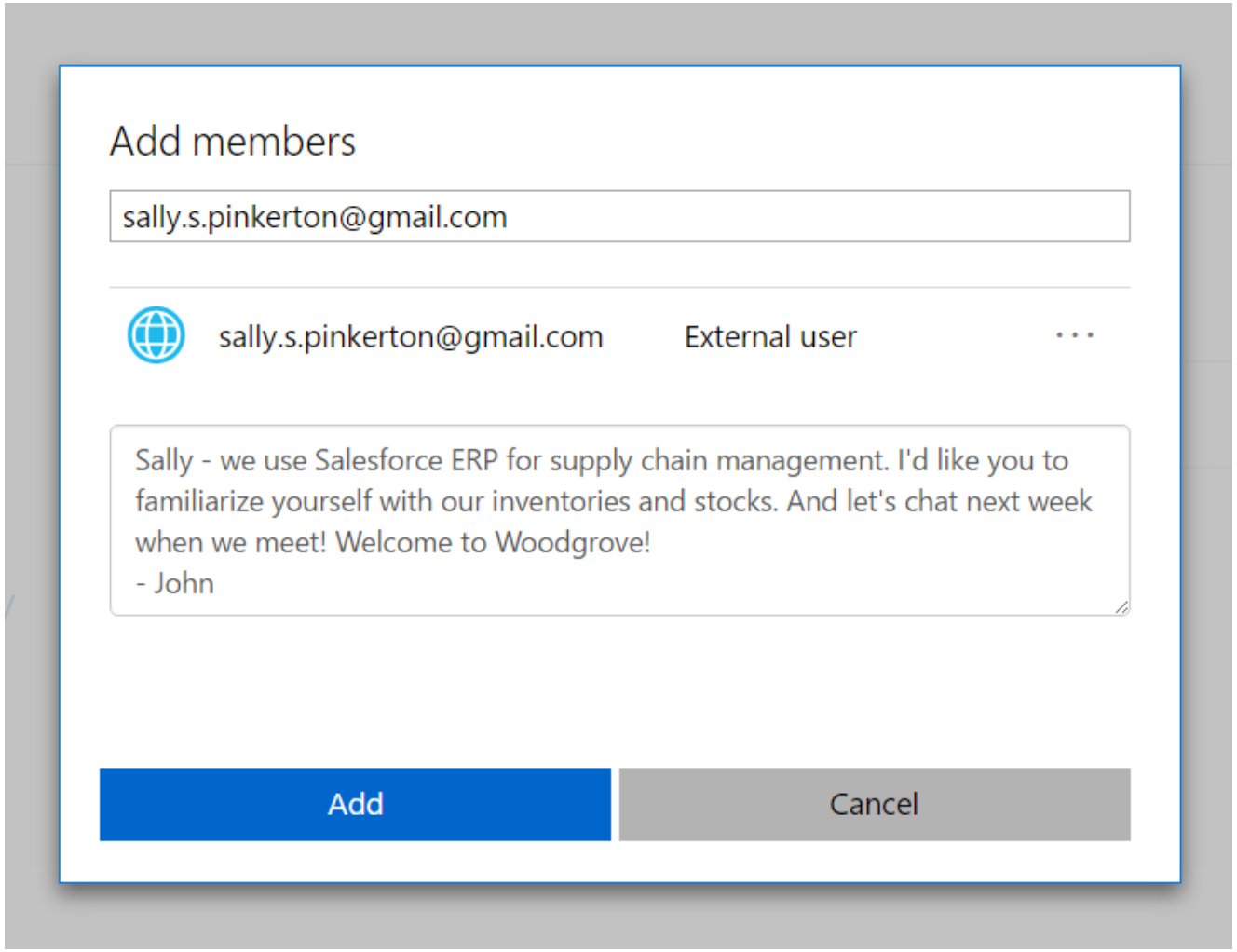


Azure Active Directory B2B

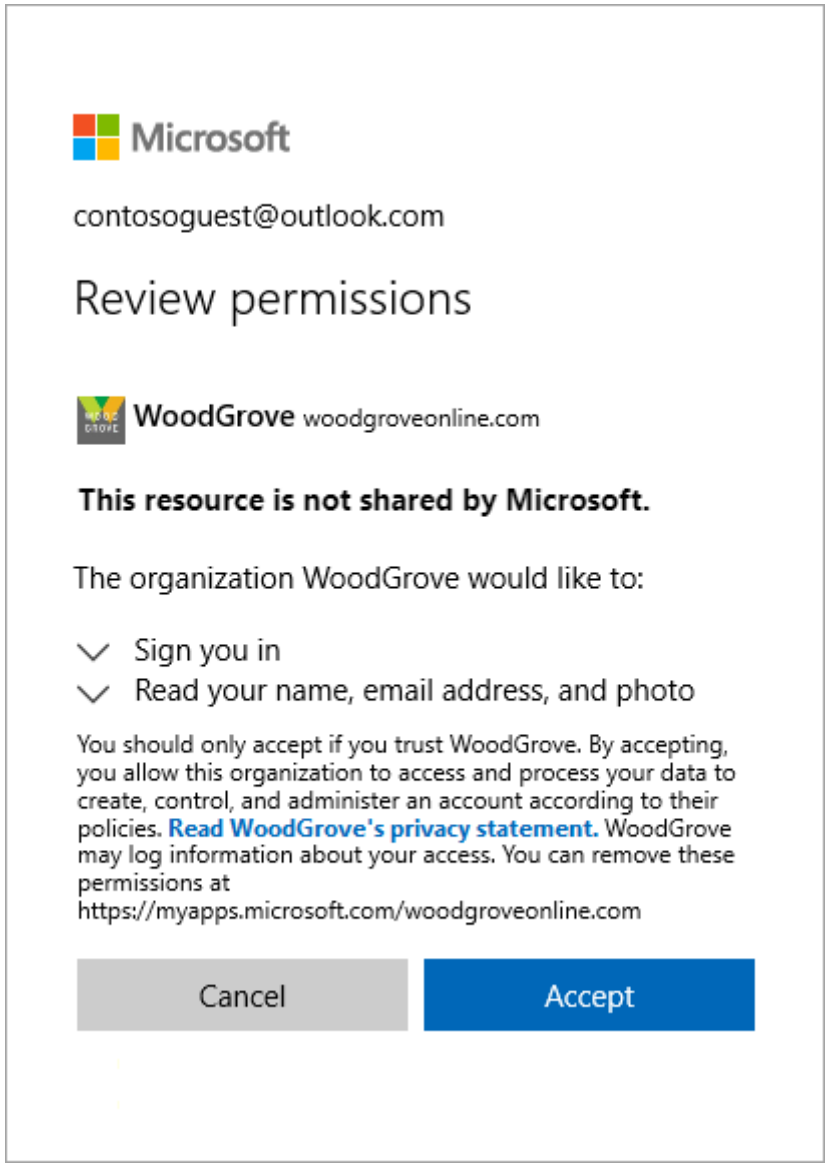
- Azure Active Directory (Azure AD) business-to-business (B2B) collaboration lets you securely share your company's applications and services with guest users from any other organization, while maintaining control over your own corporate data.

- Work safely and securely with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources. Developers can use Azure AD business-to-business APIs to customize the invitation process or write applications like self-service sign-up portals.

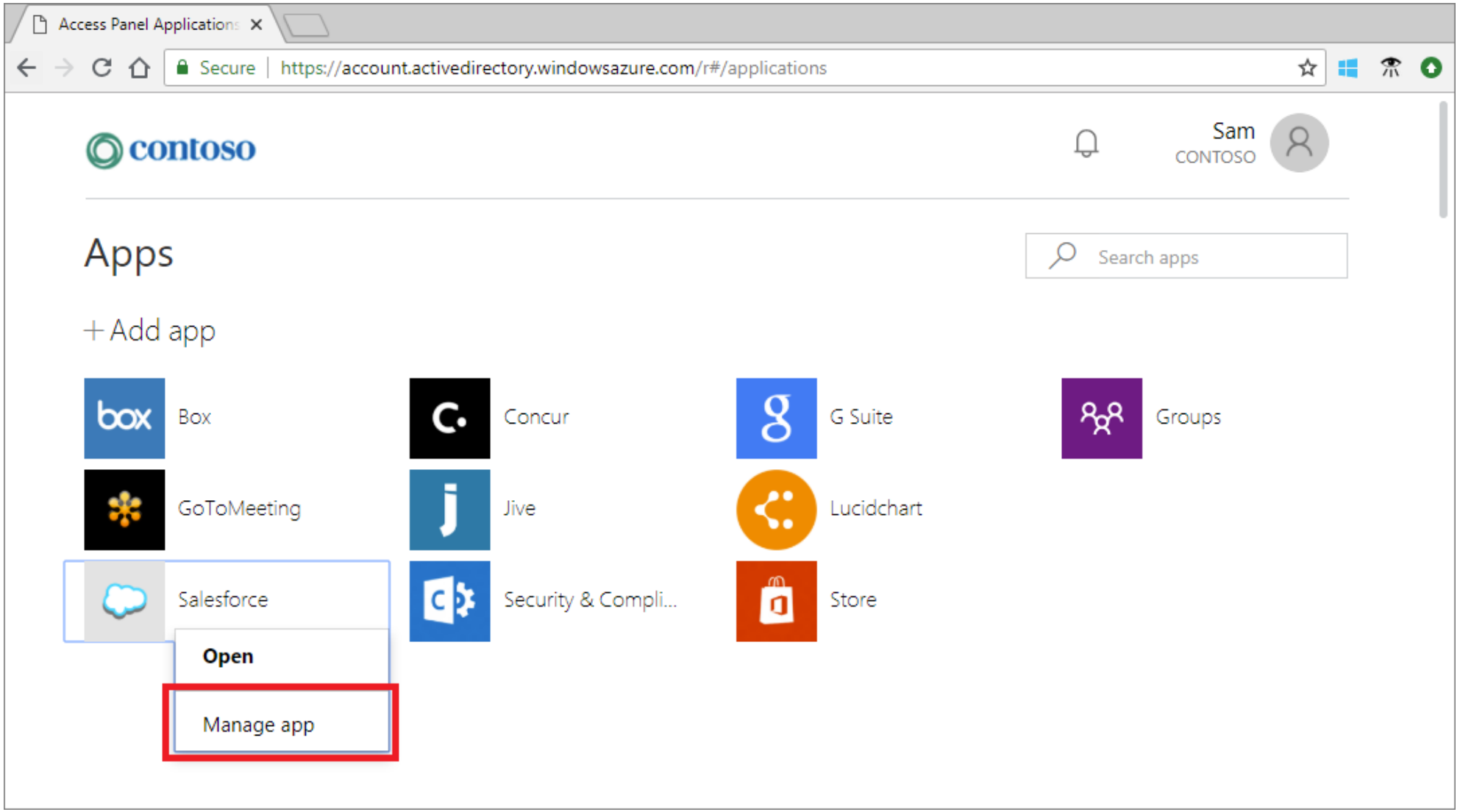
Azure Active Directory B2B



Azure Active Directory B2B



Let application and group owners manage their own guest users



Authentication Methods for Password Reset

- Choose the:
  - Number of authentication methods required to reset a password
  - Number of authentication methods available to users
- Authentication methods include:
  - Email notification
  - Text or code sent to phone
  - Number of security questions to be registered and how many must be correctly answered