Microsoft SC-900 Notes

Microsoft Security, Compliance, and Identity Fundamentals

Hassen Hannachi

December 12, 2025

Contents

List of Figures

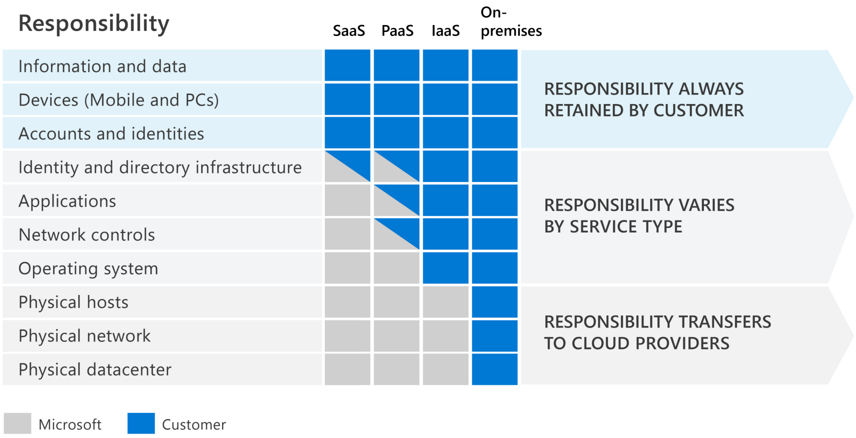
Learn about core concepts that are foundational to security, compliance, and identity solutions, including shared responsibility, Zero Trust, data residency, the role of identity providers, and more.

1 Introduction to security, compliance, and identity concepts

1.1 Describe security and compliance concepts

Learn about common security and compliance concepts that are foundational to Microsoft solutions. Topics include the shared responsibility and Zero Trust models, encryption, data residency and data sovereignty, and more.

1.1.1 Unit 1: Describe Shared responsibility model



Responsibility	SaaS	PaaS	IaaS	On-premises	
Information and data	🟦	🟦	🟦	🟦	RESPONSIBILITY ALWAYS RETAINED BY CUSTOMER
Devices (Mobile and PCs)	🟦	🟦	🟦	🟦	
Accounts and identities	🟦	🟦	🟦	🟦	
Identity and directory infrastructure	◩	◩	🟦	🟦	RESPONSIBILITY VARIES BY SERVICE TYPE
Applications	⬜	◩	🟦	🟦	
Network controls	⬜	◩	🟦	🟦	
Operating system	⬜	⬜	🟦	🟦	
Physical hosts	⬜	⬜	⬜	🟦	RESPONSIBILITY TRANSFERS TO CLOUD PROVIDERS
Physical network	⬜	⬜	⬜	🟦	
Physical datacenter	⬜	⬜	⬜	🟦	

⬜ Microsoft 🟦 Customer

Figure 1: share responsibility model

- ***On-premises datacenters***: In an on-premises datacenter, hardware and software, the organization is 100 percent responsible for implementing security and compliance.

- ***Infrastructure as a Service (IaaS)***: Of all cloud services, IaaS requires the most management by the cloud customer. Customers still have responsibility for software components running on that computing infrastructure such as operating systems, network controls, applications, and protecting data.

- ***Platform as a Service (PaaS)***: PaaS provides an environment for building, testing, and deploying software applications. With PaaS, the cloud provider manages the hardware and operating systems, and the customer is responsible for applications and data.

- ***Software as a Service (SaaS)***: SaaS is hosted and managed by the cloud provider, for the customer. The cloud provider is responsible for managing everything except data, devices, accounts, and identities.

For all cloud deployment types, you, the cloud customer, own your data and identities. You're responsible for protecting the security of your data and identities, and on-premises resources including mobile devices, PCs, printers, and more. In summary, responsibilities always retained by the customer organization include:

- Information and data
- Devices (mobile and PCs)
- Accounts and identities

1.1.2 Unit 2: Defense in depth

Defense in depth uses a layered approach to security, rather than relying on a single perimeter. Each layer provides protection so that, if one layer is breached, a subsequent layer will prevent an attacker getting unauthorized access to data.

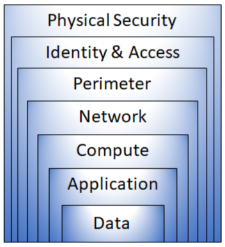


Figure 2: defense in depth

- ***Physical*** security such as limiting access to a datacenter to only authorized personnel.
- ***Identity and access*** security controls, such as multifactor authentication or condition-based access, to control access to infrastructure and change control.
- ***Perimeter*** security of your corporate network includes distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- ***Network*** security, such as network segmentation and network access controls, to limit communication between resources.
- ***Compute*** layer security such as securing access to virtual machines either on-premises or in the cloud by closing certain ports.
- ***Application*** layer security to ensure applications are secure and free of security vulnerabilities.
- ***Data*** layer security including controls to manage access to business and customer data and encryption to protect data.

Confidentiality, Integrity, Availability (CIA

Defense in-depth strategy uses a series of mechanisms to slow the advance of an attack. All the different mechanisms (technologies, processes, and training) are elements of a cybersecurity strategy, whose goals include ensuring confidentiality, integrity, and availability; often referred to as CIA.

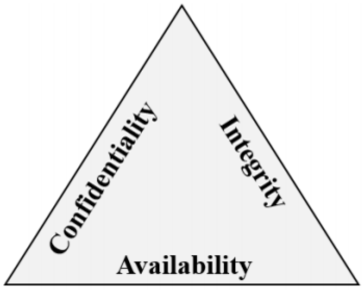


Figure 3: confidentiality, integrity, availability (CIA)

- ***Confidentiality*** refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data. You can encrypt data to keep it confidential. but then you also need to keep the encryption keys confidential.
- ***Integrity*** refers to keeping data or messages correct. Integrity is about having confidence that data hasn't been tampered with or altered.
- ***Availability*** refers to making data available to those who need it, when they need it.

1.1.3 Unit 3: Describe the Zero Trust model

The Zero Trust model operates on the principle of "trust no one, verify everything."

Trust Guiding Principles

The Zero Trust model has three principles which guide how security is implemented:

- ***Verify explicitly***. Always authenticate and authorize based on the available data points, including user identity, location, device, service or workload, data classification, and anomalies.
- ***Least privileged access***. Limit user access with just-in-time and just-enough access (JIT/JEA), risk-based adaptive policies, and data protection to protect both data and productivity.
- ***Assume breach***. Segment access by network, user, devices, and application. Use encryption to protect data, and use analytics to get visibility, detect threats, and improve your security.

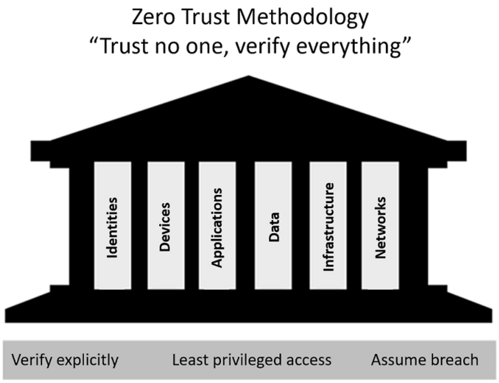


Figure 4: six foundational pillars

Six Foundational Pillars

In the Zero Trust model, all elements work together to provide end-to-end security. These six elements are the foundational pillars of the Zero Trust model:

- ***Identities*** may be users, services, or devices. When an identity attempts to access a resource, it must be verified with strong authentication and follow least privilege access principles.
- ***Devices*** create a large attack surface as data flows from devices to on-premises workloads and the cloud. Monitoring devices for health and compliance is an important aspect of security.
- ***Applications*** are the way that data is consumed. This includes discovering all applications being used, sometimes called Shadow IT because not all applications are managed centrally. This pillar also includes managing permissions and access.
- ***Data*** should be classified, labeled, and encrypted based on its attributes.
- ***Infrastructure***, whether on-premises or cloud based, represents a threat vector. To improve security, you assess for version, configuration, and JIT access, and use telemetry to detect attacks and anomalies.
- ***Networks*** should be segmented, including deeper in-network micro segmentation. Also, real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.

1.1.4 Unit 4: Describe encryption and hashing

Encryption is the process of making data unreadable and unusable to unauthorized viewers. To use or read encrypted data, it must be decrypted, which requires the use of a secret key.

- Symmetric encryption uses the same key to encrypt and decrypt data.

- Asymmetric encryption uses a public key and private key pair. Either key can encrypt data, but the key used to encrypt can't be used to decrypt encrypted data.
- Asymmetric encryption is used for things such accessing sites on the internet using the HTTPS protocol and electronic data signing solutions.
- Encryption may protect data at rest, or in transit.

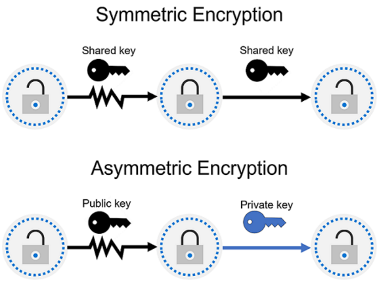


Figure 5: encryption

Encryption for data at rest

Data at rest is the data that's stored on a physical device, such as a server (or stored in a database or a storage account), encryption of data at rest ensures the data is unreadable without the keys and secrets needed to decrypt it.

Encryption for data in transit

Data in transit is the data moving from one location to another, such as across the internet or through a private network. Secure transfer can be handled by several different layers. It could be done by encrypting the data at the application layer before sending it over a network. HTTPS is an example of encryption in transit.

Encryption for data in use

A common use case for encryption of data in use involves securing data in nonpersistent storage, such as RAM or CPU caches. This can be achieved through technologies that create an enclave (think of this as a secured lockbox) that protects the data and keeps data encrypted while the CPU processes the data.

Hashing

uses an algorithm to convert text to a unique fixed-length value called a hash. Each time the same text is hashed using the same algorithm, the same hash value is produced.

- Hashing is different to encryption in that it doesn't use keys

- Hashed value isn't subsequently decrypted back to the original.
- Hashing is often used to store passwords.

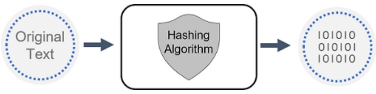


Figure 6: hashing

1.1.5 Unit 5: Describe governance, risk, and compliance (GRC) concepts

Organizations face increasing complexity and change in regulatory environments, calling for a more structured approach for managing governance, risk, and compliance (GRC).

As organizations establish GRC competency they can establish a framework that includes implementing specific policies, operational processes, and technologies.

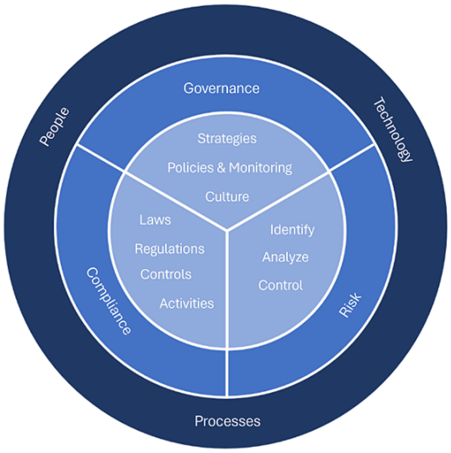


Figure 7: governance, risk, and compliance (GRC)

Governance

is the set of rules and processes an organization uses to direct and control its operations. Many of these come from external standards and requirements. For example, organizations define who can access resources, what they can do, where and when they can do it, and who gets administrative privileges and for how long.

Risk management

is the process of identifying, assessing, and addressing threats that could impact company or customer goals. Risks come from both external and internal sources. External risks include political or economic changes, weather events, pandemics, and security breaches. Internal risks arise within the organization, such as data leaks, intellectual property theft, fraud, or insider threats.

Compliance

refers to the laws and regulations—local, national, or international—that an organization must follow. These rules define what data must be protected, what processes are required, and the penalties for failing to comply.

Compliance is not the same as security. Compliance focuses on meeting legal minimum standards, while security involves all the practices and technologies used to protect sensitive data and prevent breaches. However, strong security is often essential for meeting compliance requirements. Some compliance-related concepts include:

- ***Data residency*** in compliance, data residency rules define where data can be physically stored and how/when it can be transferred, processed, or accessed across borders. These requirements vary widely by jurisdiction.
- ***Data sovereignty*** is the principle that data—especially personal data—is governed by the laws of the country or region where it's collected, stored, or processed. This creates complexity because a single piece of data may be collected in one place, stored in another, and processed in a third, making it subject to multiple legal jurisdictions.
- ***Data privacy*** Providing clear notice and being transparent about how personal data is collected, used, processed, and shared are core principles of privacy laws. Personal data includes any information that identifies or can be linked to an individual. Organizations must follow numerous laws, regulations, codes of conduct, and industry standards that govern how this data is protected and managed.

All organizations manage data so understanding terminology and concepts related to compliance is important as they work to meet the minimum, mandated laws and/or regulations.

1.2 Describe identity concepts

Identity is the way in which people and things are identified on your corporate network, and in the cloud. Being certain about who or what is accessing your organization's data and other resources is a fundamental part of securing your environment.

1.2.1 Unit 1: Define authentication and authorization

Authentication

is the process of proving that a person is who they say they are.

When you want to access a computer or device, you may get asked to enter a username and password. The username states who you are, but by itself isn't enough to grant you access. When combined with the password, which only that user should know, it allows access to your systems. The username and password, together, are a form of authentication. Authentication is sometimes shortened to AuthN.

Authorization

Once you authenticate a user, you'll need to decide where they can go, and what they're allowed to see and touch. This process is called authorization. In cybersecurity terms, authorization determines the level of access or the permissions an authenticated person has to your data and resources. Authorization is sometimes shortened to **`AuthZ`**.

1.2.2 Unit 2: Define identity as the primary security perimeter

Digital collaboration has evolved. Employees and partners now need to access resources from anywhere, on any device, without losing productivity. Remote work has also increased significantly, accelerating this shift.

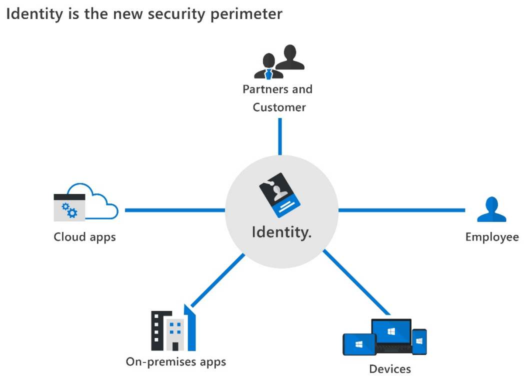


Figure 8: security perimeter

The security perimeter can no longer be viewed as the on-premises network. It now extends to:

- SaaS applications for business-critical workloads that might be hosted outside the corporate network.
- The personal devices that employees are using to access corporate resources (BYOD, or bring your own device) while working from home.
- The unmanaged devices used by partners or customers when interacting with corporate data or collaborating with employees
- Internet of things, referred to as IoT devices, installed throughout your corporate network and inside customer locations.

An identity may be associated with a user, an application, a device, or something else.

1.2.3 Unit 3: Describe the role of the identity provider

Modern authentication relies on a central identity provider. The identity provider creates, manages, and maintains identity information, and delivers authentication, authorization, and auditing services.

- With this model, all authentication flows through a single provider, which centrally stores and manages the information used to verify users.
- This centralization allows organizations to enforce consistent authentication and authorization policies, monitor user behavior, detect suspicious activity, and reduce malicious attacks.
- With modern authentication, the client provides an identity to the identity provider, which verifies it. Once verified, the identity provider issues a security token that the client presents to the server.
- The server validates the token through its trust relationship with the identity provider. Using the token and its contained information, the user or application gains access to server resources. The identity provider centrally manages both the token and authentication service.

Examples of cloud-based identity providers include Microsoft Entra ID, Google, Amazon, LinkedIn, and GitHub.

Single sign-on

Another fundamental capability of an identity provider and "modern authentication" is the support for single sign-on (SSO). With SSO, the user logs in once and that credential is used to access multiple applications or resources. When you set up SSO between multiple identity providers, it's called federation.

1.2.4 Unit 4: Describe the concept of directory services and Active Directory

In computer networks, a directory is a hierarchical structure that stores information about network objects. A directory service manages this data and makes it accessible to users, administrators, services, and applications.

Microsoft's Active Directory (AD), introduced with Windows 2000, is a set of directory services for on-premises, domain-based networks. Its primary service, Active Directory Domain Services (AD DS), stores information about domain members, verifies credentials, and defines access rights. Servers running AD DS are called domain controllers (DCs). AD DS allows organizations to manage multiple on-premises systems using a single user identity. However, it does not natively support mobile devices, SaaS applications, or modern authentication methods.

The rise of cloud services, SaaS, and personal devices has driven the evolution of AD-based identity solutions. Microsoft Entra ID (formerly Azure Active Directory) is an example, offering Identity as a Service (IDaaS) for both cloud and on-premises applications.

1.2.5 Unit 5: Describe the concept of federation

Federation allows access to services across organizational or domain boundaries by creating trust between their identity providers. It eliminates the need for users to have separate usernames and passwords for different domains.

A simplified view of federation works like this:

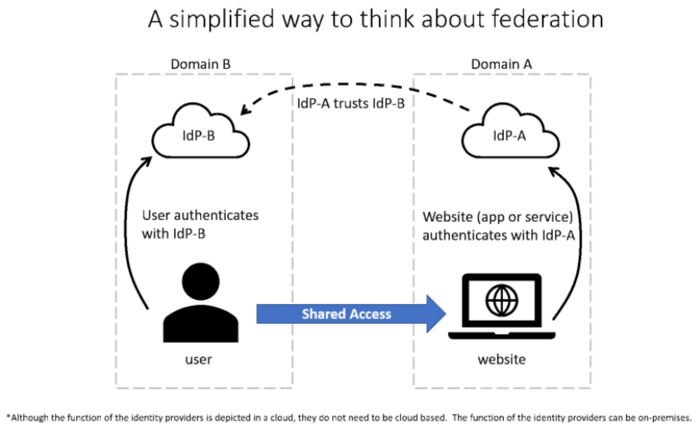

A simplified way to think about federation
Domain B
Domain A
IdP-A trusts IdP-B
IdP-B
IdP-A
User authenticates with IdP-B
Website (app or service) authenticates with IdP-A
Shared Access
user
website
*Although the function of the identity providers is depicted in a cloud, they do not need to be cloud based. The function of the identity providers can be on-premises.

Figure 9: federation

- A website in domain A uses Identity Provider A (IdP-A) for authentication.
- A user in domain B authenticates with Identity Provider B (IdP-B).
- IdP-A trusts IdP-B, so when the user provides credentials, the website grants access based on this trust.

Federation trust isn't always bidirectional; access from domain A to B only works if the trust is explicitly configured.

A common example is logging into a third-party site using a social media account. Here, the social media platform acts as the identity provider, and the third-party site (e.g., using Microsoft Entra ID) trusts it, allowing access without separate credentials.

2 Introduction to Microsoft Entra

2.1 Describe the function and identity types of Microsoft Entra ID

2.1.1 Unit 1: Describe Microsoft Entra ID

Microsoft Entra ID (formerly Azure Active Directory) is Microsoft's cloud-based identity and access management service. It allows employees, guests, and partners to sign in and access needed resources, including:

- Internal apps on the corporate network or intranet
- Cloud apps built by the organization
- External services like Microsoft 365, the Azure portal, and various SaaS apps

Entra ID streamlines authorization and access by providing one identity system for both cloud and on-premises applications. It can be synced with on-premises Active Directory, integrated with other directory services, or used on its own. It also supports secure use of personal devices and enables easy collaboration with partners and customers.

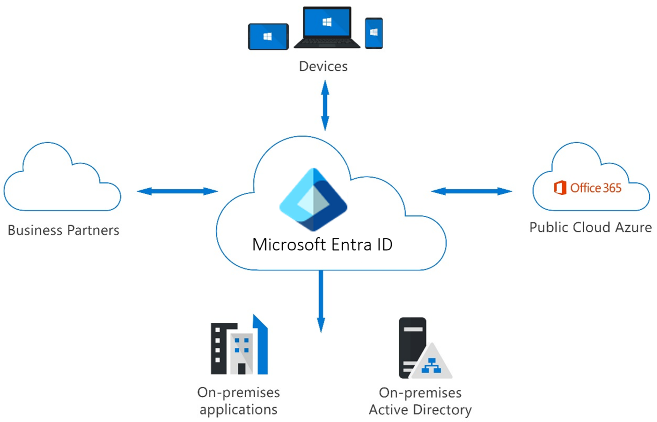
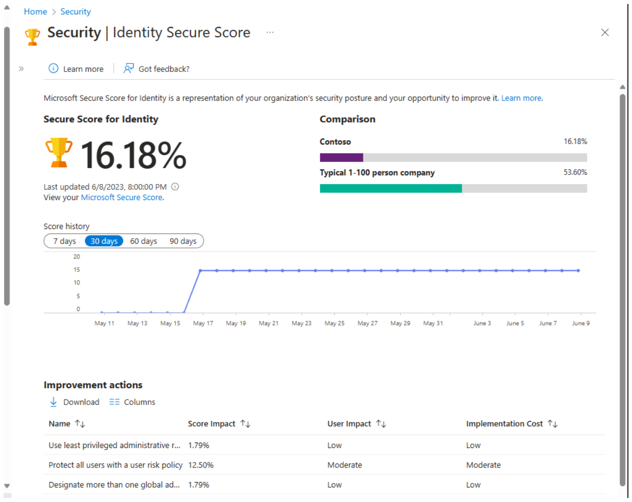


Figure 10: microsoft entra ID

Identity Secure Score

Microsoft Entra ID provides an identity secure score—a percentage that shows how closely your setup aligns with Microsoft's security best practices. Each recommended improvement is customized to your environment. This score, available in all Entra ID editions, helps you measure your identity security posture, prioritize improvements, and track progress over time.



Microsoft Secure Score for Identity is a representation of your organization's security posture and your opportunity to improve it. Learn more.

Secure Score for Identity

16.18%

Last updated 6/8/2023, 8:00:00 PM
View your Microsoft Secure Score.

Comparison

Contoso	16.18%
Typical 1-100 person company	53.60%

Improvement actions

Name ↑↓	Score Impact ↑↓	User Impact ↑↓	Implementation Cost ↑↓
Use least privileged administrative r...	1.79%	Low	Low
Protect all users with a user risk policy	12.50%	Moderate	Moderate
Designate more than one global ad...	1.79%	Low	Low

Figure 11: secure score

Basic terminology

Here's a simplified explanation of key Microsoft Entra ID terms:

- `Tenant` – A Microsoft Entra tenant is a dedicated instance of Entra ID for a single organization. It contains users, groups, devices, app registrations, and access policies. Each tenant has a unique tenant ID and domain (like contoso.onmicrosoft.com) and serves as a security and administrative boundary.

- `Directory` – Often used interchangeably with "tenant," the directory is the logical container that stores identity and access objects such as users, groups, apps, and devices. A tenant contains exactly one directory.

- `Multi-tenant` – A multi-tenant organization has more than one Entra ID tenant. This can happen due to multiple subsidiaries, mergers and acquisitions, regional data residency requirements, or independent business units.

Who uses Microsoft Entra ID

- `IT administrators` use Microsoft Entra ID to manage access to corporate apps and resources based on business needs. They can enforce policies like multi-factor authentication and use built-in tools to protect identities, credentials, and access governance.

- `Developers` use Entra ID to add standards-based single sign-on (SSO) to their applications, allowing users to sign in with existing credentials. Entra ID's APIs also let developers build personalized app experiences using organizational data.

- `Azure, Microsoft 365, and Dynamics 365 subscribers` automatically receive a Microsoft Entra ID tenant. They can use the included features and optionally upgrade to premium licenses for enhanced capabilities.

2.1.2 Unit 2: Describe types of identities

Microsoft Entra ID supports several identity types, including user identities, workload identities, device identities, external identities, and hybrid identities. These categories define what can be assigned an identity within Entra ID.

Identities can be assigned to three main types of objects:

- `People (users)`: This includes internal employees and external users such as customers, consultants, vendors, and partners. These are referred to as user identities.

- `Devices`: Physical devices like mobile phones, computers, and IoT devices can have identities.

- `Software-based objects`: Applications, virtual machines, services, and containers can all be assigned identities. These are known as workload identities.

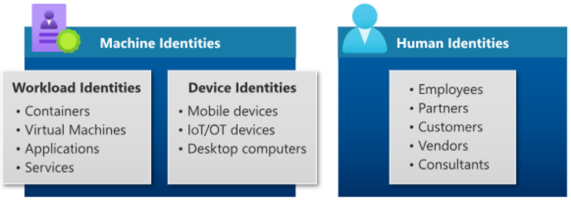
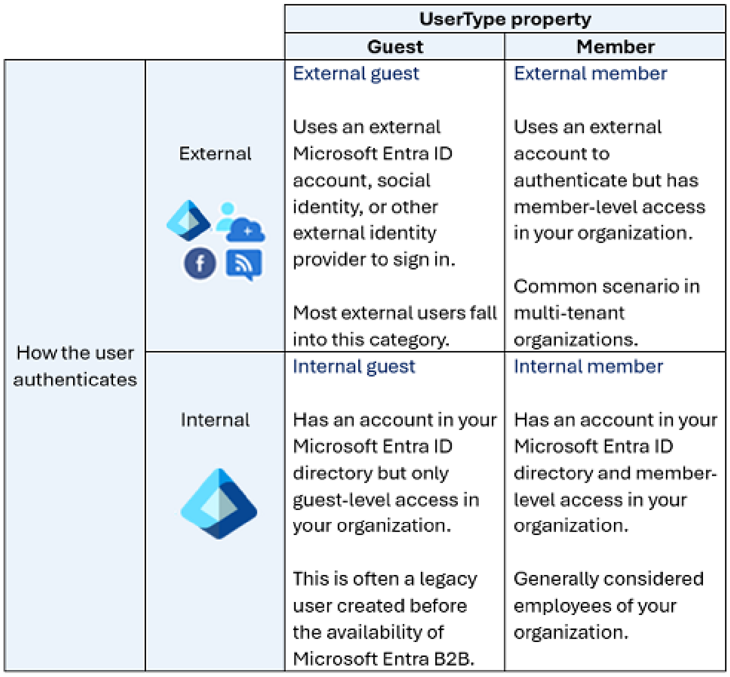


Figure 12: types of identities

User

User identities represent people-employees as well as external users like customers, vendors, consultants, and partners. In Microsoft Entra ID, user identities are defined by two things: how they authenticate and their user type.



		UserType property	
		Guest	Member
How the user authenticates	External	External guest Uses an external Microsoft Entra ID account, social identity, or other external identity provider to sign in. Most external users fall into this category.	External member Uses an external account to authenticate but has member-level access in your organization. Common scenario in multi-tenant organizations.
	Internal	Internal guest Has an account in your Microsoft Entra ID directory but only guest-level access in your organization. This is often a legacy user created before the availability of Microsoft Entra B2B.	Internal member Has an account in your Microsoft Entra ID directory and member-level access in your organization. Generally considered employees of your organization.

Figure 13: user identities

Authentication method:

- Internal users sign in using an account hosted in the organization's Entra tenant.
- External users authenticate with an identity from another Entra tenant, a social account, or another external identity provider.

User type:

- A user can be a member (an internal user) or a guest (an external user).

- Guests typically have more limited permissions within the organization's directory compared to members.

External guests and external members are part of Microsoft Entra's B2B collaboration model, covered later under External Identities.

Workload identities

Workload identity is an identity assigned to software—such as applications, services, VMs, and containers—so they can authenticate and access other resources securely.

Securing these identities is critical because, unlike humans, software often uses multiple credentials, which must be stored and managed safely. It can also be difficult to track when a workload identity is created or when it should be removed, increasing the risk of breaches if credentials are misused or left active too long.

Microsoft Entra Workload ID helps address these challenges by providing secure, manageable identities for software workloads. In Microsoft Entra, workload identities include applications, service principals, and managed identities.

Applications and service principals

A service principal is an identity used by an application. Before an app can use Microsoft Entra ID for authentication and authorization, it must be registered. Once registered, a service principal is created in every tenant where the app is used. This service principal is what allows the application to authenticate and access resources protected by that tenant.

Application developers must manage and secure the credentials used by service principals. If these credentials aren't handled properly, they can create security risks. Managed identities solve this problem by handling credential management automatically, reducing the burden on developers and improving security.

Managed identities

Managed identity is a special type of service principal that Microsoft Entra ID manages automatically. They remove the need for developers to create, store, or rotate credentials.

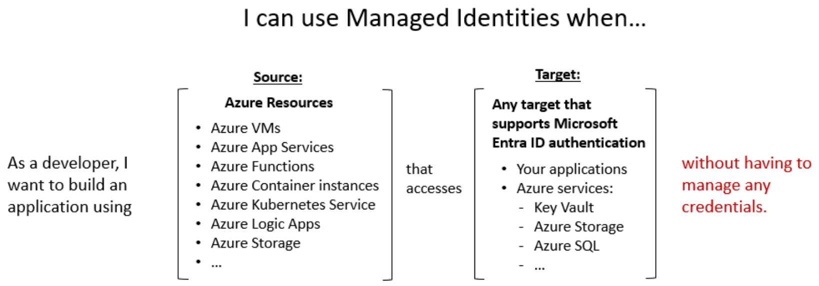

I can use Managed Identities when…
As a developer, I want to build an application using
Source:
Azure Resources
• Azure VMs
• Azure App Services
• Azure Functions
• Azure Container instances
• Azure Kubernetes Service
• Azure Logic Apps
• Azure Storage
• …
that accesses
Target:
Any target that supports Microsoft Entra ID authentication
• Your applications
• Azure services:
- Key Vault
- Azure Storage
- Azure SQL
- …
without having to manage any credentials.

Figure 14: managed identities

Managed identities give applications a secure, automatically maintained identity they can use to access Azure resources that support Entra authentication — at no additional cost. Managed identities in Microsoft Entra ID come in two types: system-assigned and user-assigned.

`System-assigned:`

- Enabled directly on an Azure resource, like a virtual machine.
- The identity is tied to the resource's lifecycle.
- When the resource is deleted, Azure automatically deletes the identity.
- Ideal for workloads contained within a single resource.

`User-assigned:`

- Created as a standalone Azure resource.
- Can be assigned to one or more Azure resources, such as multiple VMs.
- Managed separately from the resources; deleting a resource doesn't delete the identity.
- Must be explicitly deleted when no longer needed.
- Useful when multiple resources share the same permissions or when resources are frequently recycled.

Device identities

Device identities represent hardware such as laptops, mobile devices, servers, or printers. They provide administrators with information to manage access and configuration. In Microsoft Entra ID, devices can be set up in three ways:

- **`Entra registered devices`**: Designed for BYOD or personal mobile devices. Users can access organizational resources without signing in with an organizational account.
- **`Entra joined devices`**: Devices owned by the organization and joined to Entra ID using an organizational account for sign-in.
- **`Entra hybrid joined devices`**: Devices joined to both on-premises Active Directory and Entra ID, requiring an organizational account. Useful for organizations with existing AD infrastructure.

Registering or joining devices enables Single Sign-On (SSO) to cloud resources. Entra joined devices also provide SSO to apps that rely on on-premises Active Directory.

Administrators can manage devices using tools like Microsoft Intune, which provides mobile device (MDM) and mobile application (MAM) management.

Groups

Groups in Microsoft Entra ID help manage access for multiple identities with similar needs, allowing permissions to be assigned to the group instead of individually. This supports the Zero Trust principle of limiting access to only those who need it. There are two main types of groups:

`Security groups:`

- Used to manage access for users and devices to shared resources.
- Examples include enforcing a security policy like self-service password reset or applying conditional access policies such as MFA.
- Members can include users (internal and external), devices, other groups, and service principals.
- Requires a Microsoft Entra administrator to create.

`Microsoft 365 groups:`

- Designed for collaboration and often called distribution groups.
- Members get access to shared mailboxes, calendars, files, SharePoint sites, etc.
- Can include internal and external users.
- Users can create these groups by default; an admin role isn't required.

Groups can have assigned membership (manually selected members) or dynamic membership, which uses rules to automatically add or remove members.

2.1.3 Unit 3: Describe Hybrid identity

Many organizations use a mix of on-premises and cloud applications, yet users expect seamless access. To meet this need, a single identity across all applications is essential, which is achieved through hybrid identity.

Hybrid identity allows a common identity for authentication and authorization across on-premises and cloud resources. It is implemented through:

- **`Inter-directory provisioning`**: Creating an identity in one directory (e.g., Active Directory) and provisioning it to another (e.g., Microsoft Entra ID).
- **`Synchronization`**: Keeping identity information for on-premises users and groups consistent with the cloud.

Microsoft Entra Cloud Sync helps achieve hybrid identity goals. Using the Entra cloud provisioning agent, it provides a lightweight bridge between Active Directory and Entra ID. The agent is deployed on-premises or in an IaaS environment, while provisioning configurations are stored and managed in Entra ID.

The Microsoft Entra Cloud Sync provisioning agent uses the SCIM (System for Cross-domain Identity Management) standard with Entra ID to provision and deprovision users and groups. SCIM automates the exchange of identity information between domains, such as between Active Directory and Entra ID, and is widely adopted as the standard for provisioning.

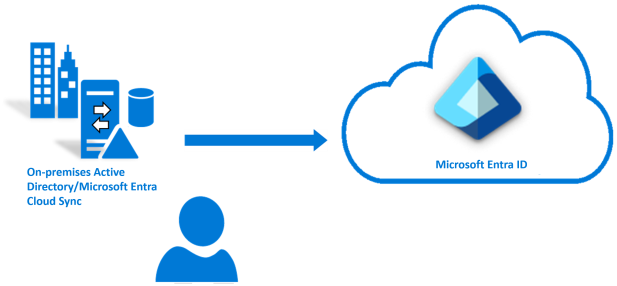


Figure 15: microsoft entra cloud sync

2.1.4 Unit 4: Describe external identity

In today's collaborative world, organizations often need to give external users access to applications and data.

Microsoft Entra External ID provides solutions to securely manage these external identities. It allows partners, customers, and other external users to access resources using their own identities—ranging from corporate or government accounts to social providers like Google or Facebook.

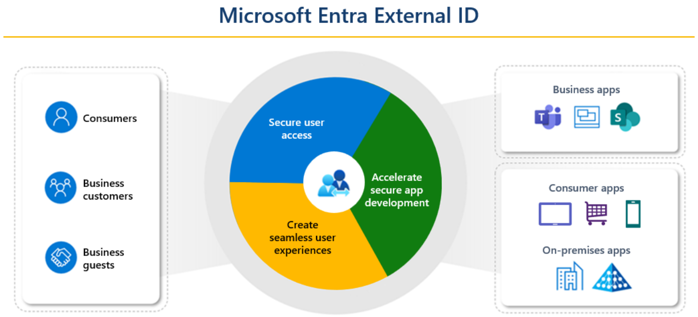


Figure 16: microsoft entra external ID

Microsoft Entra External ID provides solutions to securely manage these external identities. It allows partners, customers, and other external users to access resources using their own identities—ranging from corporate or government accounts to social providers like Google or Facebook.

Microsoft Entra External ID supports two main scenarios for working with external users:

- Collaborate with business guests

- Secure apps for consumers and business customers Each scenario requires a different tenant configuration:

- Workforce tenant: Designed for employees and internal resources. External partners and guests can be invited to collaborate within this tenant.

- External tenant: Used solely for External ID scenarios, enabling organizations to publish apps to consumers or business customers.

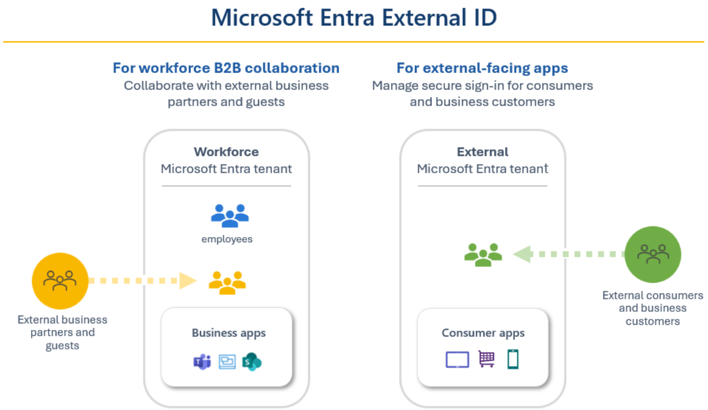

Microsoft Entra External ID
For workforce B2B collaboration
Collaborate with external business partners and guests
For external-facing apps
Manage secure sign-in for consumers and business customers
Workforce
Microsoft Entra tenant
employees
External business partners and guests
Business apps
External
Microsoft Entra tenant
External consumers and business customers
Consumer apps

Figure 17: tenant configuration

Collaborate with business guests

To enable employees to work with external partners, use Microsoft Entra External ID for B2B collaboration.

B2B collaboration allows your workforce to share applications and services with external guests while keeping corporate data secure. Guests sign in using their own credentials from their home organization or identity provider. Your organization then verifies their eligibility to access the shared apps and resources.

This approach is ideal for granting business guests access to Office 365, SaaS apps, and line-of-business applications. Guests do not have separate credentials with your organization.

Secure your apps for consumers and business customers

Organizations and developers can use Microsoft Entra External ID to add authentication and Customer Identity and Access Management (CIAM) to their applications. Entra External ID's CIAM features include:

- Self-service registration

- Personalized sign-in experiences, including SSO with social and enterprise identities

- Customer account management

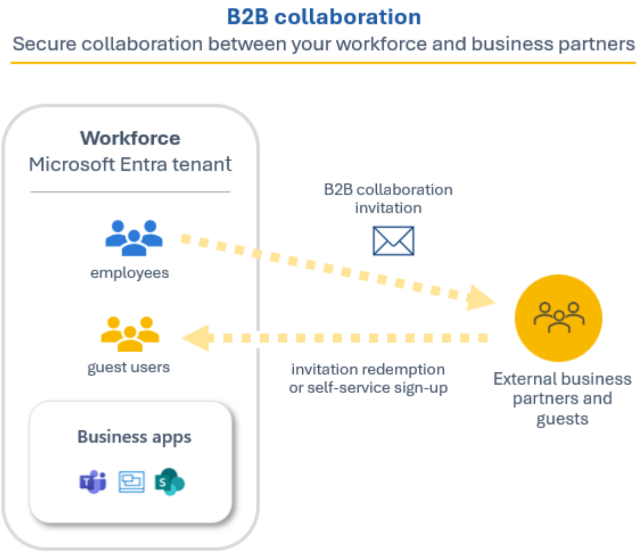

B2B collaboration
Secure collaboration between your workforce and business partners
Workforce
Microsoft Entra tenant
employees
guest users
Business apps
B2B collaboration invitation
invitation redemption or self-service sign-up
External business partners and guests

Figure 18: external ID B2B collabotation

Built into Entra ID, these capabilities also provide enhanced security, compliance, and scalability for your applications.

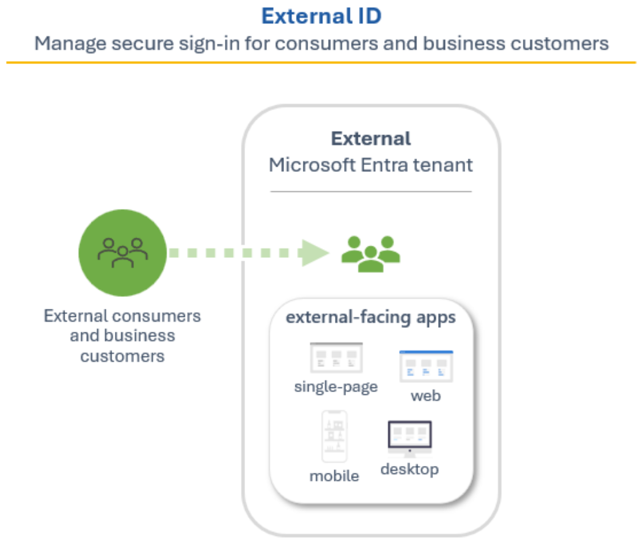

External ID
Manage secure sign-in for consumers and business customers
External
Microsoft Entra tenant
External consumers and business customers
external-facing apps
single-page
web
mobile
desktop

Figure 19: external ID and access management (CIAM)