**[Secure access to your applications by using Azure identity services](https://docs.microsoft.com/en-us/learn/modules/secure-access-azure-identity-services/?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.az-900-describe-identity-governance-privacy-compliance-features)**

# **Compare authentication and authorization**

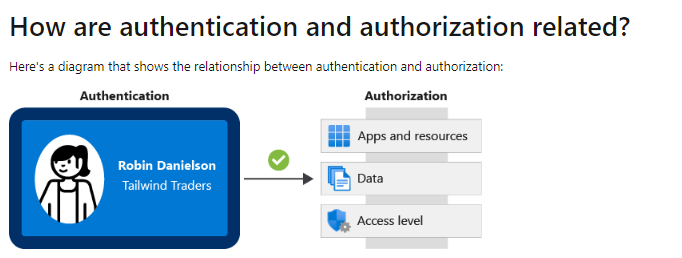
1. Two fundamental concepts that you need to understand when talking about identity and access are **authentication (AuthN) and authorization (AuthZ)**

## **What is authentication?**

1. **Authentication** is the process of **establishing** the **identity** of a person or service
2. It establishes whether the user is who they say they are

## **What is authorization?**

1. **Authorization** is the process of **establishing** what **level** of **access** an authenticated person or service has



# **What is Azure Active Directory?**

1. Azure AD supports single sign-on (SSO)
2. **Scenario:** The Company **doesn't** **want** its **users** to have a **different** **username** and **password** to remember for accessing applications and data in the cloud. **Can** the **company** **integrate** its existing **Active** **Directory** instance with cloud identity services to create a **seamless** experience for its **users**?

## **How does Azure AD compare to Active Directory?**

1. Active Directory is related to Azure AD, but they have some key differences:
   1. Azure AD – Service available **globally**
   2. **On**-**premises** with Active Directory, **Microsoft** doesn't **monitor** **sign**-**in** **attempts**

## **Who uses Azure AD?**

1. **IT administrators**
2. **App developers**
3. **Users**
4. **Online service subscribers: e.g. Office 365.** A tenant is a representation of an organization

## **What services does Azure AD provide?**

1. **Authentication:** This includes verifying identity to access applications and resources. Includes**. Self-service password reset**, **multifactor authentication**, a **custom** **list** of **banned** **passwords**, and **smart** **lockout** services.
2. **Single sign-on: SSO** **enables** you to **remember** only **one** **username** and one **password** to access **multiple** **applications**. . As users change roles or leave an organization, access modifications are tied to that identity
3. **Application management:**  Features like Application Proxy, SaaS apps, the My Apps portal
4. **Device management:** Azure AD supports the registration of devices. **Register** **devices** through **Microsoft** **Intune**.

## **What kinds of resources can Azure AD help secure?**

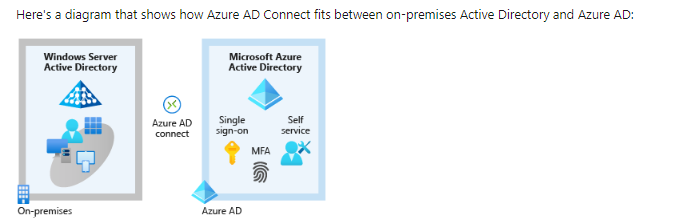
1. **External** **resources** might include **Microsoft** **Office** **365**, the **Azure** **portal** and **(SaaS) applications**
2. **Internal** **resources** might include **apps** on your **corporate** **network** and **intranet**

## **What's single sign-on?**

1. **SSO** enables a **user** to **sign** in **one** **time** and use that credential to access multiple resources and applications
2. **The** **more** **passwords** a user has to manage, the **greater** the **risk** of a credential-related **security** **incident**
3. **Consider** the process of **managing** all those **identities**
4. **With** **SSO**, you need to remember **only** **one** **ID** and **one** **password**

## **How can I connect Active Directory with Azure AD?**

1. **Connecting** **Active** **Directory** with **Azure** **AD** **enables** you to **provide** a **consistent** **identity** **experience** to your **users**
2. Most **popular** **method** of connection is to use **Azure** **AD** **Connect**
3. Azure AD Connect **synchronizes** on premise with **Azure**



# **What are multifactor authentication and Conditional Access?**

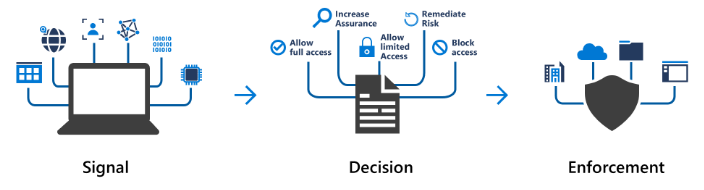
1. **What's multifactor authentication?**
   1. **Multifactor** **authentication** when a **user** is **prompted** during the **sign**-**in** **process** for an **additional** **form** of **identification**.
   2. **Examples** include a code on their **mobile** **phone** or a **fingerprint** **scan**
   3. These elements fall into three categories:
      1. **Something the user knows: Email address or password**
      2. **Something the user has:** Code sent to phone
      3. **Something the user is:** Biometric property

## **What's Azure AD Multi-Factor Authentication?**

1. Service that **provides** multifactor **authentication** capabilities
2. Azure AD **Multi**-**Factor** **Authentication** enables users to choose an **additional** **form** of **authentication** during **sign**-**in**, **e.**g. **Phone**
3. Azure AD Multi-Factor Authentication capabilities:
   1. **Azure Active Directory:**  **Enables** Azure AD Multi-Factor Authentication for **administrators**. Enforce for all users via the Microsoft Authenticator app only.
   2. **Multifactor authentication for Office 365**

## **What's Conditional Access?**

1. **Conditional** **Access** is a **tool** that **Azure** **Active** **Directory** **uses** to **allow** (or **deny**) **access** to resources based on identity **signals**
2. Signals include:
   1. Who the user is
   2. Where the user is
   3. What device
3. Conditional Access helps IT administrators:
   1. **Empower** users to be productive
   2. **Protect** the organization's assets
4. A user **might** **not** be **challenged** for **second** authentication factor if they're at a **known** **location**
5. **During** **sign**-**in**, **Conditional** **Access** **collects** **signals** from the **user**, **makes** **decisions** **based** on those **signals**, and then **enforces**



1. **Signal** might be the user's **location**, the user's **device**, or the **application**

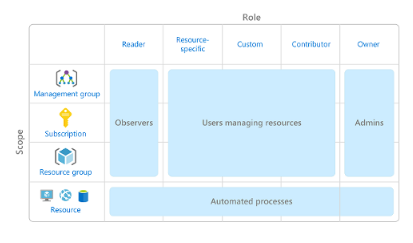
### When can I use Conditional Access?

1. Conditional Access is useful when you need to:
   1. Require **multifactor** **authentication** to access an **application**
   2. Require access to services only through **approved** **client** **applications**
   3. Require users to access your application only from **managed** **devices**
   4. **Block** **access** from **untrusted** **sources**, such as access from unknown or unexpected locations
2. Conditional Access comes with a **What** **If** **tool**
3. To use Conditional Access, you need an **Azure** **AD** **Premium** **P1** or **P2** license

# **2) Control access to cloud resources by using Azure role-based access control**

1. When you have multiple IT and engineering teams, how can you control what access?
2. Azure enables you to control access through [**Azure role-based access control**](https://docs.microsoft.com/en-us/azure/role-based-access-control/overview)**(Azure RBAC)**

## **How is role-based access control applied to resources?**

1. Role-based access control is **applied** to a **scope**
2. **Scope**: set of resources that this access applies to
3. **Scope includes:** Management group, single subscription, resource group and single resource
4. **Observers**, **Users** **managing** **resources**, **Admins**, and **Automated** **processes** illustrate the kinds of **users** or **accounts**
5. When you **grant** **access** at a **parent** scope, those **permissions** are **inherited** by all **child** scopes
6. When you assign the [**Owner**](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#owner) role to a user at the **management** **group** **scope**, that user can **manage** **everything** in all **subscriptions**
7. When you assign the [**Reader**](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#reader) role to a group at the subscription scope, the members of **that** group can **view** **every** resource **group** and resource **within** the subscription

## **When should I use Azure RBAC?**

1. Allow one **user** to **manage** **VMs** in a subscription
2. Allow a **database** **administrator** group to **manage** **SQL** **databases**
3. Allow a **user** to **manage** all **resources** in a **resource** **group**
4. Allow an **application** to **access** all **resources**

## **How is Azure RBAC enforced?**

1. Enforced on any action that's initiated against an Azure resource
2. **Azure** **RBAC** **doesn't** **enforce** access **permissions** at the **application** or **data** level
3. **RBAC** uses an **allow** **model**
4. **RBAC** **allows** you to perform certain **actions**, such as **read**, **write**, or **delete**

## **Who does Azure RBAC apply to?**

1. You can **apply** **Azure** **RBAC** to an **individual** person or to a **group**

## **How do I manage Azure RBAC permissions?**

1. You manage access permissions on the **Access control (IAM)** pane in the Azure portal

# **Prevent accidental changes by using resource locks**

1. A [**resource lock**](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources) **prevents** resources from being **accidentally** **deleted** or **changed**
2. **Even** with **Azure** **role**-**based** access control (**Azure** **RBAC**) **policies** in place, there's still a **risk** that **people** with the right level of access could **delete** critical cloud resources
3. **Resource** **lock** is a **warning** **system** that **reminds** you that a **resource** should not be **deleted** or **changed**

## **How do I manage resource locks?**

1. From **Azure** **portal**, **PowerShell**, the **Azure** **CLI**, or from an **Azure** **Resource** **Manager** **template**
2. Go to the **Settings** section of any resource's **Settings** pane in the Azure portal.

## **What levels of locking are available?**

1. You can **apply** **locks** to a **subscription**, a **resource** **group**, or an **individual** **resource**.
   1. Lock Levels:
      1. **CanNotDelete**
      2. **ReadOnly**

## **How do I delete or change a locked resource?**

1. To modify a locked resource, you must first remove the lock
2. After you remove the lock, you can apply any action you have permissions to perform

## **Combine resource locks with Azure Blueprints**

1. What if a cloud administrator **accidentally** deletes a **resource** **lock**?
2. To make the protection **process** **more** **robust**, you can combine resource locks with **Azure** **Blueprints**

## **Organize your Azure resources by using tags**

1. Resource **tags** are **another** way to **organize** **resources**
2. **Tags** provide **extra** **information**, or **metadata**, about your resources
3. This metadata is useful for:
   1. **Resource management**
   2. **Cost management and optimization**
   3. **Operations management**
   4. **Security**
   5. **Governance and regulatory compliance**
   6. **Workload optimization and automation**

## **How do I manage resource tags?**

1. You can **add**, **modify**, or **delete** resource **tags** through **PowerShell**, **the Azure CLI**, **Azure Resource Manager** templates, the **REST** **API**, or the **Azure** **portal**
2. You can also **manage** **tags** by using **Azure** **Policy**
3. Mission-critical resources have the **Impact** tag

# **Control and audit your resources by using Azure Policy**

1. [**Azure Policy**](https://azure.microsoft.com/services/azure-policy) is a service in Azure that enables you to **create**, **assign**, and **manage** **policies** that **control** or **audit** your **resources**

## **How does Azure Policy define policies?**

1. Can have **individual** **policies** and **groups** of **related** **policies,** knownas **initiatives**
2. Can be applied to **Storage**, **Networking**, **Compute**, **Security** **Center**, and **Monitoring**
3. After you **enable** a **policy**, that **policy** is **applied** when you create **new** **VMs**

## **Azure Policy in action**

1. Implementing a policy in Azure Policy involves these three steps:
   1. Create a policy definition:
      1. A policy definition **expresses** what to **evaluate** and what **action** to take. Here are some Examples:
         1. **Allowed virtual machine SKUs**
         2. **Allowed locations**
         3. **MFA should be enabled on accounts with write permissions on your subscription**
         4. **CORS should not allow every resource to access your web applications**
         5. **System updates should be installed on your machines**
   2. Assign the definition to resources
      1. To implement your policy definitions, you assign definitions to resources
      2. A **policy** **assignment** is a **policy** **definition** that takes place within a specific scope. Scope being **Management** **Group**, **single** **subscription** or resource **group**.
   3. Review the evaluation results
      1. When a **condition** is **evaluated** against your existing **resources**, each resource is marked as **compliant** or **noncompliant**

## **What are Azure Policy initiatives?**

1. An **Azure** **Policy** **initiative** is a way of **grouping** related **policies** into **one** **set**
2. **Azure** **Policy** includes an initiative named **Enable Monitoring in Azure Security Center**
3. This initiative does the following:
   1. **Monitor unencrypted SQL Database in Security Center**
   2. **Monitor OS vulnerabilities in Security Center**
   3. **Monitor missing Endpoint Protection in Security Center**

### How do I define an initiative?

1. By using the Azure Portal

### How do I assign an initiative?

1. **Assigned** to a specific scope of a **management** **group**, a **subscription**, or a **resource** **group**

# **Govern multiple subscriptions by using Azure Blueprints**

1. What happens when you have to **scale** **subscriptions**?
2. Instead of using Azure Policy for each subscription, you can use Azure Blueprints
3. Azure Blueprints orchestrates:
   1. Role Assignments
   2. Policy Assignments
   3. Azure Resource Manager Templates
   4. Resource Groups

## **Azure Blueprints in action**

1. Implementing a Blueprint involves 3 steps:
   1. Create an Azure blueprint
   2. Assign the blueprint
   3. Track the blueprint
2. Blueprints are also **versioned**

## **What are blueprint artifacts?**

1. **Each** **component** in the **blueprint** definition is known as an **artifact**
2. It is **possible** for **artifacts** to have **no** additional **parameters** or configurations.

## **How will Tailwind Traders use Azure Blueprints for ISO 27001 compliance?**

1. **Azure** **Blueprints** has several **built**-**in** blueprint definitions that relate to **ISO 27001**

# **Accelerate your cloud adoption journey by using the Cloud Adoption Framework for Azure**

1. The **Cloud** **Adoption** **Framework** helps you **create** and **implement** the **business** and **technology** strategies needed to **succeed** in the **cloud**
2. The Cloud Adoption Framework includes these stages: (DMRAG)
   1. **Define your strategy:**
      1. Here are the steps in this stage
         1. **Define and document your motivations**
         2. **Document business outcomes**
         3. **Evaluate financial considerations**
         4. **Understand technical considerations**
   2. **Make a plan**
      1. Here are the steps in this stage
         1. **Digital estate**: Create an inventory of the existing digital assets
         2. **Initial organizational alignment**: Ensure that the right people are involved
         3. **Skills readiness plan**: Build a plan that helps individuals build the skills
         4. **Cloud adoption plan**: Brings teams toward a shared cloud adoption goal
   3. **Ready your organization**
      1. Here are the steps in this stage
         1. **Azure setup guide**: Review the Azure setup guide and become familiar
         2. **Azure landing zone**: Begin to build out the Azure subscriptions
         3. **Expand the landing zone**: Refine your landing zone
         4. **Best practices**: Start with recommended and proven practices
   4. **Adopt the cloud**
      1. Here are the steps in this stage
         1. **Migrate**
            1. **Migrate your first workload**:
            2. **Migration scenarios**
            3. **Best practices**
            4. **Process improvements**
         2. **Innovate**
            1. **Business value consensus**
            2. **Azure innovation guide**
            3. **Best practices**
            4. **Feedback loops: Check in with customers**
   5. **Govern and manage your cloud environments**
      1. **Govern**:
         1. **Methodology**
         2. **Benchmark**
         3. **Initial governance foundation**
         4. **Improve the initial governance foundation**
      2. **Manage**
         1. **Establish a management baseline**
         2. **Define business commitments**
         3. **Expand the management baseline**
         4. **Advanced operations and design principles**

# **Create a subscription governance strategy**

1. There are three main aspects to consider when you create and manage subscriptions:
   1. **Billing:** You can create one billing report per subscription.
   2. **Access Control:** Each tenant provides administrators the ability to set granular access through defined roles
   3. **Subscription Limits:** Azure **ExpressRoute** circuits per subscription is **10.**

**Check your knowledge**

1. <https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/11-knowledge-check>

### [Examine privacy, compliance, and data protection standards on Azure](https://docs.microsoft.com/en-us/learn/modules/examine-privacy-compliance-data-protection-standards/?ns-enrollment-type=LearningPath&ns-enrollment-id=learn.az-900-describe-identity-governance-privacy-compliance-features)

# **Explore compliance terms and requirements**

1. **Microsoft's** online **services** **build** upon a common set of **regulatory** and **compliance** **controls**
2. Think of a **control** as a **known** **good** **standard** that you can **compare** your solution against to ensure **security**

## **Which compliance categories are available on Azure?**

1. **Global**, **US** **Government**, **Industry**, and **Regional**

### Criminal Justice Information Service

1. Azure is the only major cloud provider that contractually commits to conformance with the CJIS Security Policy

### Cloud Security Alliance STAR Certification

1. **Azure**, **Intune**, and **Microsoft** **Power** **BI** have obtained Cloud Security Alliance (CSA) STAR Certification
2. **STAR** **Certification** is based on **achieving** **International** **Organization** of **Standards**/**International** **Electrotechnical** **Commission** **(ISO/IEC) 27001**
3. This certification demonstrates that a cloud service provider:
   1. **Conforms** to the applicable requirements of **ISO/IEC 27001.**
   2. Has **addressed** issues critical to **cloud** **security** as outlined in the **Cloud** **Controls** **Matrix** **(CCM)**
   3. Has been assessed against the STAR Capability Maturity Model

### European Union Model Clauses

1. **Microsoft** is the **first** **company** to receive joint approval from **the EU's Article 29**

### Health Insurance Portability and Accountability Act

1. The **Health** **Insurance** **Portability** and **Accountability** **Act** **(HIPAA)**
2. **Azure** offers **customers** a **HIPAA** **Business** **Associate** **Agreement** **(BAA)**

### International Organization of Standards/International Electrotechnical Commission 27018

1. **Microsoft** is the **first** **cloud** **provider** to have **adopted** the **ISO/IEC 27018** code of practice

### Multi-Tier Cloud Security Singapore

1. **Microsoft** cloud services received **MTCS** 584:2013 Certification across all three service classifications:
   1. Infrastructure as a service (IaaS)
   2. Platform as a service (PaaS)
   3. Software as a service (SaaS

### Service Organization Controls 1, 2, and 3

1. Microsoft-covered cloud services are **audited** at **least** **annually** against the Service Organization Controls (SOC) report framework
2. **Audit** **covers** controls for **data** **security**, **availability**, **processing** **integrity**, and **confidentiality**

### National Institute of Standards and Technology Cybersecurity Framework

1. Is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risks

### United Kingdom Government G-Cloud

1. **Cloud** **computing** **certification** for **services** used by **government** **entities** in the **United** **Kingdom**.
2. **Azure** has received official **accreditation** from the **UK** **government**

# **Access the Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum**

1. You learn how the **Microsoft** **Privacy** **Statement**, the **Online** **Services** **Terms**, and the **Data** **Protection** **Addendum** explain the personal data **Microsoft** collects, how **Microsoft** **uses** it, and for **what** **purposes**

## **What's in the Microsoft Privacy Statement?**

1. The **Microsoft** **Privacy** **Statement** **explains** what **personal** **data** **Microsoft** **collects**, how Microsoft **uses** it, and for **what** purposes
2. The privacy statement covers all of **Microsoft's** **services**, **websites**, **apps**, **software**, **servers**, and **devices**
3. Also relevant to Windows and XBOX

## **What's in the Online Services Terms?**

1. The [**Online Services Terms**](https://www.microsoft.com/licensing/terms/product/ForallOnlineServices)**(OST)** is a **legal** **agreement** between **Microsoft** and the **customer**
2. The **OST** **details** the **obligations** by **both** **parties**

## **What is the Data Protection Addendum?**

1. The **Data** **Protection** **Addendum** **(DPA)** **further** defines the **data** **processing** and **security** **terms** for **online** **services**
2. **Includes:**
   1. Compliance with laws
   2. Disclosure of processed data
   3. Data Security
   4. Data transfer, retention, and deletion

# **Explore the Trust Center**

1. The [**Trust Center**](https://www.microsoft.com/trust-center?rtc=1%3Fazure-portal%3Dtrue)**showcases** **Microsoft's** **principles** for **maintaining** **data** **integrity** in the **cloud** and how **Microsoft** **implements** and supports **security**, **privacy**, **compliance**, and **transparency** in all Microsoft cloud products and services

# **Access Azure compliance documentation**

1. Payment Card Industry (**PCI**) Data Security Standard (**DSS**).

## **What is the Azure compliance documentation?**

1. The [**Azure compliance documentation**](https://docs.microsoft.com/en-us/azure/compliance/)**provides** you with **detailed** **documentation** about **legal** and **regulatory** **standards** and **compliance** on **Azure**
2. Compliance on these:
   1. Global
   2. US Government
   3. Financial Services
   4. Health
   5. Media
   6. Regional

# **What is Azure Government?**

1. [**Azure Government**](https://azure.microsoft.com/global-infrastructure/government) is a **separate** **instance** of the **Microsoft** **Azure** service
2. **Addresses** the **security** and **compliance** **needs** of **US** **federal** **agencies**, state and local governments, and their solution providers

# **What is Azure China 21Vianet?**

1. Operated by 21Vianet
2. It's a **physically** **separated** **instance** of cloud services located in **China**

## **Azure products and services available in China**

1. **Azure** **agreements** and **contracts** in **China**, where applicable, are **signed** between **customers** and **21Vianet**
2. **Azure** **China** **21Vianet** **supports** most of the same services that **global** **Azure**

**Knowledge Check**

https://docs.microsoft.com/en-us/learn/modules/examine-privacy-compliance-data-protection-standards/8-knowledge-check