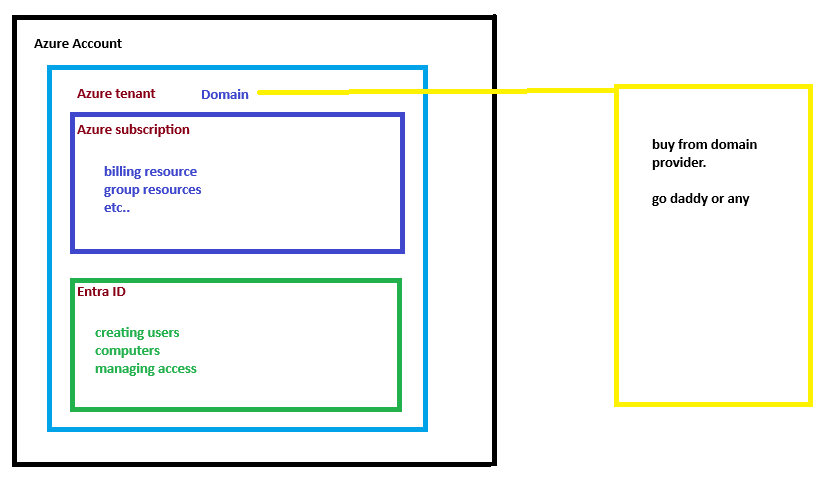
Microsoft Entra ID –

To understand this first we need to understand Microsoft account, tenant, subscription hierarchy.

Then we can understand where the entra id is getting created how can we create and maage it.

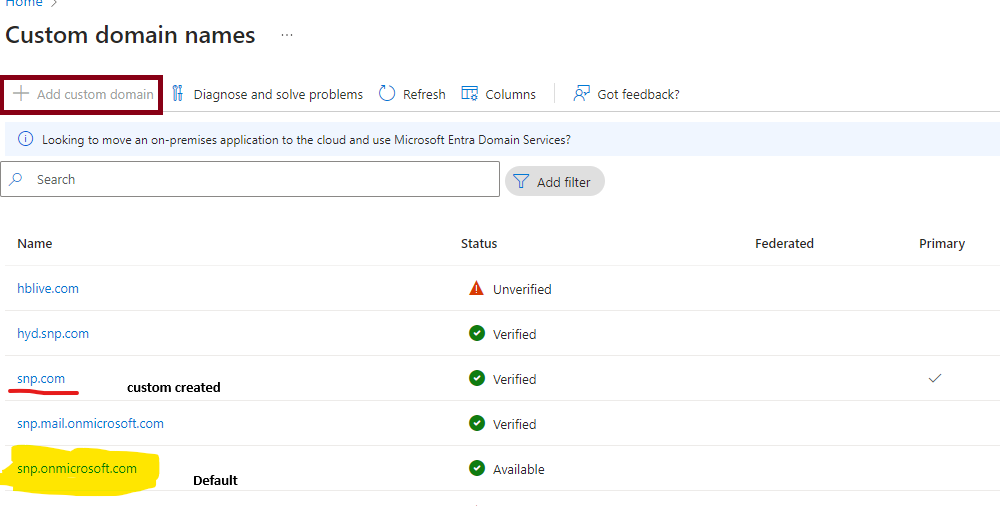


When we create a Microsoft azure account along with that account out tenant (which is globally unique, and it has a unique ID) a default domain (account name.onmicrosoft.com) a subscription (free or pay as you go. What we choose) and an entra id will be created. Also it will have a default domain name same as account name name.onmicrosoft.com.

Then we can create multiple subscriptions under the tenant and all subscription will have different billing. We can create resources in subscription.

The entra id will be used as azure AD it manages users, devices. Allow users to resources sub etc..

Now if we want a Domain name for us other then default domain given by azure. We can go to any domain name provider such as go daddy or any and can use that domain name in azure.



**Azure Hierarchy**

1. **Tenant**:
   * A tenant is a dedicated instance of Azure Active Directory (Azure AD) that an organization receives when it signs up for a Microsoft cloud service like Azure, Microsoft 365, or Dynamics 365. It contains user accounts and groups
2. **Subscription**:
   * A subscription is an agreement with Microsoft to use Azure services. It is linked to a tenant and can contain multiple resource groups and resources. Subscriptions help manage costs and resources, and each subscription has its own billing and usage reports
3. **Resource Group**:
   * A resource group is a container that holds related resources for an Azure solution. It includes resources like virtual machines, databases, and storage accounts. Resource groups help manage and organize resources based on lifecycle and permissions
4. **Resources**:
   * These are instances of services that you create, such as virtual machines, web apps, databases, and storage accounts. Resources are deployed into resource groups

**How It Works**

When you create an Azure account, you typically follow these steps:

1. **Create an Azure Account**:
   * Sign up for an Azure account, which automatically creates a tenant in Azure AD.
2. **Create a Subscription**:
   * After creating your account, you need to create a subscription. This subscription will be linked to your tenant and will be used to manage billing and resource usage.
3. **Create Resource Groups**:
   * Within your subscription, you create resource groups to organize your resources. Each resource group can contain multiple resources that share the same lifecycle and permissions.
4. **Deploy Resources**:
   * Finally, you deploy resources within your resource groups. These resources can be anything from virtual machines to databases, depending on your needs.

**Example**

Imagine you have a company called Contoso. Here's how you might set up your Azure environment:

* **Tenant**: Contoso's Azure AD tenant.
* **Subscription**: Contoso's Azure subscription for production workloads.
* **Resource Groups**:
  + Prod-WebApps for production web applications.
  + Prod-Databases for production databases.
* **Resources**:
  + Virtual machines, SQL databases, storage accounts, etc., within the respective resource groups.

Microsoft Entra ID, formerly known as Azure Active Directory (Azure AD), is a cloud-based identity and access management service. It plays a crucial role in managing identities and access to resources in Azure. Here's how it fits into the Azure hierarchy and how it works:

**Microsoft Entra ID in Azure Hierarchy**

1. **Tenant Level**:
   * **Tenant**: When you create an Azure account, you automatically get a Microsoft Entra ID tenant. This tenant is a dedicated instance of Microsoft Entra ID that contains your users, groups, and applications. It is the top-level container for identity management.
   * **Domain**: Your tenant will have a default domain in the format yourcompany.onmicrosoft.com. You can add custom domains (e.g., parthasarathi.com) to your tenant.
2. **Subscription Level**:
   * **Subscription**: Each subscription is linked to a Microsoft Entra ID tenant. Subscriptions are used to manage billing and resource usage. Multiple subscriptions can be associated with a single tenant.
3. **Resource Group and Resource Level**:
   * **Resource Groups**: Within a subscription, you create resource groups to organize your resources.
   * **Resources**: These are the actual services and applications you deploy, such as virtual machines, databases, and web apps.

**How Microsoft Entra ID Works**

1. **Identity Management**:
   * **User Accounts**: Create and manage user accounts within your tenant. Users can be employees, partners, or customers.
   * **Groups**: Organize users into groups to simplify management and access control.
2. **Access Management**:
   * **Single Sign-On (SSO)**: Users can sign in once and access multiple applications, including Microsoft 365, the Azure portal, and other SaaS applications.
   * **Conditional Access**: Implement policies to control how and when users can access resources based on conditions like location, device, and risk level
3. **Security Features**:
   * **Multifactor Authentication (MFA)**: Enhance security by requiring additional verification methods.
   * **Identity Protection**: Detect and respond to identity-based risks using machine learning and behavioral analytics
4. **Integration with Azure Services**:
   * **Azure Resources**: Use Microsoft Entra ID to manage access to Azure resources. For example, you can assign roles to users and groups to control access to virtual machines, databases, and other services.
   * **Hybrid Identity**: Integrate on-premises Active Directory with Microsoft Entra ID to provide a unified identity for accessing both on-premises and cloud resources

**Example**

Imagine you have a company called Contoso:

* **Tenant**: Contoso's Microsoft Entra ID tenant (contoso.onmicrosoft.com).
* **Custom Domain**: Added parthasarathi.com to the tenant.
* **Subscription**: Contoso's Azure subscription linked to the tenant.
* **Resource Groups**: Prod-WebApps, Prod-Databases.
* **Resources**: Virtual machines, SQL databases, storage accounts.

By using Microsoft Entra ID, you can manage identities, control access, and secure your resources effectively within Azure

Can we create multiple entra id for one tenant?

No, you cannot create multiple Microsoft Entra ID (formerly Azure AD) instances within a single tenant. Each tenant is a unique instance of Microsoft Entra ID and serves as the top-level container for identity management, including users, groups, and applications.

**Key Points**

* **Single Entra ID per Tenant**: Each Azure tenant has one Microsoft Entra ID instance. This instance is used to manage all identities and access within that tenant
* **Multiple Tenants**: If you need separate identity management environments, you can create multiple tenants. Each tenant will have its own Microsoft Entra ID instance
* **Multitenant Organizations**: For organizations that need to manage multiple tenants, Microsoft Entra ID offers multitenant capabilities. This allows for cross-tenant collaboration and management, such as B2B collaboration and cross-tenant synchronization

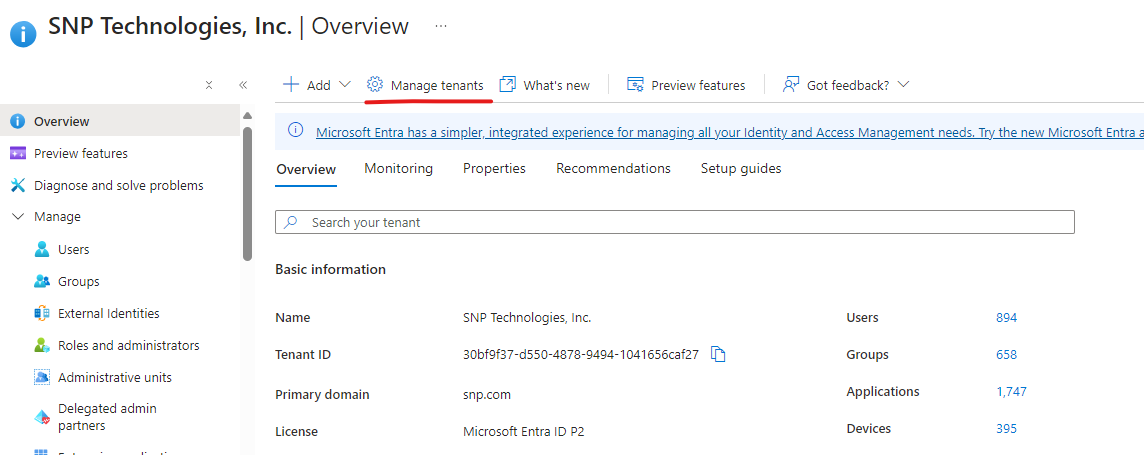
**Example Scenarios**

1. **Single Tenant**:
   * Your company, Contoso, has one tenant (contoso.onmicrosoft.com). All users, groups, and applications are managed within this single Microsoft Entra ID instance.
2. **Multiple Tenants**:
   * If Contoso acquires another company, Fabrikam, and wants to keep their identity management separate, they can create a new tenant (fabrikam.onmicrosoft.com). Each tenant will have its own Microsoft Entra ID instance.
3. **Multitenant Organization**:
   * Contoso and Fabrikam can use multitenant capabilities to enable seamless collaboration between their tenants. This includes features like cross-tenant access settings and B2B direct connect

This is azure managed active directory to manage users devise and assign permissions.

Go to azure portal and then go for Microsoft entra id.

Go to manage tenants.

****

how microsoft intune are related to entra id how does this works?

Microsoft Intune and Microsoft Entra ID (formerly Azure AD) are closely related and work together to provide comprehensive identity and device management solutions. Here's how they are connected and how they work:

**Relationship Between Microsoft Intune and Entra ID**

1. **Identity Management with Entra ID**:
   * **Microsoft Entra ID** is a cloud-based identity and access management service. It provides identity management and access control capabilities, ensuring secure access to applications and resources. It includes features like user and group management, single sign-on (SSO), and multifactor authentication (MFA)
2. **Device and Application Management with Intune**:
   * **Microsoft Intune** is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). It allows organizations to manage devices, enforce security policies, and ensure that applications are securely deployed and managed

**How They Work Together**

1. **Integration**:
   * Intune relies on Microsoft Entra ID for identity management. When you enroll devices in Intune, they are registered with Entra ID. This integration ensures that only authenticated and authorized users can access corporate resources
2. **Device Enrollment**:
   * Devices can be enrolled in Intune through various methods, such as automatic enrollment for Entra ID-joined devices, manual enrollment, or using provisioning packages. Once enrolled, Intune can manage these devices, enforce policies, and deploy applications
3. **Policy Enforcement**:
   * Intune uses Entra ID to apply conditional access policies. These policies can restrict access to resources based on device compliance status, user location, and other factors. For example, you can require that devices meet certain security standards before accessing sensitive data
4. **Unified Management**:
   * The integration of Intune with Entra ID provides a unified management experience. Administrators can manage users, devices, and applications from a single console. This simplifies the management process and enhances security

**Example Scenario**

Imagine your organization, Contoso, uses Microsoft Entra ID and Intune:

* **User Enrollment**: Employees' devices are enrolled in Intune and registered with Entra ID.
* **Policy Application**: Intune applies security policies, such as requiring devices to have encryption and a passcode.
* **Conditional Access**: Entra ID enforces conditional access policies, ensuring that only compliant devices can access corporate email and data.
* **Unified Management**: Administrators manage users, devices, and applications through the Intune and Entra ID portals.

**Additional Resources**

* Microsoft Entra ID Overview
* Microsoft Intune Overview
* Enroll Devices in Intune

How to update logo for office 365?

**To change your company Logo in Microsoft 365 and Azure, follow these steps:**

**Microsoft Azure**

1. **Sign in to the Azure portal with your account.**
   * Navigate to Microsoft Entra ID.
2. **Select "Company Branding" under the "Manage" section.**
   * Click "Default Sign-In" to start customizing your existing branding.
3. **Upload the new company logo and make any necessary adjustments.**
   * You can upload the new logo in place of old Logo.
   * Save your changes.

**Office 365**

1. **Sign in to the Office 365 admin center.**
   * Navigate to ORG Settings under settings section
2. **Under ORG Settings, Click ORG Profile.**
   * Under ORG Profile, Click Custom themes.
3. **Upload the new company logo and make any necessary adjustments.**
   * Click save changes.

**To change your company name in Microsoft 365 and Azure, follow these steps:**

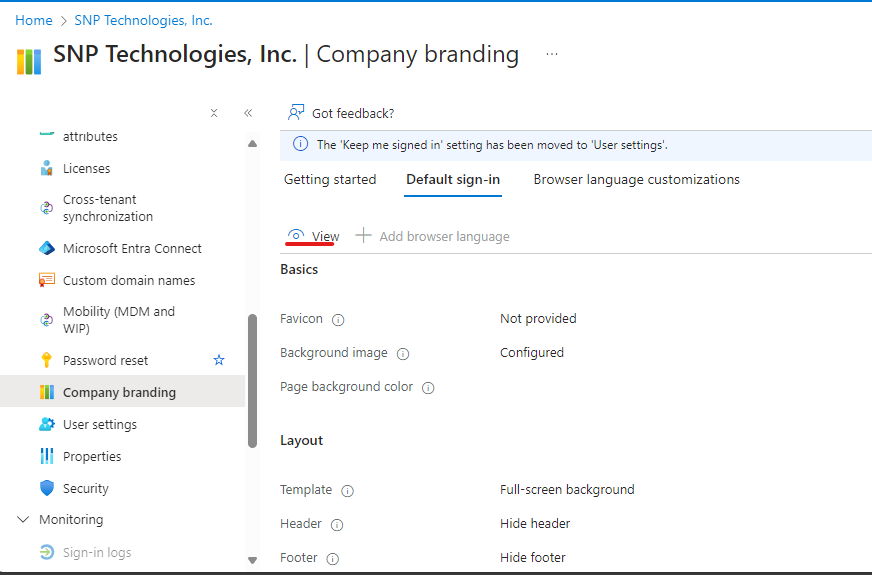
**For Microsoft 365**

1. **Sign in to the Microsoft 365 Admin Center**:
   * Go to the Microsoft 365 Admin Center.
   * Use your admin credentials to sign in.
2. **Navigate to Organization Profile**:
   * In the left-hand menu, select Settings.
   * Under Settings, choose Org settings.
   * Select Organization profile and then Organization information.
3. **Update Your Organization's Name**:
   * Edit the Name field with your new company name.
   * Save your changes

**For Azure (Microsoft Entra ID)**

1. **Sign in to the Azure Portal** **using your admin credentials:**
   * Go to the Azure Portal.
   * Use your admin credentials to sign in.
2. **Access Azure Active Directory**:
   * In the left-hand menu, select Microsoft Entra ID.
   * Under Manage, select Company branding.
3. **Update Company Name**:
   * Edit the Name field with your new company name.
   * Save your changes

Reference Article for more information:  <https://learn.microsoft.com/en-us/entra/fundamentals/how-to-customize-branding>



how to enable mfa based security requiredment for each users on entra id?

Enabling Multi-Factor Authentication (MFA) for users in Microsoft Entra ID (formerly Azure AD) enhances security by requiring additional verification methods during sign-in. Here’s how you can enable MFA for each user:

**Steps to Enable MFA for Users in Microsoft Entra ID**

1. **Sign in to the Azure Portal**:
   * Go to the Azure portal and sign in with an account that has the Global Administrator role.
2. **Navigate to Azure Active Directory**:
   * In the left-hand navigation pane, select **Azure Active Directory (Entra ID)**.
3. **Access MFA Settings**:
   * Under **Manage**, select **Users**.
   * In the **Users** pane, select **Per-user MFA**.
4. **Enable MFA for Users**:
   * You will see a list of users. Select the users for whom you want to enable MFA.
   * Click on **Enable** at the top of the page.
5. **Configure MFA Settings**:
   * After enabling MFA, users will be prompted to configure their MFA settings the next time they sign in. They can choose from various verification methods, such as the Microsoft Authenticator app, phone call, or SMS.

**Using Conditional Access Policies (Recommended)**

For more granular control, you can use Conditional Access policies to enforce MFA:

1. **Create a Conditional Access Policy**:
   * In the Azure portal, navigate to **Azure Active Directory** > **Security** > **Conditional Access**.
   * Click on **+ New policy**.
2. **Define Policy Conditions**:
   * Name your policy (e.g., "Require MFA for All Users").
   * Under **Assignments**, select **Users and groups** and choose the users or groups to which the policy will apply.
   * Under **Cloud apps or actions**, select the applications that require MFA.
3. **Set Access Controls**:
   * Under **Access controls**, select **Grant**.
   * Choose **Require multi-factor authentication** and click **Select**.
4. **Enable the Policy**:
   * Set the policy to **On** and click **Create**.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated