**Agenda: Azure Active Directory**

* Azure AD Introduction
* Azure AD Editions
* Managing Active Directories
* Adding a custom domain name to Azure AD
* Managing Azure AD Users, Groups and Devices
* Synchronizing On-Premise AD Identities with Azure AD
* Azure AD User Sign-In Options

**Azure Active Directory Introduction**

* Microsoft Azure Active Directory (Azure AD) is a **multi-tenant** cloud-based **identity and access management solution** for the resources that exist in the cloud.
* Azure AD is highly scalable and highly available by design. Therefore, organizations do not have to maintain related infrastructure or worry about disaster recovery. Running out of multiple data centers around the world with **automated failover**, you’ll have the comfort of knowing that Azure AD is highly reliable and that even if a data center goes down, copies of your directory data are live in at **least two** more regionally dispersed data centers and available for instant access.
* Many applications built on different platforms such as **.Net, Java, Node.js, Python, Go and PHP** can use industry standard protocols such as **Security Assertion Markup Language (SAML) 2.0**, **WS-Federation**, and **OpenID Connect** to integrate the identity management provided by Azure AD into the application logic. Through the support of **OAuth 2.0**, developers can develop mobile and web service applications that integrate with Microsoft’s identity platform for cloud authentication and access management.
* Azure AD provides access to its content via **REST-based Graph API**, rather than by Lightweight Directory Access Protocol (LDAP), on which Active Directory relies.

**You can use Azure AD to:**

* Provide an identity management solution.
* Manage users and groups.
* Role based Access Control (RBAC).
* Enable federation between organizations.
* Identify irregular sign-in activity.
* Configure SSO to cloud-based SaaS applications like Microsoft365, Salesforce.com, DropBox etc…
* Configure access to the on-premise applications.
* Configure multi-factor authentication (MFA).
* Extend existing on-premises Active Directory implementations to Azure AD.

**Azure AD editions:**

* **Free edition** provides
  + User and group management
  + Self-service **password change** for cloud users.
  + **Synchronize** with on-premises directories.
  + Get **single sign-on** across Azure, Office 365, and thousands of popular SaaS applications like Salesforce, Workday, Concur, DocuSign, Google Apps, Box, ServiceNow, Dropbox, and more.
  + End-users are entitled to get single sign-on access for **up to 10 applications**.
* **Premium P1 edition** is designed for task workers with cloud-first needs.It supports
  + Extends the free edition’s capabilities
  + Company Branding (Logon Pages / Access Panel customization)
  + Self-service **password reset** for cloud users.
  + Azure Active Directory Application Proxy (to publish on-premises web applications using Azure Active Directory)
  + Multi-Factor Authentication (MFA)
  + Self-service identity and access management (IAM)
  + Advanced reports for security and usage information.
  + Dynamic groups and self-service group management.
  + Microsoft Identity Manager (an on-premises identity and access management suite)
  + Self-service password reset **with password writeback** for on-premises users.
* **Premium P2 edition** is designed to accommodate organizations with more demanding identity and access management needs.It supports
  + All features of Azure AD Premium P1
  + Azure Active Directory **Identity Protection** leverages billions of signals to provide risk-based conditional access to your applications and critical company data.
  + We also help you manage and protect privileged accounts with Azure Active Directory **Privileged Identity Management** so you can discover, restrict and monitor administrators and their access to resources and provide **just-in-time access** when needed.

**Comparison Between Editions**

**[https://azure.microsoft.com/en-in/pricing/details/active-directory](https://azure.microsoft.com/en-in/pricing/details/active-directory/?&ef_id=EAIaIQobChMI8o3y-9ip5QIVyzUrCh16pAAQEAAYASAAEgK1GfD_BwE:G:s&OCID=AID2000081_SEM_NdagNnl8&MarinID=NdagNnl8_342698145259_azure%20ad%20pricing_e_c__62389845774_kwd-322430644000&lnkd=Google_Azure_Brand&dclid=CN6krP3YqeUCFU6Fjwod55MOXQ)**

**Working with Azure AD Tenant**

**Azure Accounts**

* Any user with Microsoft ID (Outlook / Hotmail / MSN / Skype / etc…) can create an Azure Subscription.

**Default Roles Assined to User when the first subscription is created:**

1. Global Administrator for AD Tenant
2. Account Administrator is able to manage billing and invoice related issues of Subscription.
3. Service Administrator is to manage Azure Services like VM, Storage etc...

### Tenants and Initial Domain

* A tenant is simply a dedicated **instance** of Microsoft Entra ID that your organization receives and owns when it signs up for a Microsoft cloud service such as Azure or Office 365.
* Every Tenant has a unique ID and initial domain name in the form **xxxxxxx.onmicrosoft.com**.
* A tenant houses the users in a company and the information about them - their passwords, user profile data, permissions, and so on.
* It also contains groups, applications, and other information pertaining to an organization and its security.
* You can have multiple tenants within your organization. Each tenant can have a different purpose and fulfill a different scenario. For example, you might have tenant for Testing, Office365, and Production.

**Adding a New Directory / Tenant:**

1. Azure Active Directory 🡪 Manage tenants 🡪 **Create**
2. Add Directory Dialog,
   * Name = Sandeep Demo Organization
   * Domain Name = **sandeepdemoorg**.onmicrosoft.com
   * Country = INDIA
3. Refresh your browser
4. **To change directory:**

Click the Gear Icon in Toolbar 🡪 Swith to All Directories 🡪 Select Switch againt your New Tenant

A screenshot of a computer

Description automatically generated

Note that you are a Global Administrator for the New AD Tenant Created/

**Activate Azure AD Premium P2 trial**

1. In the Azure portal, while signed in by using the Microsoft account that has the **Owner role** in the Azure subscription and is a **Global Administrator** of the Azure AD tenant associated with that subscription, navigate to the Azure AD tenant blade.
2. From the Azure AD tenant blade, navigate to the **Licenses** blade.
3. From the **Licenses** blade, navigate to the **Licenses - All products** blade.
4. From the **Licenses - All products** blade, navigate to the **Activate** blade and activate the **Azure AD Premium P2** trial.

**Assign Azure AD Premium P2 licenses**

1. Navigate to the **Users - All users** blade of the Azure AD tenant associated with your Azure subscription.
2. From the **Users - All users** blade, display the [**admin@sandeepsonideccansoft.onmicrosoft.com**](mailto:admin@sandeepsonideccansoft.onmicrosoft.com) **- Profile** blade.
3. **Edit** **Settings** 🡪 **Usage location** matching the location of the Azure AD tenant.
4. Navigate back to the **Licenses - Overview** blade of the Azure AD tenant associated with your Azure subscription.
5. From the Azure Active Directory 🡪 **Licenses - Overview** blade, navigate to the **Products** blade.
6. From the **Products** blade, navigate to the **Azure Active Directory Premium P2 - Licensed users** blade.
7. From the **Azure Active Directory Premium P2 - Licensed users**, navigate to the **Assign license** blade.
8. From the **Assign license** blade, assign an Azure AD Premium P2 license to the [**admin@sandeepsonideccansoft.onmicrosoft.com**](mailto:admin@sandeepsonideccansoft.onmicrosoft.com)user account.

**Deleting an Azure AD directory:**

By using a user account with global administrative rights, you can delete an Azure AD directory if the following conditions are met:

1. You deleted all the users in the directory except the Global Administrator for the directory that you want to delete. The Global Administrator’s name cannot have the same suffix as the directory you intend to delete.
2. All applications configured for SSO are removed from the directory.
3. The directory is not associated with any of the cloud services such as Azure, Microsoft 365, or Azure AD Premium.
4. No multi-factor authentication providers are linked to the directory.

**Step:** Azure Portal 🡪 Switch to the Directory from the Menu on top right 🡪 Azure Active Directory 🡪 Delete directory (in menu of overview blade)

## Add a custom domain name to Azure AD

Although the initial domain name for a directory can't be changed or deleted, you can add any routable custom domain name you control. This simplifies the user sign-on experience by allowing user to logon with credentials they are familiar with.

Only a global administrator can perform domain management tasks in Azure AD.

**Adding and Verifying Custom Domain Names**

1. Azure Portal 🡪 **Azure** **Active Directory** 🡪 Domain names 🡪 + **Add domain name**.
2. Enter the name of your custom domain, such as **'deccansoft.net**'.   
   Be sure to include the .com, .net, or other top-level extension, and leave the checkbox for "single sign-on" (federation) cleared 🡪 Add
3. In the Microsoft cloud service portal, note the DNS records that will need to be created at your domain registrar or DNS hosting provider.
4. Sign-in to your domain registrar or DNS hosting provider, and create the DNS records.

Note: A domain name can be verified in only a single directory. If a domain name was previously verified in another directory, it must be deleted there before it can be verified in your new directory.

You can add up to **900 custom domain** names to each Azure AD directory.

Azure AD provides the required DNS information, either TXT (preferably), or MX records if your DNS provider does not support TXT records.

The following is an example of a TXT record used for custom domain verification:

Alias or Host name: **@**

Destination or Points to Address: **MS=ms96744744**

TTL: **1 hour**

After verification, the administrator can make the domain the primary domain for the Azure tenant. For example, you can replace adatum12345.onmicrosoft.com with adatum.com, so that new users will be automatically created in this directory.

## Delete a custom domain name

To delete a custom domain name, you must first ensure that no resources in your directory rely on the domain name.

You can't delete a domain name from your directory if:

* Any user has a user name, email address, or proxy address that includes the domain name.
* Any group has an email address or proxy address that includes the domain name.
* Any application in your Azure AD has an app ID URI that includes the domain name.

**Steps:** Azure Portal 🡪 **Azure** **Active Directory** 🡪 **Custom Domain names** 🡪 Select Domain name 🡪 Delete

**To add company branding to your directory**

1. **Azure** **Active Directory** 🡪 Users and groups
2. On the **Users and groups - Company branding** blade, select the **Edit** command.
3. Modify the elements you want to customize. All elements are optional.
4. Click **Save**.

Note: This feature is available in Azure AD Premium only.

Likewise Password reset and Sign-ins is also available to AD Premium only.

**Managing Azure AD Users and Groups**

A directory can consist of the following three types of identities:

* Users added manually to the directory (cloud only identities)
* Third-party accounts (third-party identities)
* Users synced from existing Active Directory installations (on premise identities)

**Types of User**

1. Member user in your organization.
2. Guest User with existing Microsoft account (any email id registered with https://signup.live.com)

**Creating new user in your organization:**

1. Azure Portal 🡪 Azure Active Directory 🡪 Users and groups
2. All users 🡪 + Add
3. Create the following user in the directory:

|  |  |
| --- | --- |
|  | * **Name**: the display name |
|  | * **User name**: unique name within the domain name associated with the current Azure AD tenant that the user will provide when signing in |
|  | * **Profile**: first name, last name, job title, and department |
|  | * **Properties**: Source of Authority (Azure Active Directory) |
|  | * **Groups**: groups that the user should be a member of |
|  | * **Directory role**: User |

1. Create the user and record the temporary password.
2. At the top-right corner of the page, click your Azure subscription name, and then click **Sign Out**. **You have been signed out** page,
3. Click **SIGN IN** and Login again as JSmith.

**Note that by default this user will not have access to any resources.**

**Manage groups by using the Azure portal**

* **Microsoft 365 groups** (recommended) are a great way for teams to **collaborate** by giving them a **group email** and a shared workspace for conversations, files, and calendar events.
  + **Can have only Users.** M365 groups can contain users but cannot contain other groups or Devices.
  + **Group Types**
    - Assigned Users
    - Dynamic Users
* **Security groups** control access to OneDrive and SharePoint and are used for Mobile Device Management for Microsoft 365.
  + **Can have Users, Devices and other Groups**.
  + Security Group can container users and other Security Groups but cannot contain M365 groups.

Note: Nested group do not inherit licenses

* + **Groups Types**
    - Assigned Users
    - Dynamic Users
    - Dynamic Devices

**Steps to create a Group**

1. GROUPS 🡪 ADD A GROUP.
2. In the Add Group dialog box, enter the following settings, and then click Complete:

* NAME: Sales
* DESCRIPTION: Sales team

1. Click **Sales** 🡪 Click **ADD MEMBERS**.
2. In the **Add members** dialog box, click required Users, and click **Complete**.

**Creating a Domain Controller and Join Azure virtual machines to a domain**

1. Create a new VM (**DomainController-vm**) to be used **as Domain Controller and DNS Server.**
2. Change the Private IP to static: DomainController-vm 🡪 Networking 🡪 click on Network Interface (DomainController-vmXXX) 🡪 IP configurations 🡪 ipconfig1 🡪 **Private IP Address settings**, Assignment = **Static** 🡪 Save (**Don’t forget to note the IP address)**
3. Virtual Network 🡪 Select the VNet 🡪 **DNS** servers 🡪 Select Custom and provide **static IP** of **DomainController-vm** (eg: 10.0.0.4) from previous step.
4. Restart your **DomainController-vm**
   1. DomainController-vm 🡪 Restart
5. Promote the VM as Active Directory Domain Controller and DNS Server.
   1. RDP to DomainController-vm

For Screenshots refer: Reference: <https://www.manageengine.com/products/active-directory-audit/kb/how-to/how-to-setup-a-domain-controller.html>

* + - Server Manager 🡪 Dashboard 🡪 **Add Roles and Features** 🡪 Next 🡪 Next
    - Check **Active Directory Domain Service** and **DNS** 🡪 Next 🡪 . . . 🡪 Finish

A screenshot of a computer

Description automatically generated

* 1. After the feature installation is completed 🡪 From Notification in Server Manager Window (Top Right) 🡪 Click on ***Promote this server to a Domain Controller***

A screenshot of a computer

Description automatically generated

* 1. Select a **Add a** **New Forest** 🡪 Root domain name: ***bestazuretraining.com*** *(Custom Domain name created earlier)* 🡪 Next, Provide DSRM Password = Password@123 🡪 Next 🡪 . . . 🡪 Ignore all warnings 🡪Finish

A screenshot of a computer error

Description automatically generated

* 1. RDP to **DomainController-vm** 🡪 Server Manager 🡪 Tools 🡪 **DNS** 🡪 Right Click on **Server** 🡪 Properties 🡪 **Forwarders** 🡪 Edit 🡪 **Delete existing IP and replace with 8.8.8.8** 🡪 OK
  2. Restart your machine
  3. In VM type the following command to verify that this Machine is DNS Server

C:\> **Ipconfig** /all



1. Create New Users (Sandeep-User1 and Sandeep-User2) and Groups (Sandeep-Group1) in this New Domain Controller
   1. Administrative Tools 🡪 **Active Directory Users and Computers**
   2. Expand your Domain Name (bestazuretraining.com) 🡪 Expand Users 🡪 **Right click add New Users and Groups**

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Integrating On-Premises AD Identities with Azure AD**

* **Azure AD Connect** will integrate your on-premises directories with Azure Active Directory. This allows you to provide a common identity for your users for Office 365, Azure, and SaaS applications integrated with Azure AD.
* Integrating your on-premises directories with Azure AD makes your users more productive by providing a common identity for accessing both cloud and on-premises resources.
* The beauty of this approach is that any time your organization adds or deletes a user, or a user changes a password, *you use the same process that you use today in your on-premises environment. All of your on-premises AD changes are automatically propagated to the cloud environment.*

A diagram of a computer network

Description automatically generated

**Azure Active Directory Connect** is made up of three primary components:

1. **Sync Service** - This component is responsible for creating users, groups, and other objects. It is also responsible for making sure identity information for your on-premises users and groups is matching the cloud.
2. **Health Monitoring** - Azure AD Connect Health can provide robust monitoring and provide a central location in the Azure portal to view this activity. For additional information, see [Azure Active Directory Connect Health](https://docs.microsoft.com/en-us/azure/active-directory/connect-health/active-directory-aadconnect-health).
3. **AD FS - Federation** is an optional part of Azure AD Connect and can be used to configure a hybrid environment using an on-premises AD FS infrastructure. This can be used by organizations to address complex deployments, such as domain join SSO, enforcement of AD sign-in policy, and smart card or 3rd party MFA.

**Express Settings:**

* If you have a single forest AD then this is the recommended option to use.
* User sign in with the same password using password synchronization.
* It’s the default option and mostly used for common deployed scenario.

Note: All objects that you want to synchronize must be direct members of the group. Users, groups, contacts, and computers or devices must all be direct members. Nested group membership isn't resolved. When you add a group as a member, only the group itself is added. Its members aren't added.

**Azure AD Connect Express Installation Walkthrough**

1. ~~Azure Portal 🡪 Azure Active Directory 🡪 Users and Groups 🡪 All users 🡪 + New User 🡪 Username =~~ [~~admin@sandeepsonideccansoft.onmicrosoft.com~~](mailto:admin@sandeepsonideccansoft.onmicrosoft.com) ~~/ Dare@123, Directory Role = Global Admin.~~
2. Remote Login to DomainController-vm (Primary Domain Controller)
   * **Username**: **bestazuretraining.com\dssadmin**
3. Server Manager 🡪 Local Server 🡪 IE Enchanced Security Configuration = Off
4. Open Browser🡪 Search **Azure AD Connect Download**. Navigate to and double-click on **AzureADConnect.msi**.
5. On the Welcome screen, select the box agreeing to the licensing terms and click **Continue**.
6. On the Express settings screen, click **Use express settings.**
7. On the Connect to Azure AD screen, enter the username and password of a **global administrator** ([admin@sandeepsonideccansoft.onmicrosoft.com](mailto:admin@sandeepsonideccansoft.onmicrosoft.com) / Dare@123) for your Azure AD. Click **Next**.
8. On the Connect to AD DS screen, enter the username and password for an **enterprise admin account (**bestazuretraining.com\dssadmin**)**. Click **Next**.
9. The [**Azure AD sign-in configuration**](https://azure.microsoft.com/en-us/documentation/articles/active-directory-aadconnect-user-signin/#azure-ad-sign-in-configuration) page will only show if you did not complete verify your domains.
10. On the Ready to configure screen, click **Install**.

**The default synchronization frequency is 30 minutes**

**To customize the Scheduler Frequency for Sync Operation:**

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-feature-scheduler>

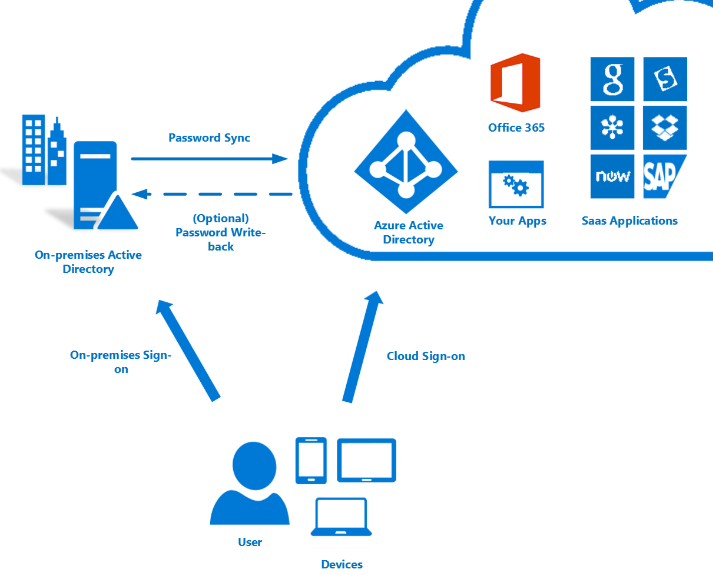
**To manually start Sync using PowerShell:**

Start-ADSyncSyncCycle -PolicyType Delta

**Azure AD User Sign-in Methods**

**Password Hash synchronization with single sign-on** (SSO):

* With password synchronization, **hashes** of user passwords are synchronized from on-premises Active Directory to Azure AD.
* Use this feature to sign in to Azure AD services like Office 365, Microsoft Intune, CRM Online, and Azure Active Directory Domain Services (Azure AD DS).
* In the background, the password synchronization component takes the user’s password hash from on-premises Active Directory, encrypts it, and passes it as a string to Azure. Azure decrypts the encrypted hash and stores the password hash as a user attribute in Azure AD.

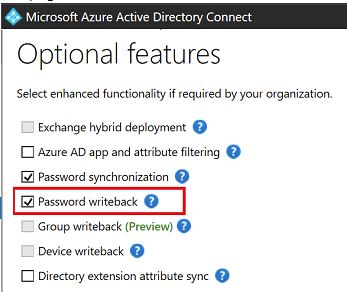


* This ensures a user signing on to Azure uses the same password as the on-premises domain, but doesn't require the additional infrastructure of a federated environment.
* It is important to understand that this is same sign-in, not single sign-on. The user still authenticates against two separate directory services, albeit with the same user name and password.
* When passwords are changed or reset on-premises, the new passwords are synchronized to Azure AD **immediately**.
* When you install Azure AD Connect by using the **Express Settings** option, password hash synchronization is automatically enabled.

**Password Writeback**

With password writeback, you can configure Azure Active Directory (Azure AD) to write passwords back to your on-premises Active Directory. Password writeback removes the need to set up and manage a complicated on-premises self-service password reset (SSPR) solution, and it provides a convenient cloud-based way for your users to reset their on-premises passwords wherever they want. Password writeback is a component of Azure Active Directory Connect that can be enabled and used by current subscribers of **Premium Azure Active Directory** editions. It’s recommended that you use the auto-update feature of Azure AD Connect.

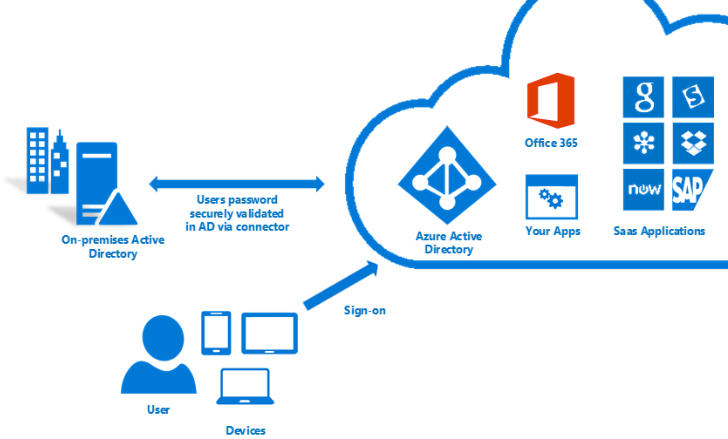
1. To configure and enable password writeback, sign in to your Azure AD Connect server and start the **Azure AD Connect** configuration wizard.
2. On the **Welcome** page, select **Configure**.
3. On the **Additional tasks** page, select **Customize synchronization options**, and then select **Next**.
4. On the **Connect to Azure AD** page, enter a global administrator credential, and then select **Next**.
5. On the **Connect directories** and **Domain/OU** filtering pages, select **Next**.
6. On the **Optional features** page, select the box next to **Password writeback** and select **Next**.



1. On the **Ready to configure** page, select **Configure** and wait for the process to finish.
2. When you see the configuration finish, select **Exit**.

**Pass-Through Authentication (PTA)**:

* The user’s password is validated against the on-premises Active Directory controller. The password doesn't need to be present in Azure AD in any form.
* Sign-in usernames can be either the on-premises default username (userPrincipalName) or another attribute configured in Azure AD Connect (known as Alternate ID).



* You need to choose Azure AD Connect **Custom Settings**. Password Synchronization in Optional Features tab must be **unchecked**.
* It uses a lightweight **on-premises agent** that listens for and responds to password validation requests.
* Agent has no management overhead. The agent automatically receives improvements and bug fixes.
* Additional agents can be installed on multiple on-premises servers to provide high availability of sign-in requests.
* Integrated with cloud-based self-service password management, including password writeback to on-premises Active Directory and password protection by **banning commonly** used passwords.
* Pass-through authentication is not only for user sign-in but allows an organization to use other Azure AD features, such as password management, role-based access control, published applications, and conditional access policies.
* Use PTA to ensure that when a user account is disabled in OnPremise Active Directory, the user account is **immediately** prevented (not after 30 minutes) from authenticating to Azure AD.
* **Limitations**: Doesn't work for scenarios that need **Azure AD Domain Services**.

**Federated SSO (with Active Directory Federation Services (AD FS))**:

* Federation is a collection of domains that have established trust. A typical federation might include a number of organizations that have established trust for shared access to a set of resources.
* With federated sign-in, your users can sign in to Azure AD-based services with their on-premises passwords. While they're on the corporate network, they don't even have to enter their passwords.
* This is mandatory for situations where User from Internet should be able to **access On-Premise Applications** using the Identity provided by Azure AD.
* It uses Claims based Authentication.

