

# Manage Identity and Access in Azure AD – Part 3

Secure your application by using OpenID  
Connect and Azure AD



What is Modern Authentication?

Create Tenant and Register an App

Deploy App to Use OAuth and OpenID



Industry Standard Protocol,  
OAuth 2.0 Provides Authorization  
for Web, Desktop, and Mobile  
Applications



OpenID Connect is the  
Authentication Layer Built on top  
of OAuth for Identity Verification  
Missing from OAuth 2.0

## Add Custom Domain to Azure AD

### Add Domain to Azure AD

Custom domain names can be added to Azure AD after you have created your Directory

### Add DNS Info. to Domain Registrar

Create a TXT record to the DNS of your domain registrar with the record generated to verify

### Verify Your Domain Name

After the DNS record has been created, return back to Azure to verify your authority over the domain name



### Azure AD connect

- **Password hash synchronization** – Synchronizes the hash, of the hash, of users password from on-premises AD to Azure AD
- **Pass-through authentication** – Password verification happens from on-premises Active Directory
- **Federation integration** – Allows configuration of federation with on-premises ADFS and Azure AD
- **Synchronization** – Operations related to synchronization of identity data between on-premises and Azure AD
- **Health Monitoring** – Provides robust monitoring of on-premises identity infrastructure

# Demo



## Summary



Secure your application by using OpenID Connect and Azure AD

What is Modern Authentication?

Create Tenant and Register an App

Deploy App to Use OAuth and OpenID

Download the training material from – <https://azure-training.com>

 [@mstechtrainings](https://twitter.com/mstechtrainings)

 <https://www.linkedin.com/in/neeraj-kumar-csm-mcts-mcse/>