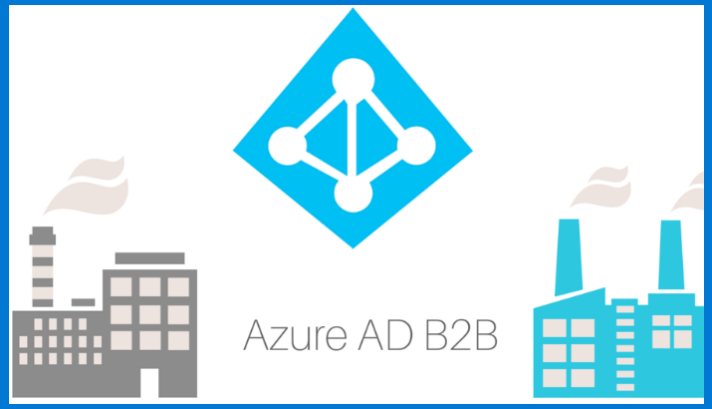
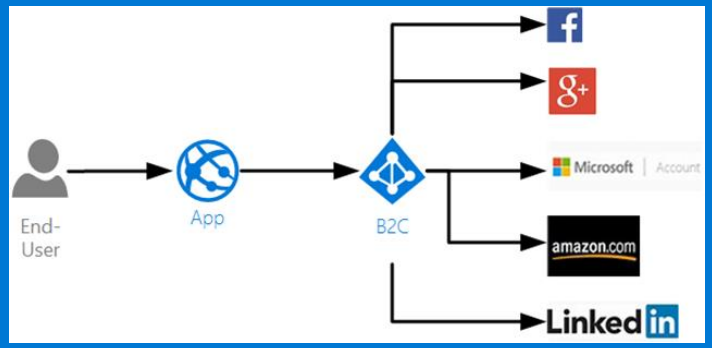
Azure AD





Secure your applications with Azure AD

Tushar Shah

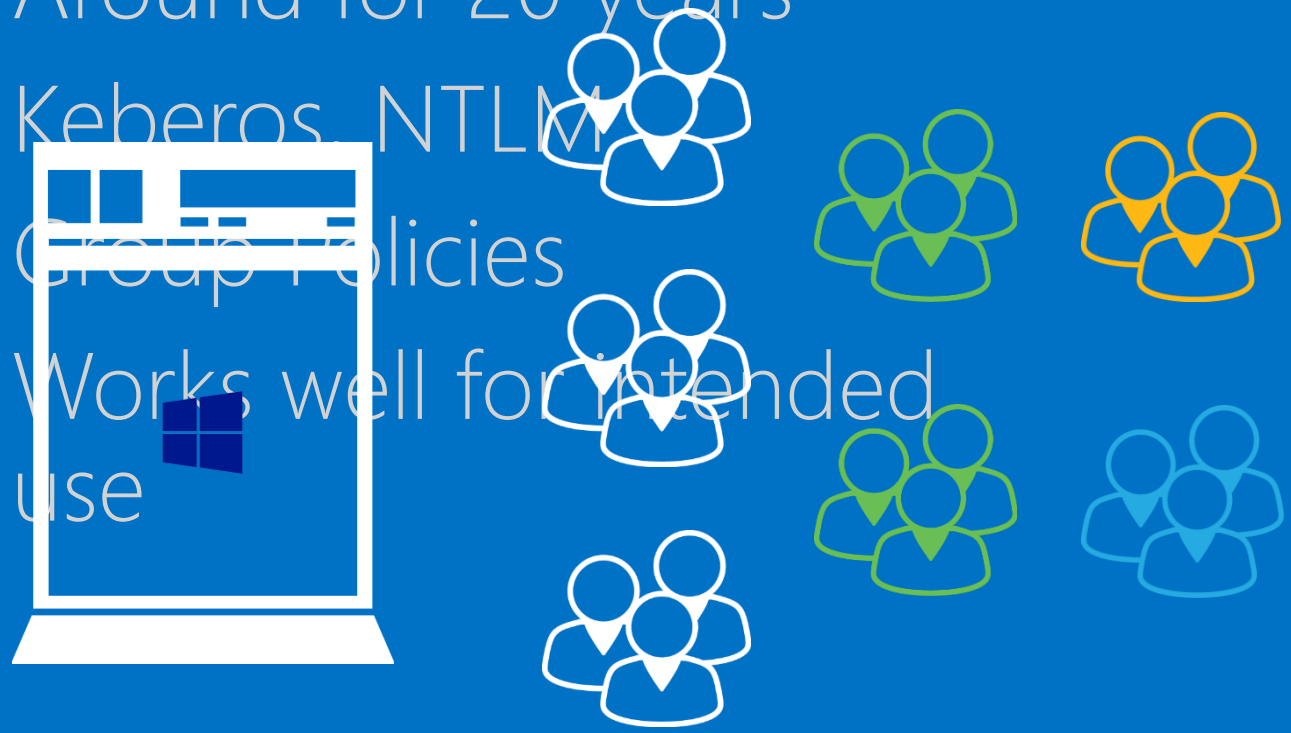
Technical Architect

Contact

Shah.Tushar@gmail.com
https://www.linkedin.com/in/tusharashah

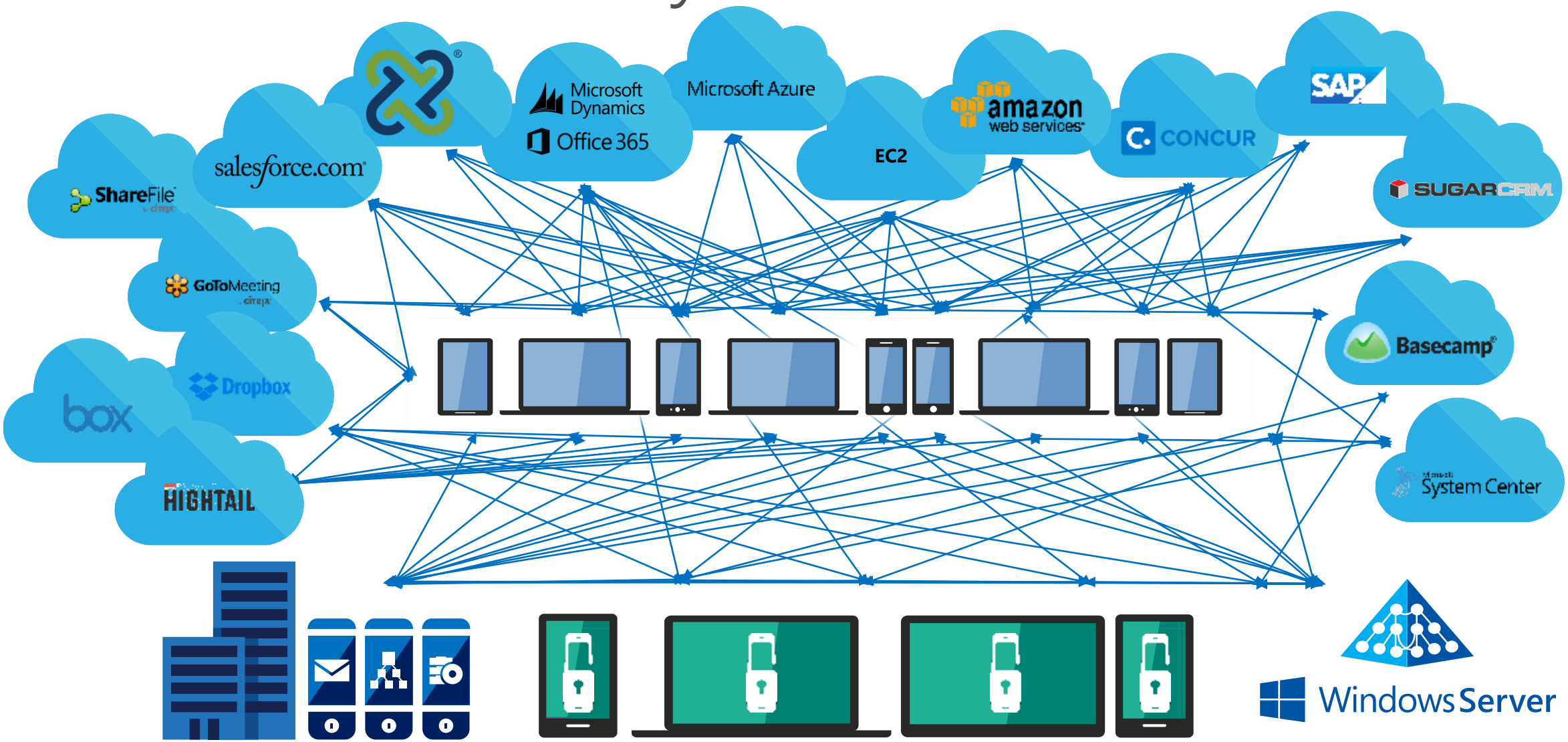
Active Directory

- Around for 20 years
- Keberos, NTLM
- Group Policies
- Works well for intended use



What's driving change?

The current reality…



Microsoft's Enterprise Mobility Solution

Access from many devices

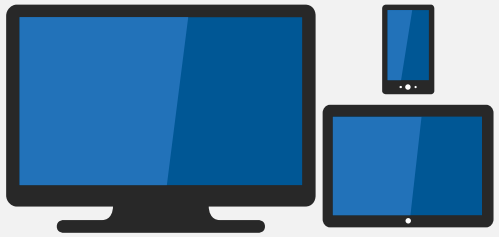
It's integrated on common identity

Manage and secure productivity

It protects Office better

Preserve existing investments

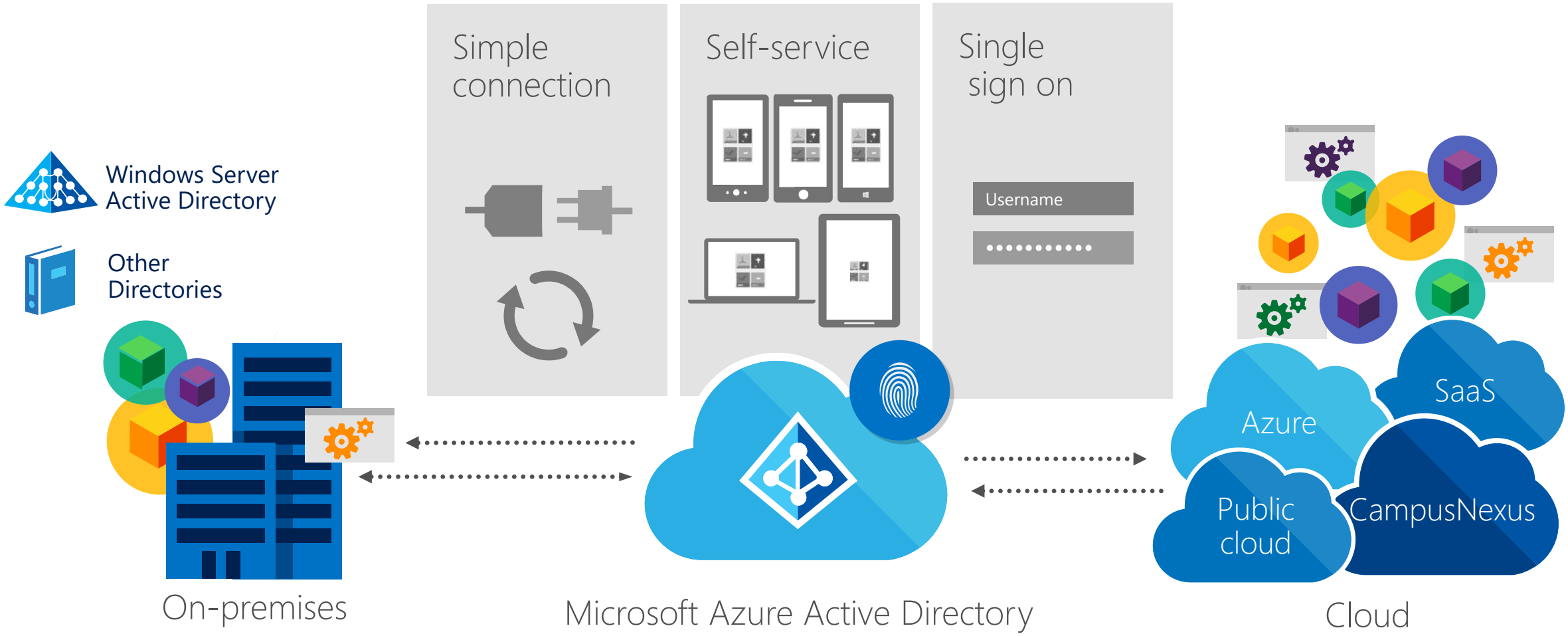
It just works



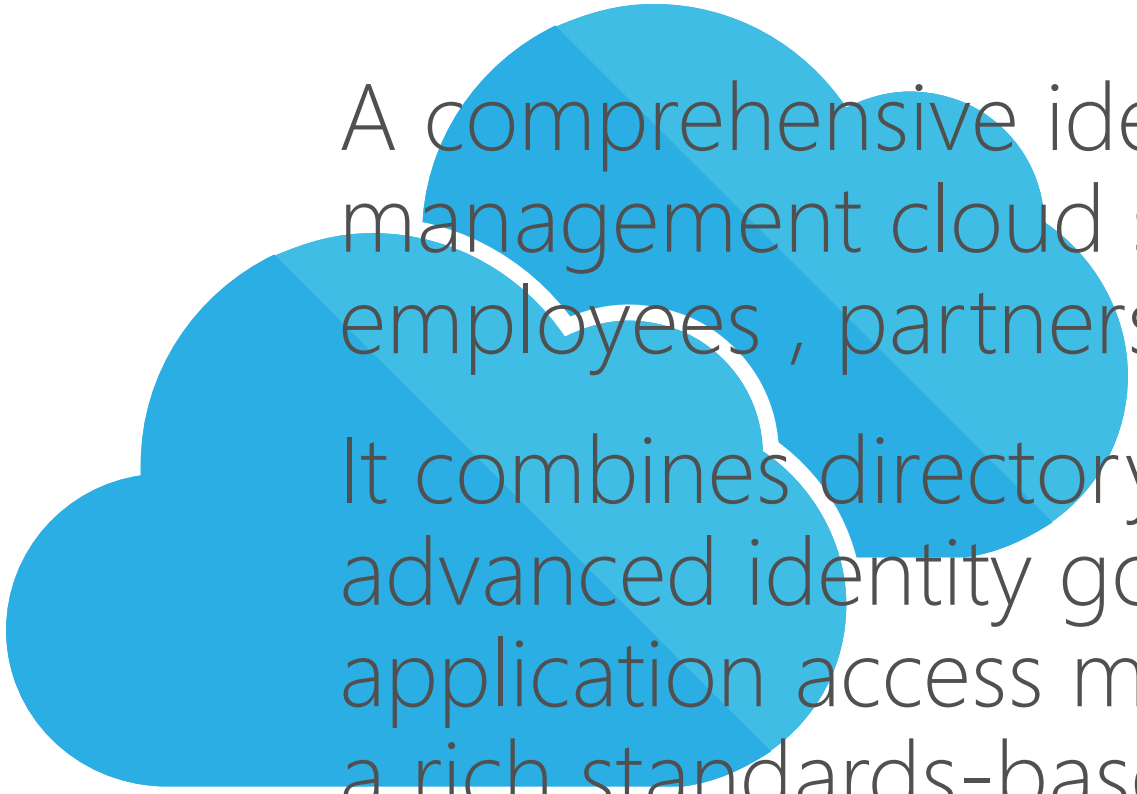
Support iOS, Android, Windows

It's comprehensive

Identity as the control plane



What is Azure Active Directory?



A comprehensive identity and access management cloud solution for your employees , partners and customers.

It combines directory services, advanced identity governance, application access management and a rich standards-based platform for developers.

B2E B2B B2C

Your Directory on the cloud

Manage everything from passwords to devices.

Monitor and protect access to cloud applications.

Empower Users

Your Directory on the cloud

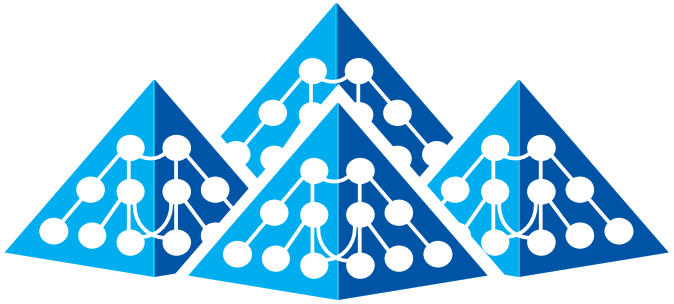
Manage everything from passwords to devices

Monitor and protect access to cloud applications.

Empower Users

Your Directory on the cloud

Connect and Sync on-premises directories with Azure.



Windows Server
Active Directory

MIIM

* Azure Active Directory Connect and Connect Health

PowerShell

SQL (ODBC)

LDAP v3

Web Services
(SOAP, JAVA, REST)

Other Directories

Microsoft Azure
Active Directory

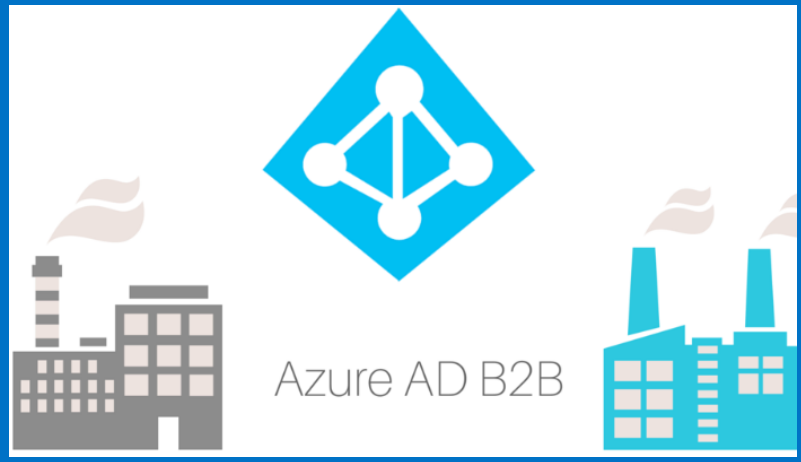
Azure AD B2B and Azure AD B2C

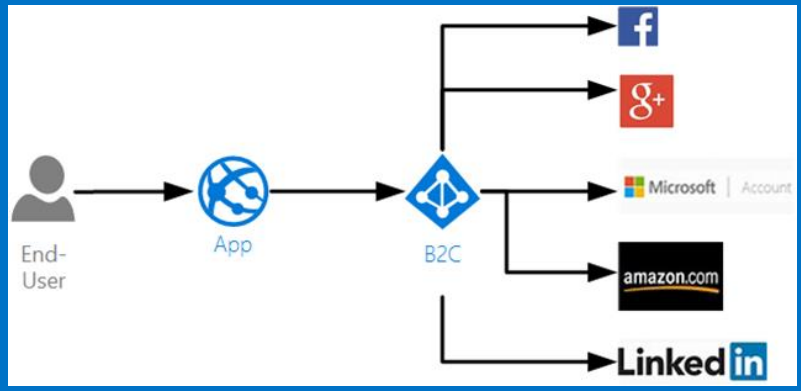
Azure AD B2B

- Work with users from partner organizations
- Partners use their own credentials
- Partners don't have to use Azure AD
- MFA and other security can be enforced on Partner users*

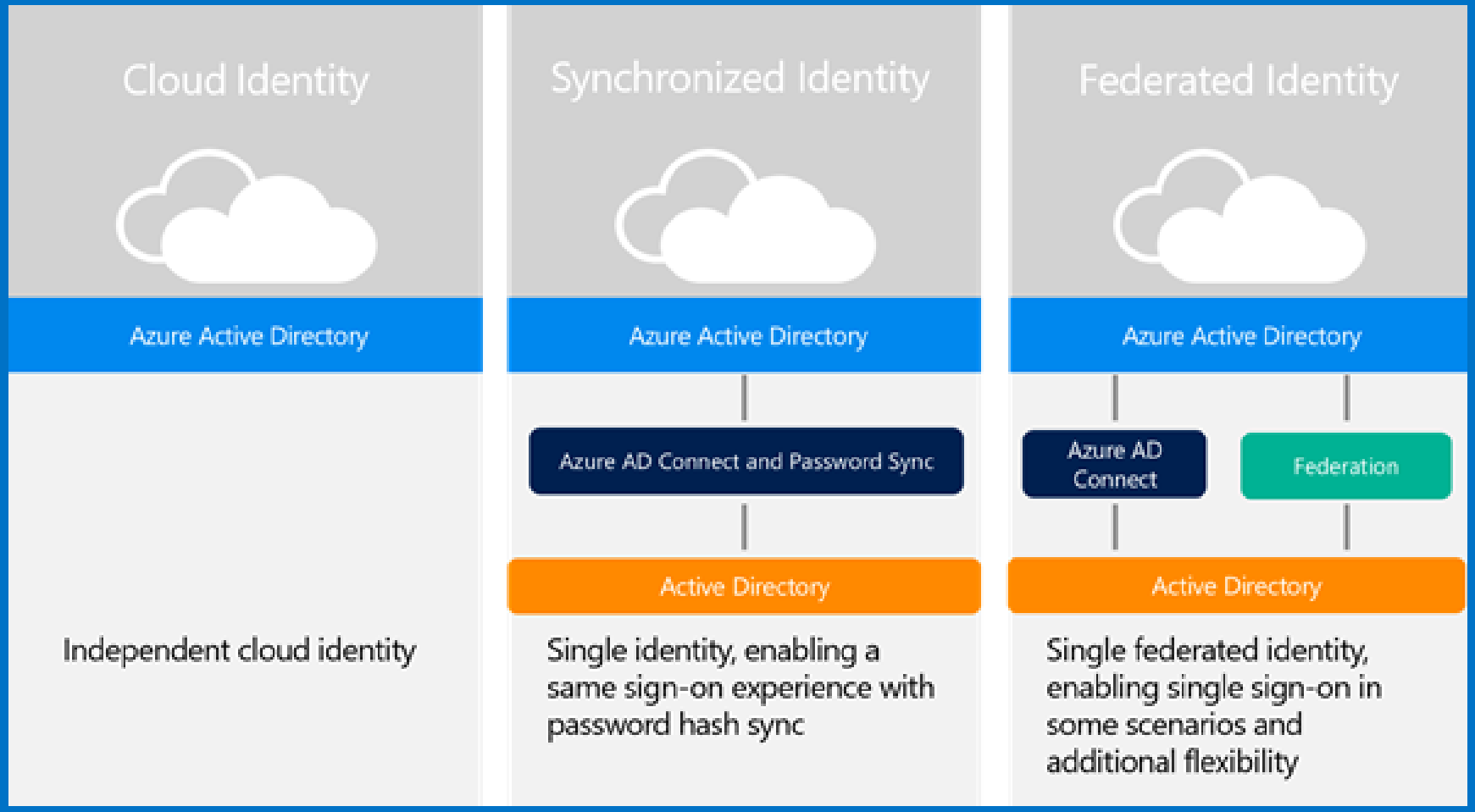
Azure AD B2C

- Allows anyone to sign up
- Social Accounts (such as Facebook, Google, LinkedIn, and more)
- Enterprise Accounts (using open standard protocols, OpenID Connect or SAML)
- Local Accounts (email address and password, or username and password)
- **Cannot be used for Office 365**

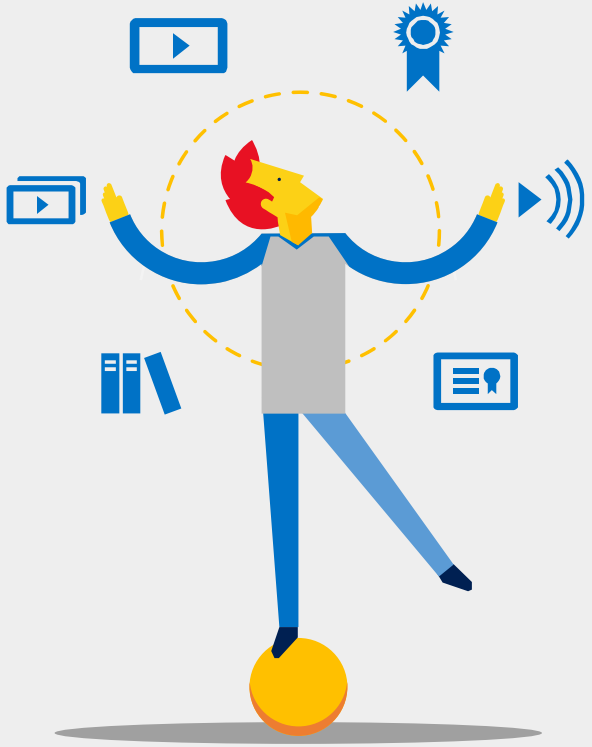




Type of identities



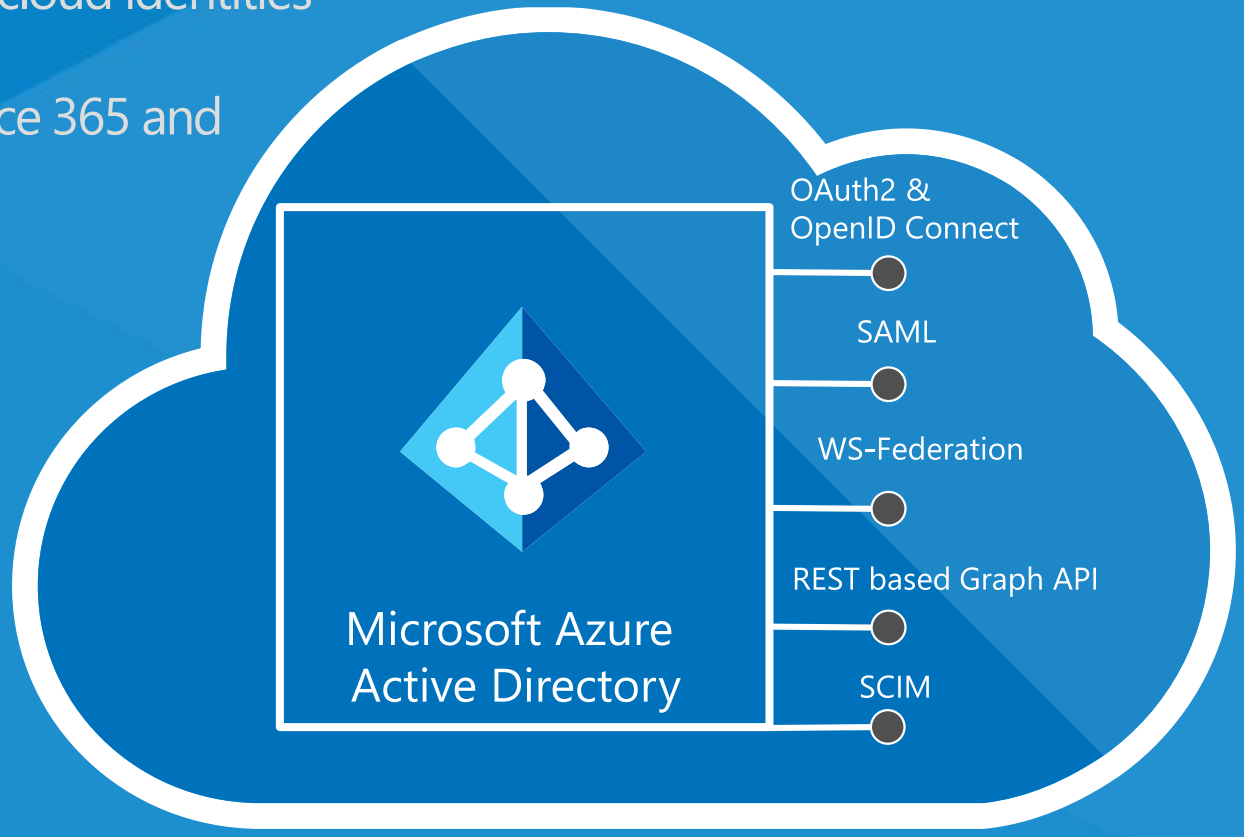
Demo



Authentication Scenarios

Rich standards-based platform for developers

- Custom LOB applications can integrate with Azure Active Directory
- Sign in to Active Directory-integrated applications with cloud identities
- Active Directory-integrated applications can access Office 365 and other web APIs
- Applications can extend Azure Active Directory schema
- Cross-platform support (iOS, Android, and Windows)
- Open Standards
  (SAML, OAuth 2.0, OpenID Connect, Odata 3.0)



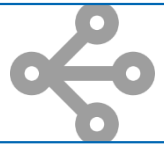
Options by application types

Single-page applications

- OAuth 2 implicit grant flow

Web app

- OpenID Connect
- SAML 2.0
- WS-Federation



Web API

- OAuth 2.0 client credentials with application identity
- OpenID connect and OAuth 2.0 authorization code with delegated user identity

Mobile & desktop app

- OAuth 2.0 authorization code grant type

Server applications

- OAuth 2.0 client credential grant type
- OAuth 2.0 On-Behalf-Of

OpenID Connect

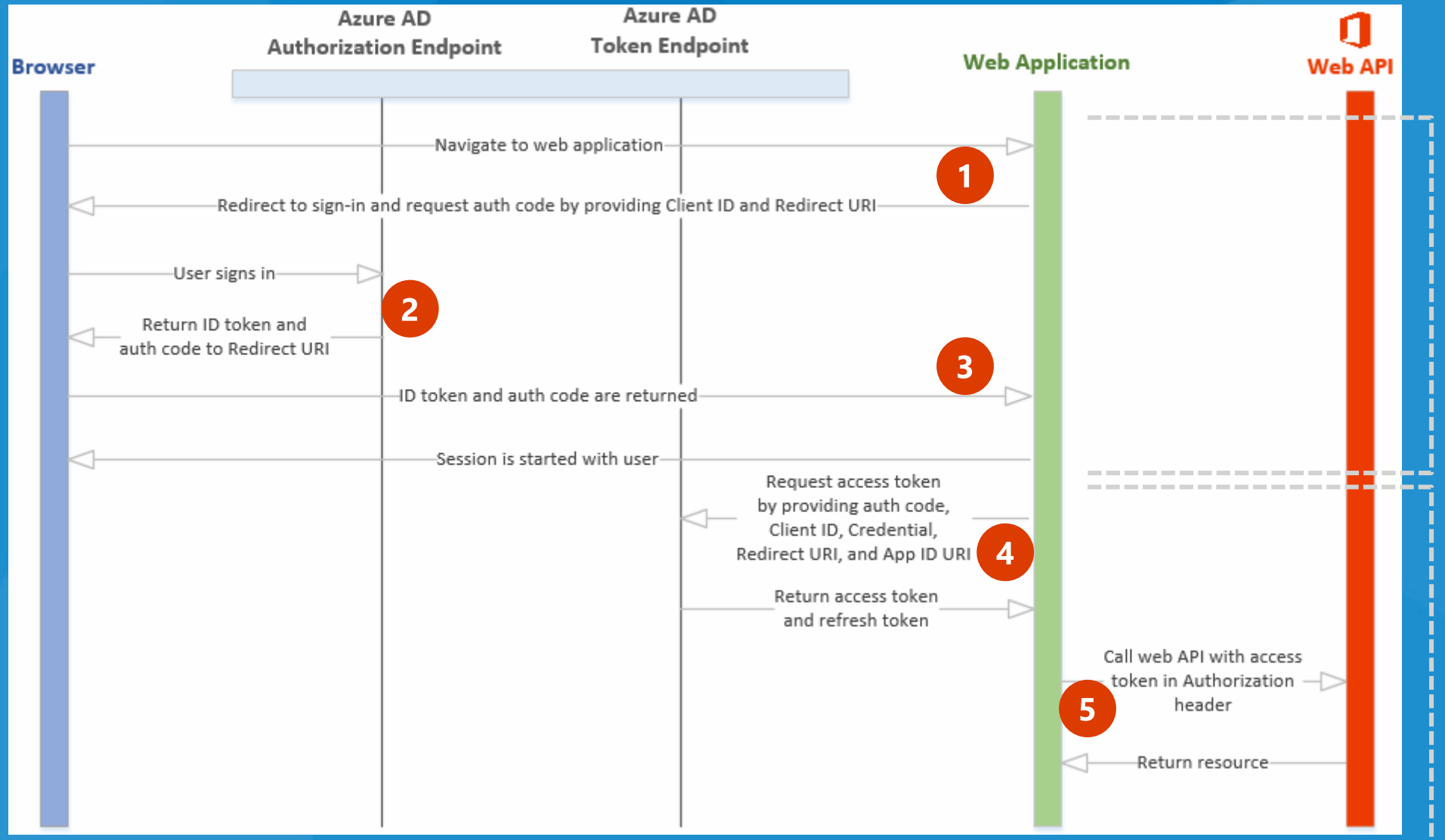
OpenID Connect 1.0 is a simple identity layer on top of OAuth 2.0

It enables clients to verify the identity of the user and to obtain basic profile information

Lightweight, yet very powerful

http://openid.net/specs/openid-connect-core-1_0.html

High level SSO protocol flow



Web sign-in using OpenID Connect

Office API access

App registration in Azure AD

Tenant

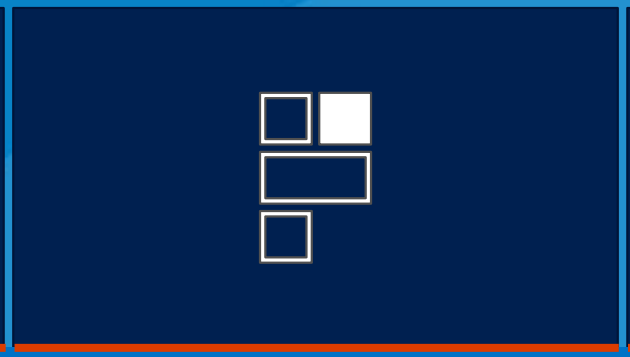
Register within an AAD tenant

LOB

SaaS app

Location

Reply address, for web apps, a valid endpoint where you app is hosted

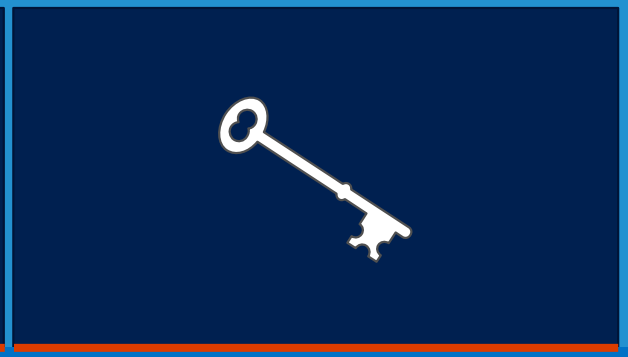


Application identifier

App ID URI for WS-FED and SAML

Client_id for OpenID Connect and OAuth

Uniqueness is enforced for SaaS app identifiers

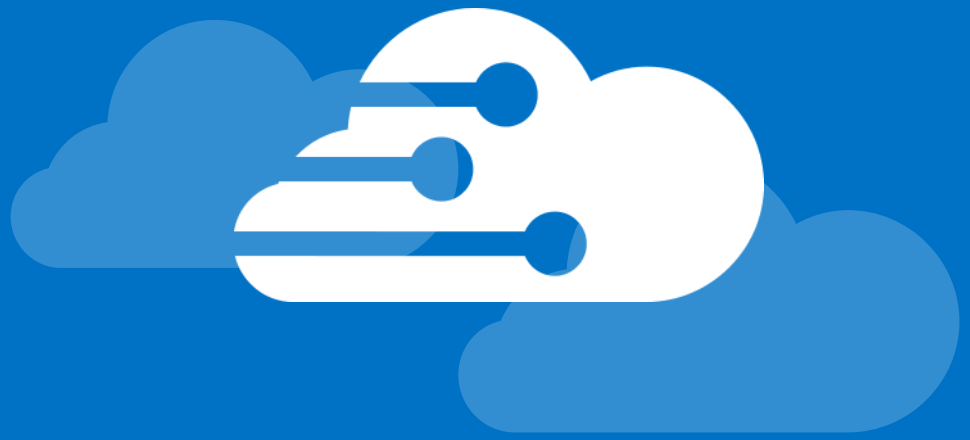


Secret keys

A key the web app can use to authenticate to AAD

For SaaS app, same key for all tenants

AAD STS endpoints



Per-protocol endpoint
https://login.windows.net/<tenant>/<protocol>[/<use>]

Example:
https://login.windows.net/contoso.com/oauth2/authorize

<tenant> can be replaced with:

- Verified domain: used to specify tenant based on user input
- Tenant ID: immutable ID saved URL
- 'Common': leave it up to the STS

Claims in sign-on token

Security

Display

```
{
  "typ": "JWT",
  "alg": "RS256",
  "x5t": "-sxMJMLCIDWMTPvZyJ6tx-CDxw0"
}.{
```

Audience	"aud": "3b17521e-0e93-4fe8-92f9-ac9285f36a51",
	"iss": "https://sts.windows.net/b59e8db6-89f7-4256-bbb5-9ac2e2407da1/",
	"exp": 1551712651,
Last Name	"family_name": "Shah",
First Name	"given_name": "Tushar",
	"ipaddr": "12.xxx.xx.66",
Name	"name": "Tushar Shah",
	"nonce": "63687305837445596 6. 1YWMzNjJZTAtZzVmZTA4NzNlMDZh",
Object Identifier	"oid": "0821d5eb-a2c8-445b-a91d-e721f3433d8b",
Name ID	"sub": "vTxoNbHN8BJDOqo_0XEIHVguzp7gKCkuwcem0i1euxo",
Tenant ID	"tid": "b59e8db6-89f7-4256-bbb5-9ac2e2407da1",
	"unique_name": "Tushar@Portal395.onmicrosoft.com",
	"upn": "Tushar@Portal395.onmicrosoft.com",
	"ver": "1.0"

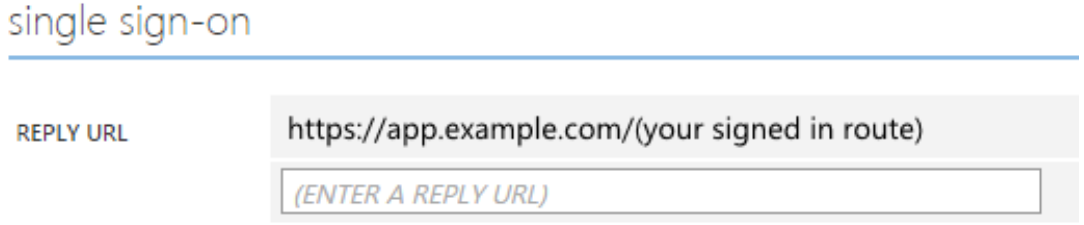
```
}
```

Auth design considerations

- Anonymous + authenticated or authenticated-only experience
- Use [Authorize] attribute for authenticated routes
- App launcher initiates sign-in to Redirect URI
- Use NaiveSessionCache in prototypes but not for production

YourController.cs

```
[Authorize]
public ActionResult YourRoute()
{
```



Configuring OpenID Connect OWIN

Startup.Auth.cs

```
public void ConfigureAuth(IAppBuilder app)
{
    app.SetDefaultSignInAsAuthenticationType(CookieAuthenticationDefaults.AuthenticationType);
    app.UseCookieAuthentication(new CookieAuthenticationOptions());
    app.UseOpenIdConnectAuthentication(new OpenIdConnectAuthenticationOptions
        {
            Client_Id = clientId,
            Authority = authority,
            Notifications = new OpenIdConnectAuthenticationNotifications()
                {
                    RedirectToIdentityProvider = (context) =>
                    {
                        string appBaseUrl = context.Request.Scheme + "://"
                            + context.Request.Host + context.Request.PathBase;
                        context.ProtocolMessage.RedirectUri = appBaseUrl + "/(your signed in route)";
                        context.ProtocolMessage.PostLogoutRedirectUri = appBaseUrl;
                        return Task.FromResult(0);
                    }
                }
        });
}
```

References

Azure AD

- Azure AD edistions: https://azure.microsoft.com/en-us/pricing/details/active-directory/
- Azure Active Directory for developers: https://docs.microsoft.com/en-us/azure/active-directory/develop/
- Authentication Scenario: https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-scenarios
- B2B vs B2C: https://docs.microsoft.com/en-us/azure/active-directory/b2b/compare-with-b2c

ADAL vs MSAL

- https://docs.microsoft.com/en-us/azure/active-directory/develop/azure-ad-endpoint-comparison
- https://github.com/AzureAD/microsoft-authentication-library-for-dotnet/wiki/Adal-to-Msal
- https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-v2-limitations

Samples

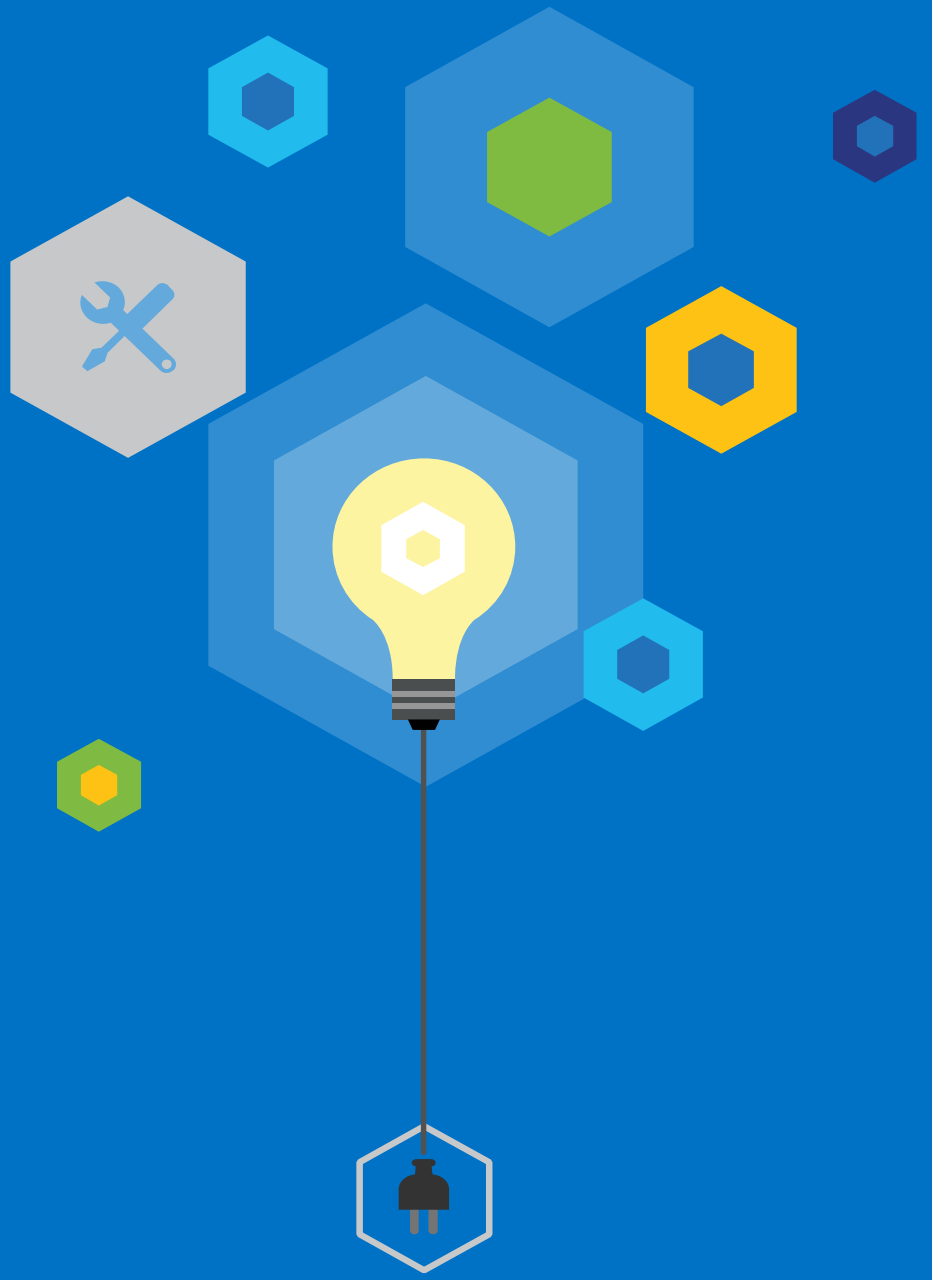
- https://github.com/Azure-Samples/
- https://github.com/Azure-Samples/active-directory-angularjs-singlepageapp
- https://github.com/ShahTushar/

Azure AD PowerShell

- https://github.com/AzureAD/azure-activedirectory-powershell
- https://docs.microsoft.com/en-us/powershell/module/azuread/?view=azureadps-2.0

Other resources

- A Guide To OAuth 2.0 Grants: https://alexbilbie.com/guide-to-oauth-2-grants/
- Blog: http://community.campusmgmt.com/?s=Tushar



Tushar Shah | Shah.Tushar@gmail.com | http://www.linkedin.com/in/tusharashah

Tushar Shah

Shah.Tushar@gmail.com
https://www.linkedin.com/in/tusharashah
https://github.com/ShahTushar/