

PHOLAX

Azure Active Directory

Anthony Clendenen

Cloud Architect MVP, P-TSP, CCSK, Azure Certified Architect, Author, Speaker

Ground Rules

- Please hold questions I have 60 slides
- I am here all day to answer questions
- There is a ton of content to cover so find me after for more details
- Some details may need to dated

PHODIAX

Agenda & Goals

- Overview of Azure AD
- Deployment lessons from the real world
- Outline items that can accelerate your deployment
- Avoid things that can slow you down
- Deep Dive on common technical challenges and how to over come them

What is Azure AD?



Extension of AD to the cloud

Synchronized copy of AD Modern authentication protocols

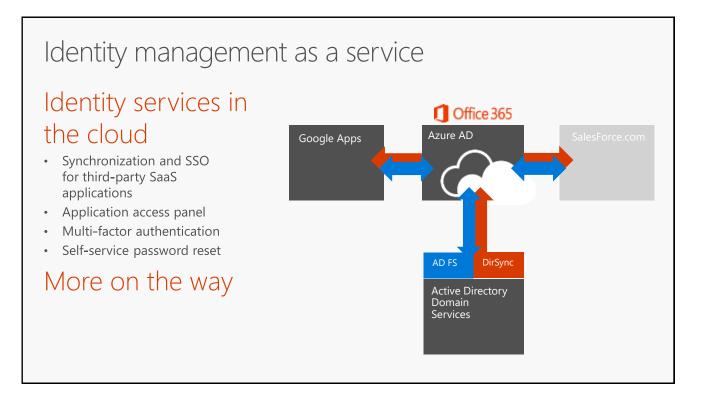
WS-Federation SAML 2.0 OAuth 2.0 OpenID Connect

Graph API for directory lookups

REST API for CRUD operations

Azure AD AD FS DirSync Active Directory Domain Services

Multi-tenant identity service Identity marketplace for applications • Common endpoints • Common signing certificate • Customer control for trusted applications Identity across organizational boundaries



Identity platform for MS online services

Facilitates authentication and provides directory information for:

- Office 365 (Exchange Online, Lync Online, SharePoint Online)
- Microsoft Dynamics CRM Online
- Microsoft Intune
- Azure Portal
- Azure Rights Management Services
- More and more all the time...

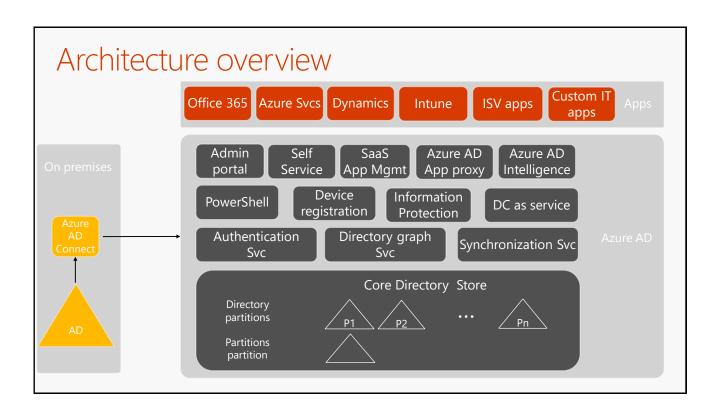
Any customer on Office 365 is already an Azure AD customer

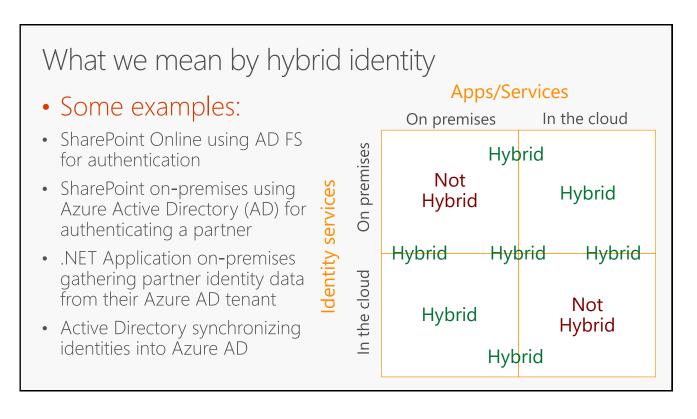
Premium identity capabilities

Self service SAAS app management Multi-factor authentication Azure AD intelligence Administrative units Azure AD Domain Services

Azure AD architecture









Taking advantage of identity as a service

- Self Service Password Reset with Azure AD
- Self Service Group Management with Azure AD
- Azure AD Join
- Azure AD Privileged Identity Management
- Azure AD SaaS Application Access
- Azure Multi-Factor Authentication
- Azure AD Business to Business
- Azure AD Business to Consumer
- Cloud App Discovery
- Azure AD Security Reports and Alerts



Integrating apps with hybrid identity

- Azure AD domain services
- Web app sign-in
- Using web APIs
- Azure AD app proxy
- Authorizing users to applications
- Accessing user data



Software assurance

SLA - 99.95

High availability and disaster recovery

Safeguards on operator access

- 2FA required for operators
- Auditing of changes
- Just in time elevation system

Secure storage of hashes only

Azure AD architecture

Natively multi tenant

Multi tenancy is enforced in software

Built on open standards

- http/REST and standard protocols to maximize reach and enterprise acceptance
- Authentication: SAML, WS-Fed, Oauth 2.0, Open ID connect
- Directory access: Directory Graph API (REST/OData 3.0)

High scale

- Partitioned (on tenant boundary)
- · Designed to scale to millions of tenants, billions of objects

Azure AD architecture (continued)

High availability across data centers

Active/active for reads across data centers; active/passive for writes. Writes are 2-GEO replicated prior to acknowledgement, or are replayable

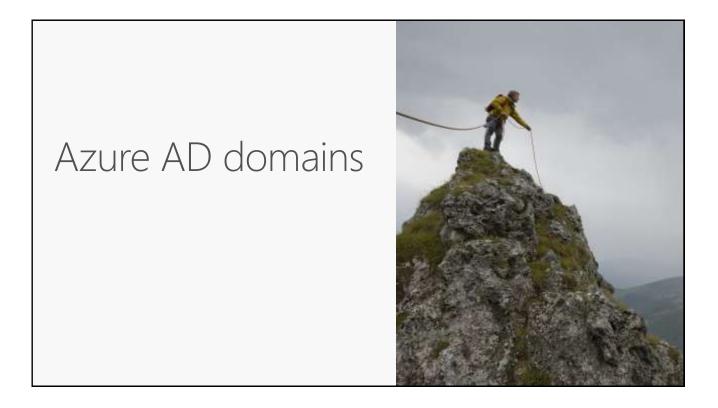
System is resilient to loss of any one datacenter

Support compliance standards

ISO 270001 FISMA/FEDRAMP. Segregated partitions for high security government clouds EU model clauses

Very high operational reliability

Azure AD down = All Microsoft services down



What is an organization ID?



User identifier in Azure Active Directory

- The only way users identify themselves to AAD
- · Users need to know their identifier, even when federated
- We cannot support simple username or DOMAIN\User

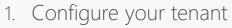
Domains in Azure AD Azure AD domain != AD DS domain In AD DS, domain is security, storage, and trust boundary In Azure AD, domain is more synonymous with a DNS domain A domain is the boundary for configuration options Federated or standard Password policy Used for Home Realm Discovery (HRD) Every tenant is assigned <tenant>.onmicrosoft.com

Cloud identities are created with this domain

Custom domains

- Need to be registered with Azure AD to allow users to sign in with anything other than <tenant>.onmicrosoft.com
- Domains must be public
- Ownership must be verified via DNS
- New TXT or MX record with a value provided by Azure AD
- Multiple domains can be registered with a single tenant
- Be aware of the parent/child relationship

High level deployment plan



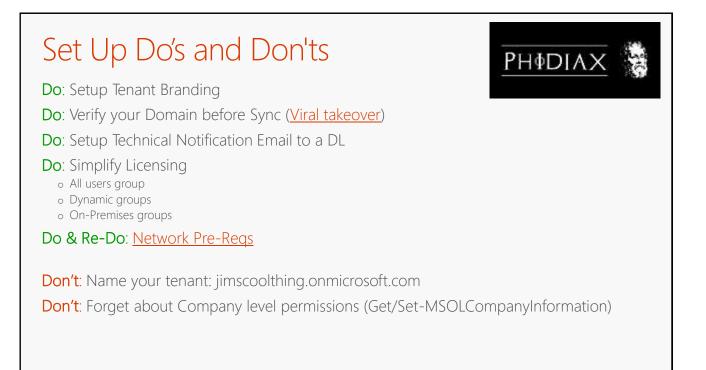
- 2. Choose your Authentication method
- 3. Deploy AAD Connect & Connect Health
- 4. Enable SSPR + Password Write-back
- 5. Configure Conditional Access + MFA
- 6. Deploy App Proxy
- 7. Turn on Identity Protection

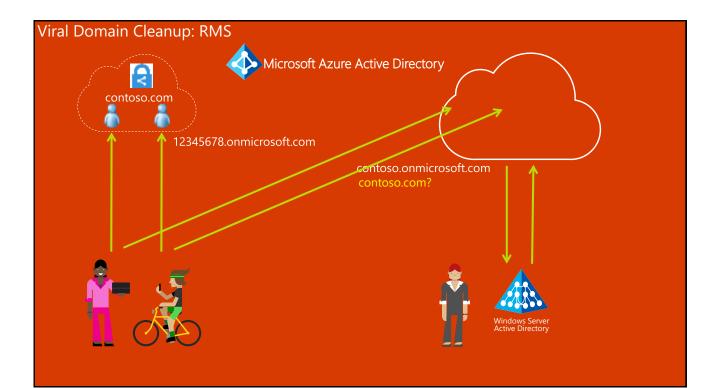


ΡΗΦΟΙΑΧ



Setting Up Your Tenant

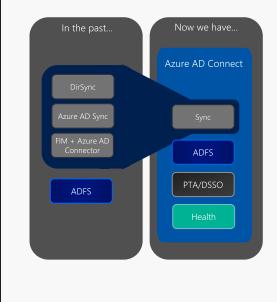




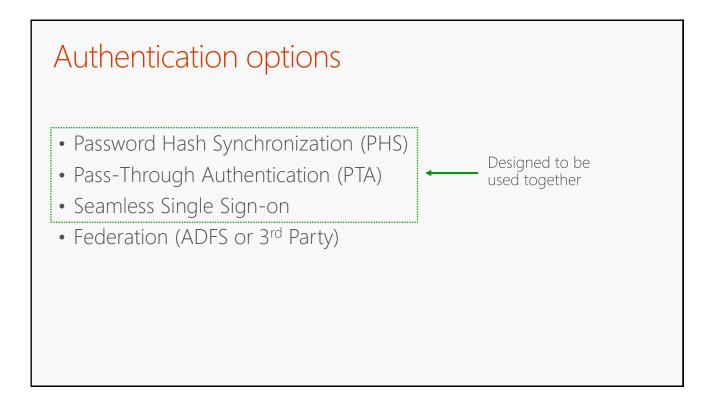


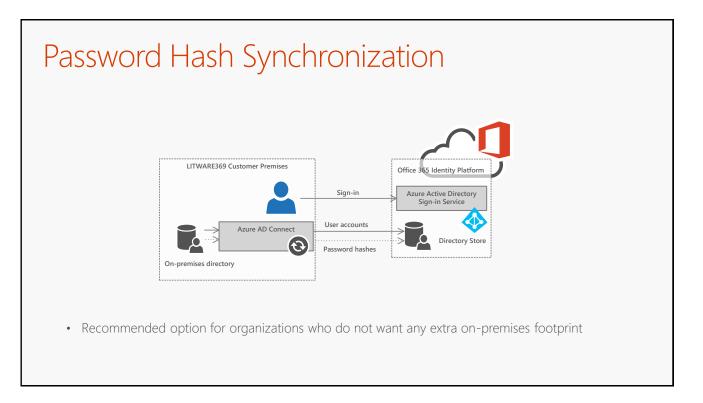
Sync & Auth

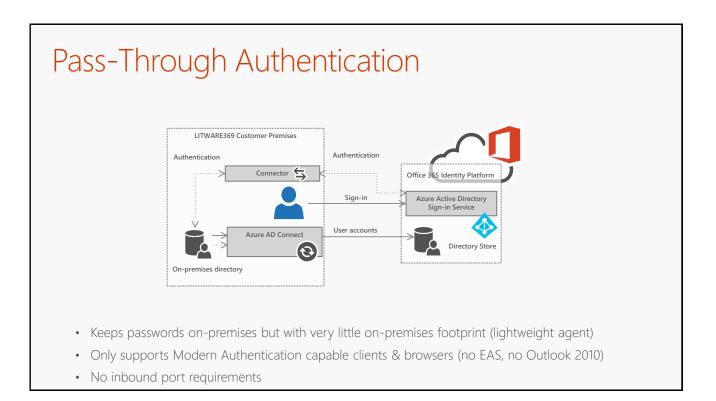
Azure AD Connect

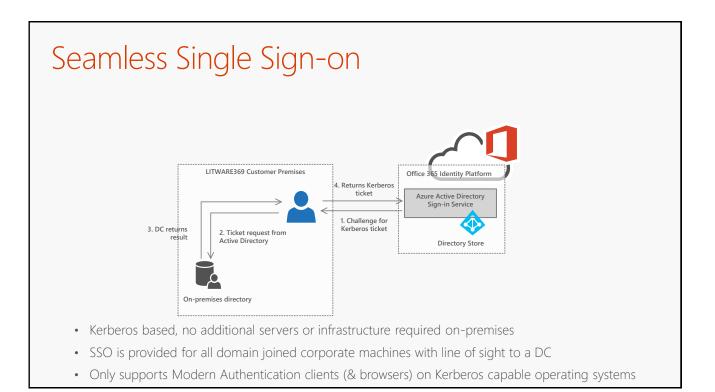


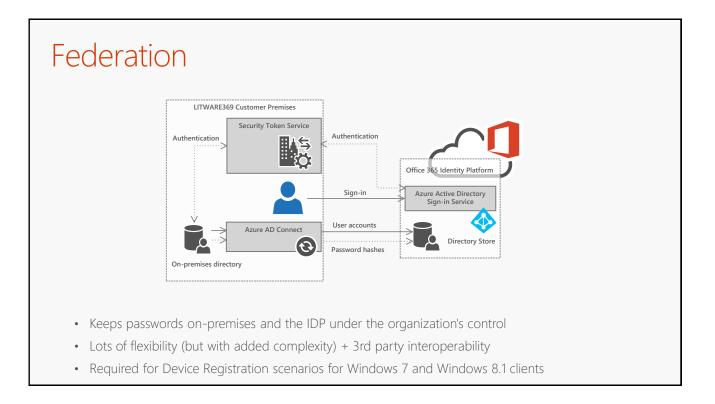
- Tool which simplifies connecting on-premises identity infrastructure with Azure AD
- Beyond synchronizing users from AD to Azure AD, provides various features for simplifying hybrid identity management
- Express Settings gets customers connected in a matter of minutes
 - ~80% of installations use Express settings(~5 clicks)
- All future investments will only be available with AAD Connect
- Note: End of Support is approaching for DirSync & AADSync: April 2017









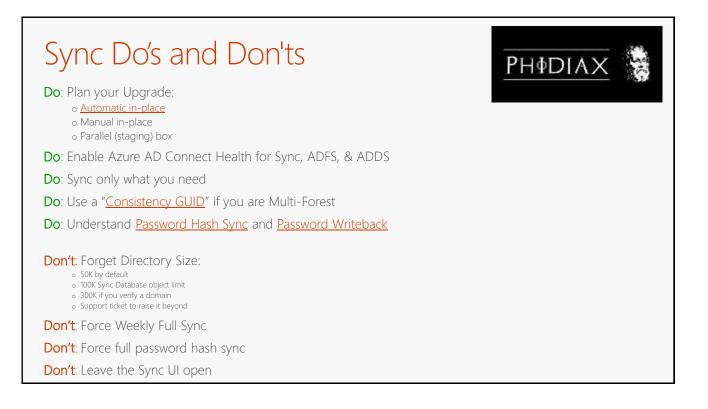


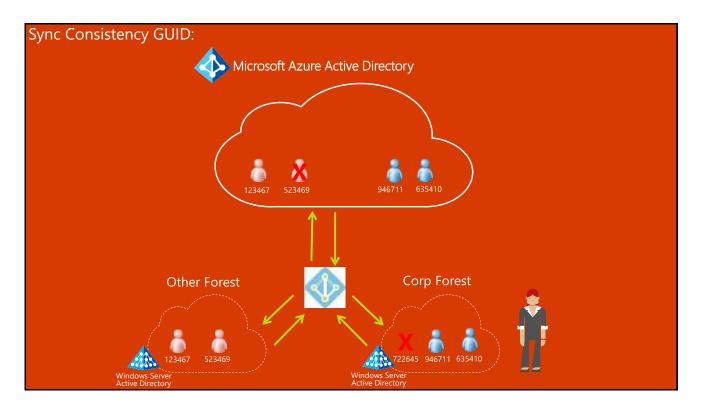
Auth Do's and Don'ts

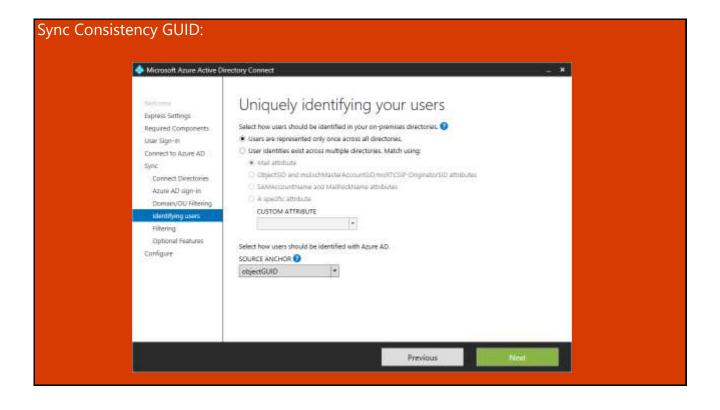
Do: Choose the simplest authN method for your needs

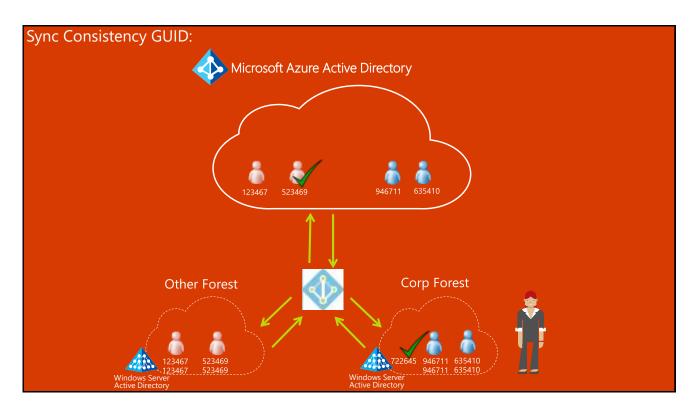
- Do: Look at using Windows 10 if you want the best SSO experience possible
- Do: Know which clients, scenarios & applications support which methods
- Do: Understand the nuances between Single Sign-on vs Same Sign-on
- Do: Enable Password Hash Sync even if you are federated (leaked credential report)
- Do: Leave a global admin @onmicrosoft.com account when federated

Don't: Default to deploying AD FS Don't: Forget about signing certificates rolling annually in AD FS











PHOLAX

Azure AD Connect Health

Connect Health

- Simple, low noise alerting system with helpful troubleshooting information
- Supports the monitoring of:
 - o AD FS
 - o AD DS (in preview)
 - o Azure AD Connect (Sync)
- Reports and operational insights about usage, trends and more
- Extremely easy to onboard (agent based)

Connect Health Reporting & Alerting

- Sync error reports for AAD Connect
- Replication status and health of Domain Controllers
- AD FS performance and usage trends
- AD FS bad password attempts



PHOLAX

Connect Health Do's and Don'ts

Do: Deploy all health agents

Do: Upgrade to latest and greatest AD Connect

Do: Delegate access to health portal

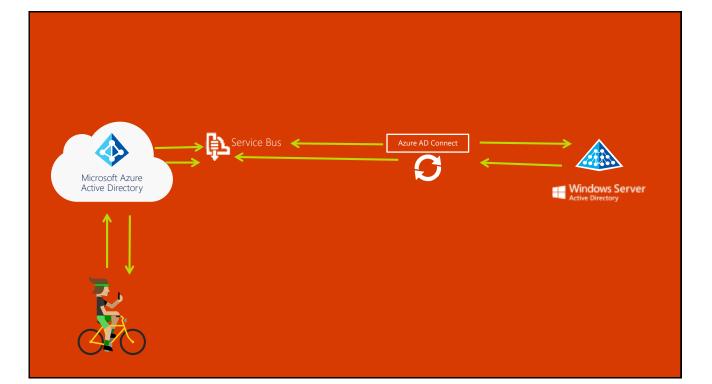
- Do: Follow best practices suggested by health agents
- Do: Enable agent auto update

Do: Install AD DS Health agent to see: Replication, Logins by type, DCs, Domains Sites

Don't: Not deploy the health agents Gotcha: Password Writeback not monitored yet



Self Service Pwd Reset (SSPR)



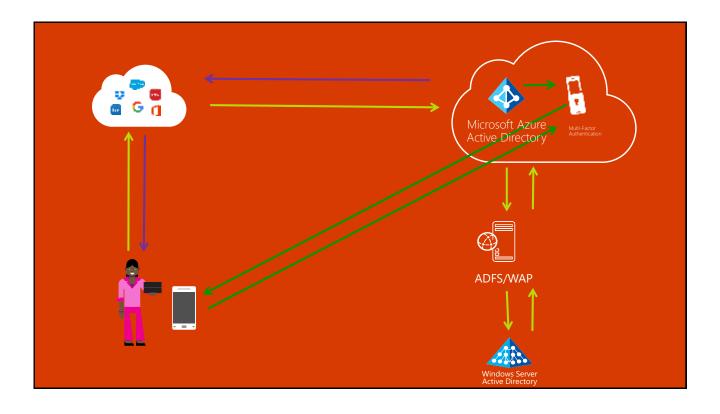
in one of the following opti-

SSPR Do's and Don'ts

- Do: Your pre/post data homework
- Do: Get executive sponsorship and communicate to end users
- Do: Enable Password Write-back
- Do: Know that write-back works for federated scenarios
- Do: Stage using "Restrict Access to Password Reset"
- Do: Use "Require Users To Register When Signing In"
- Do: Deploy alongside an app that users want to use
- Do: Consider building an SSPR site

Don't: test with an Administrative Account



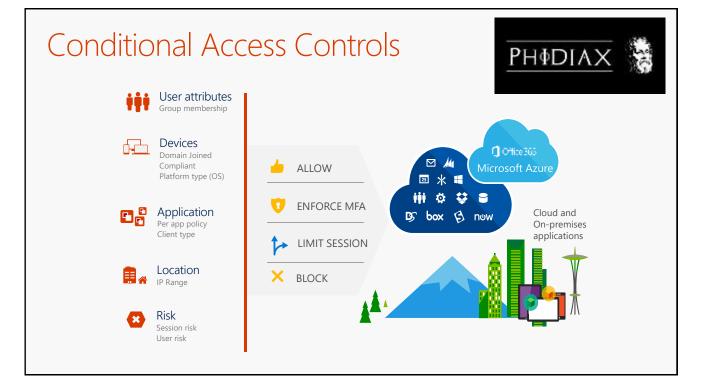


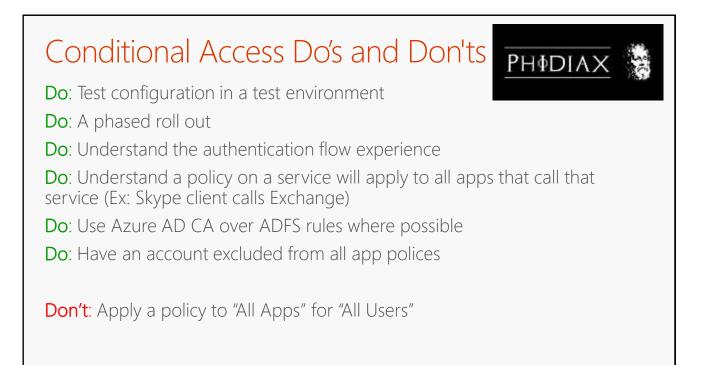
MFA Do's and Don'ts

- Do: Use cloud-based Azure MFA over On-Prem MFA Server
- Do: Know how to troubleshoot MFA authentications
- Do: Know how to troubleshoot Modern Auth issues <u>http://aka.ms/icesdptool</u>
- Do: Use the Mobile App over SMS
- Do: Use Conditional Access
- Do: Consider using Identity Protection

Don't: Assume users / business units will understand why Don't: Forget about the last 5%

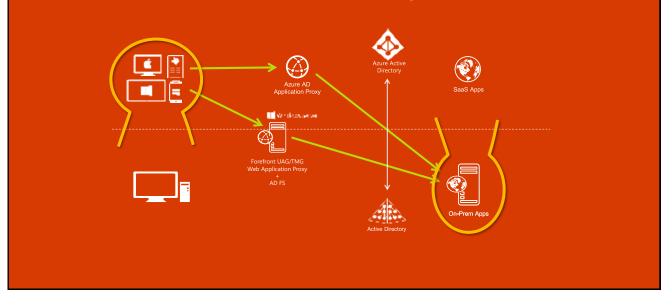
Conditional Access

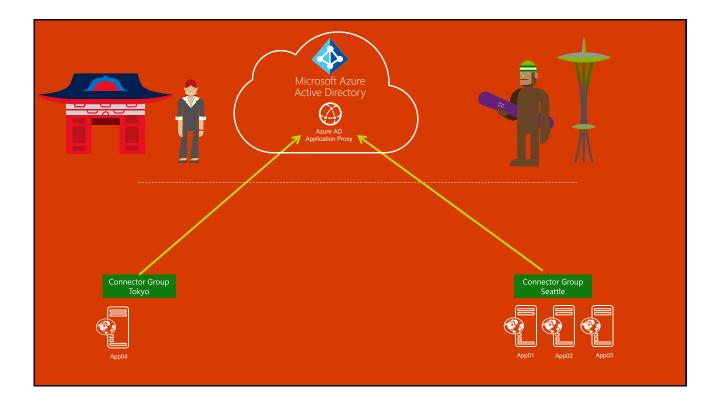




Azure AD Application Proxy

Azure AD App Proxy Reminder





App Proxy Do's and Don'ts

Do: Understand the connector group model
Do: Onboard new apps into their own connector group to start
Do: Set App Proxy Connector Service recovery to restart

Do: Deploy multiple connectors for load balancing / redundancy

Don't: Place the connector in the DMZDon't: Forget about pass through scenariosDon't: Forget about hyperlinks to other internal sites

Azure Active Directory Identity Protection



Azure AD Identity Protection

- Gain real-time insights into threats and suspicious sign-in activity
- Monitor your users patterns and expose obvious threats
- Protect against leaked or compromised credentials
- Enforce conditional access based on risk profile
- Use it as a method to pre-register users for MFA

Identity Protection Do's and Don'ts

- Do: Use group scope for rollout
- Do: Use MFA Pre-Registration
- Do: Enable Sign-in Risk Policy
- Do: Attest/verify MFA registrations
- Do: Delegate read only access to security team

Don't: Enable before you understand User Risk and Sign-in Risk. New Location = MFA challenge **Gotcha**: Securing initial MFA registration



PHOLAX