Identity

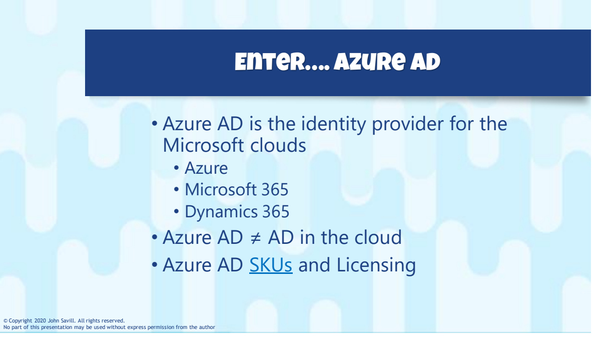
Identity Basics
AD and Azure AD
Conditional Access and MFA
PIM

28

The Need for Identity

- For any service it’s critical to be able to apply the principle of least privilege
- This requires granting certain actions (roles) to certain security principals at a defined scope
- We are focusing on the security principals
- Any actor should be uniquely identifiable
- A central store for the identities is required along with capabilities to use them

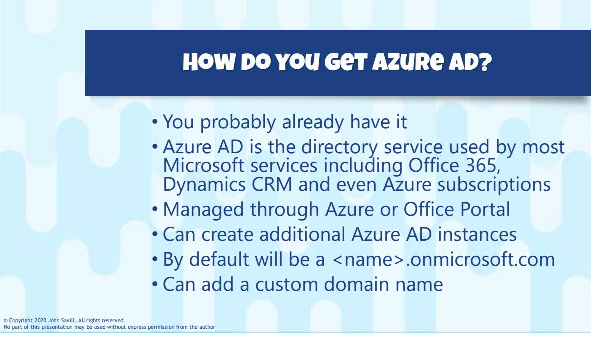
29



Enter.... Azure AD

- Azure AD is the identity provider for the Microsoft clouds
  - Azure
  - Microsoft 365
  - Dynamics 365
- Azure AD ≠ AD in the cloud
- Azure AD SKUs and Licensing

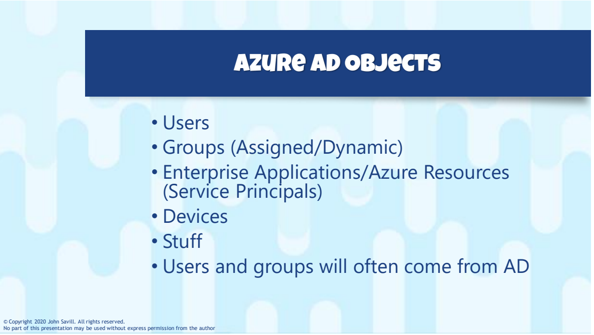
30



How do you get Azure AD?

- You probably already have it
- Azure AD is the directory service used by most Microsoft services including Office 365, Dynamics CRM and even Azure subscriptions
- Managed through Azure or Office Portal
- Can create additional Azure AD instances
- By default will be a <name>.onmicrosoft.com
- Can add a custom domain name

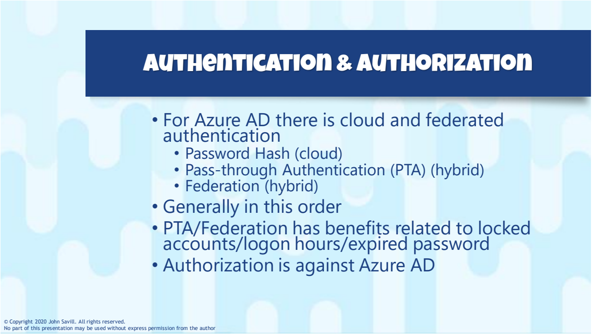
31



Azure AD Objects

- Users
- Groups (Assigned/Dynamic)
- Enterprise Applications/Azure Resources (Service Principals)
- Devices
- Stuff
- Users and groups will often come from AD

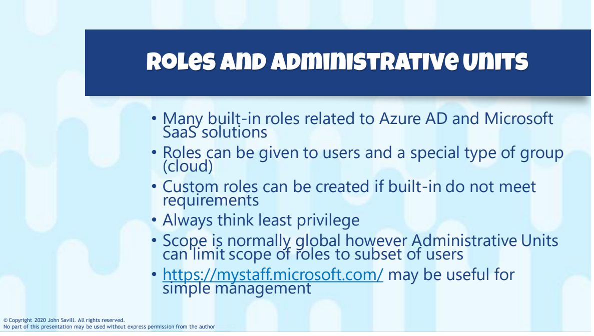
32



Authentication & Authorization

- For Azure AD there is cloud and federated authentication
  - Password Hash (cloud)
  - Pass-through Authentication (PTA) (hybrid)
  - Federation (hybrid)
- Generally in this order
- PTA/Federation has benefits related to locked accounts/logon hours/expired password
- Authorization is against Azure AD

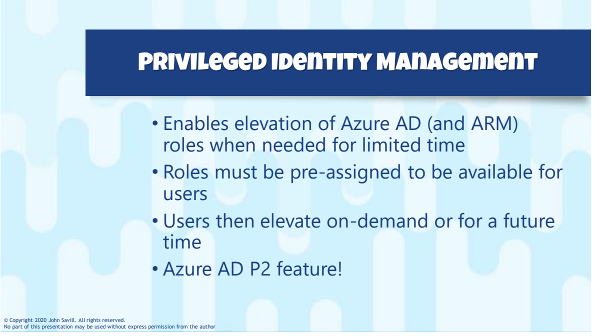
33



Roles and Administrative Units

- Many built-in roles related to Azure AD and Microsoft SaaS solutions
- Roles can be given to users and a special type of group (cloud)
- Custom roles can be created if built-in do not meet requirements
- Always think least privilege
- Scope is normally global however Administrative Units can limit scope of roles to subset of users
- https://mystaff.microsoft.com/ may be useful for simple management

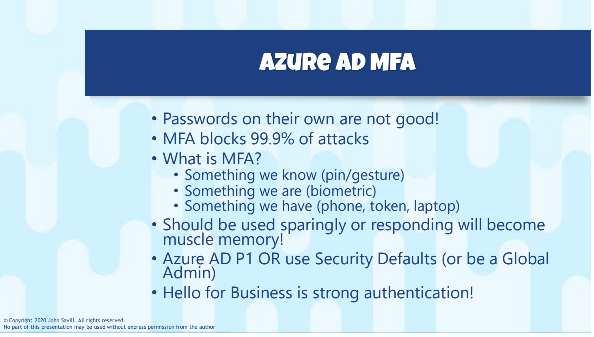
34



Privileged Identity Management

- Enables elevation of Azure AD (and ARM) roles when needed for limited time
- Roles must be pre-assigned to be available for users
- Users then elevate on-demand or for a future time
- Azure AD P2 feature!

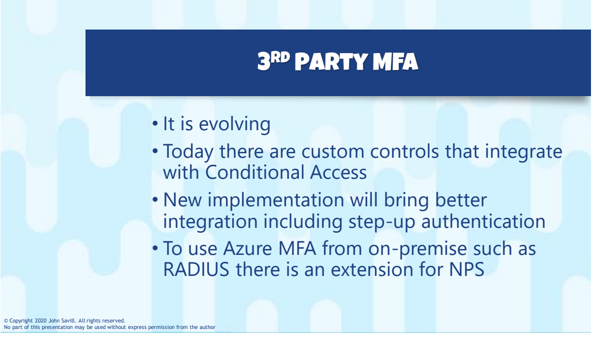
35



Azure AD MFA

- Passwords on their own are not good!
- MFA blocks 99.9% of attacks
- What is MFA?
  - Something we know (pin/gesture)
  - Something we are (biometric)
  - Something we have (phone, token, laptop)
- Should be used sparingly or responding will become muscle memory!
- Azure AD P1 OR use Security Defaults (or be a Global Admin)
- Hello for Business is strong authentication!

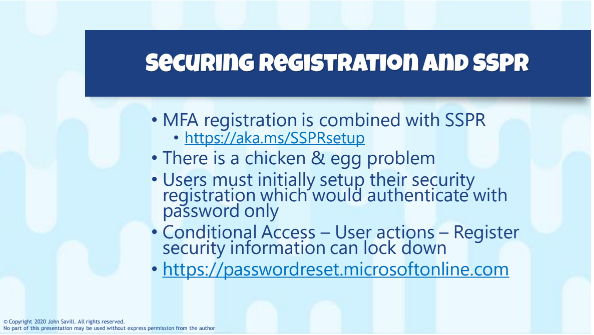
36



3rd Party MFA

- It is evolving
- Today there are custom controls that integrate with Conditional Access
- New implementation will bring better integration including step-up authentication
- To use Azure MFA from on-premise such as RADIUS there is an extension for NPS

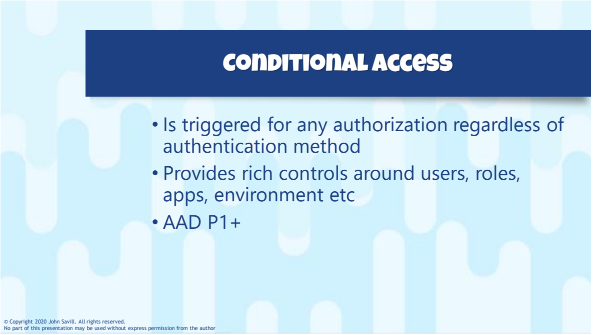
37



Securing Registration and SSPR

- MFA registration is combined with SSPR
  - https://aka.ms/SSPRsetup
- There is a chicken & egg problem
- Users must initially setup their security registration which would authenticate with password only
- Conditional Access – User actions – Register security information can lock down
- https://passwordreset.microsoftonline.com

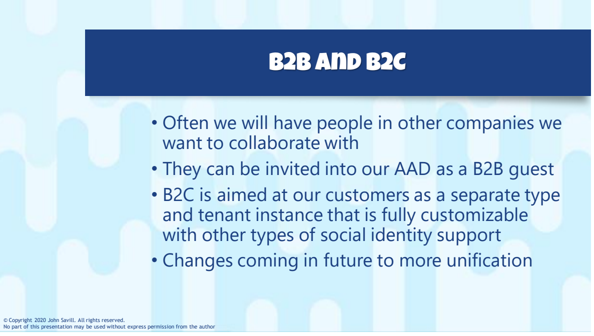
38



Conditional Access

- Is triggered for any authorization regardless of authentication method
- Provides rich controls around users, roles, apps, environment etc
- AAD P1+

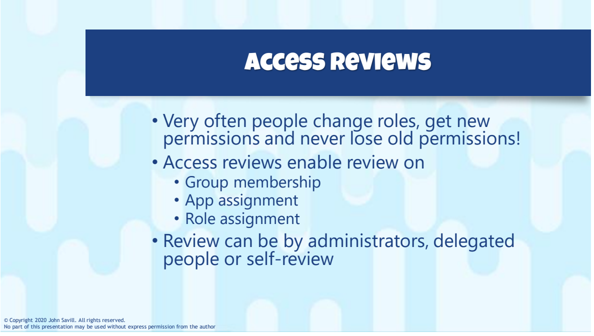
39



B2B and B2C

- Often we will have people in other companies we want to collaborate with
- They can be invited into our AAD as a B2B guest
- B2C is aimed at our customers as a separate type and tenant instance that is fully customizable with other types of social identity support
- Changes coming in future to more unification

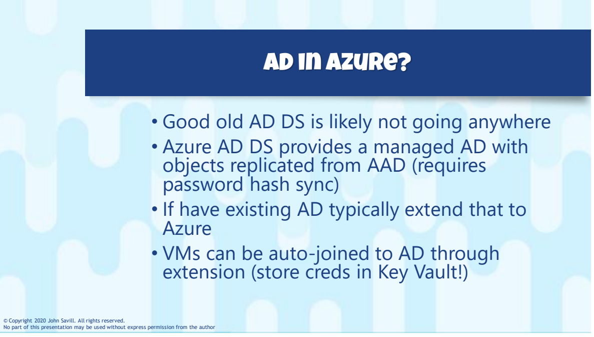
40



Access Reviews

- Very often people change roles, get new permissions and never lose old permissions!
- Access reviews enable review on
  - Group membership
  - App assignment
  - Role assignment
- Review can be by administrators, delegated people or self-review

41



AD in Azure?

- Good old AD DS is likely not going anywhere
- Azure AD DS provides a managed AD with objects replicated from AAD (requires password hash sync)
- If have existing AD typically extend that to Azure
- VMs can be auto-joined to AD through extension (store creds in Key Vault!)

42

Questions?

ASK IN THE COMMENTS

43