NIC Future Edition

Azure AD Authentication and Single-Sign-On deep-dive

John Craddock
Identity and security architect, XTSeminars Ltd
johncra@xtseminars.co.uk @john_Craddock

XTSeminars

What's in this session

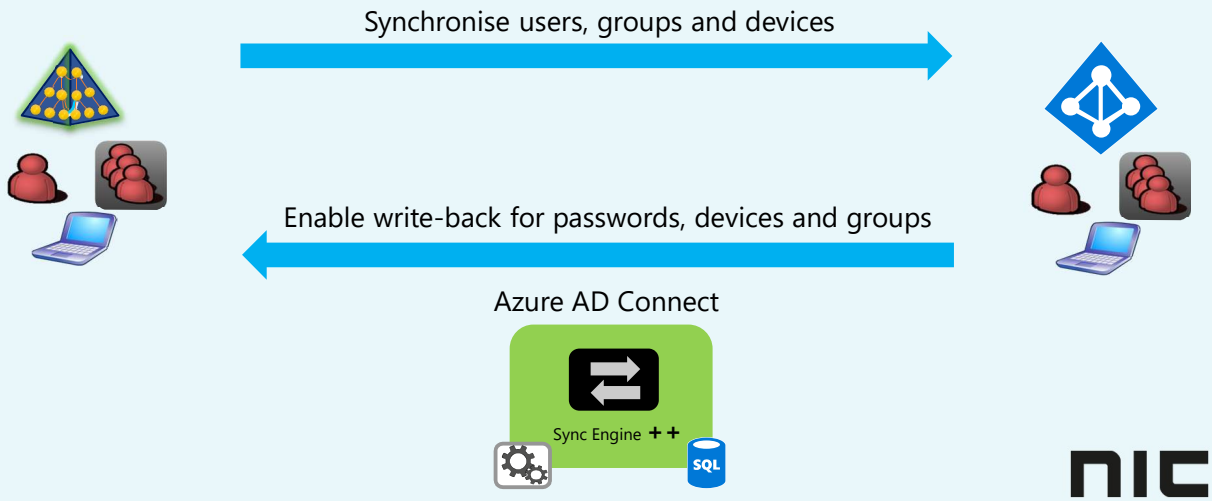
NIC XTSeminars

What's in this session

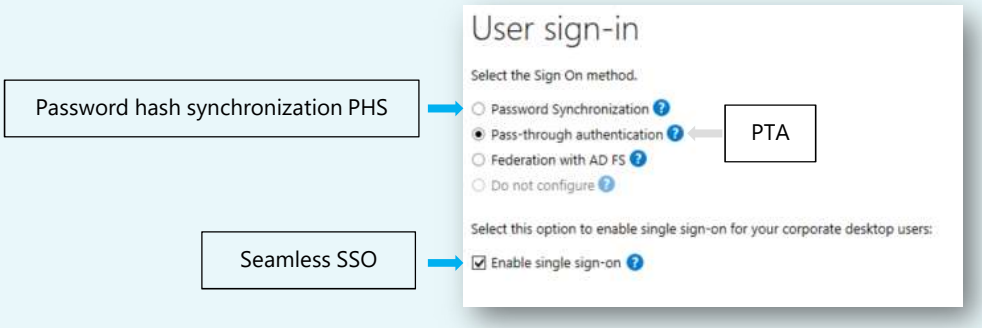
Unleash on-premises AD users

On-premises

Azure AD



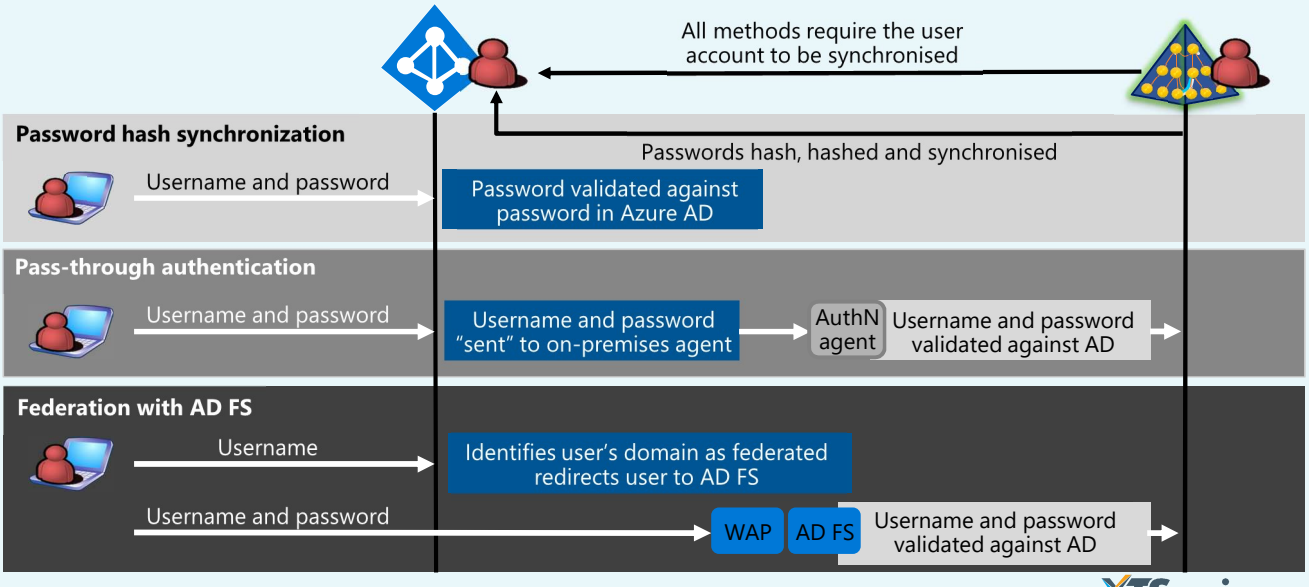
Configuring Azure AD sign-in options



- The options defines how a synchronized on premises user signs in to Azure AD
  - "Do not configure" is used if a 3rd party federated solution is being used
- Seamless SSO works with PHS and PTA

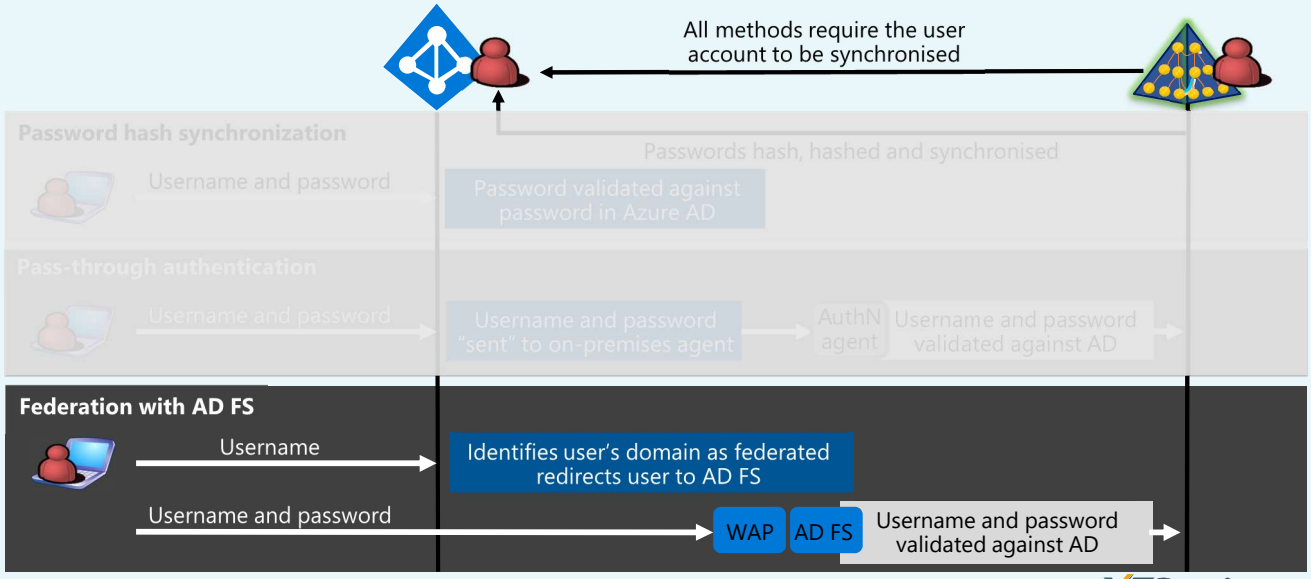
XTSeminars

On-premises user sign-in to Azure AD



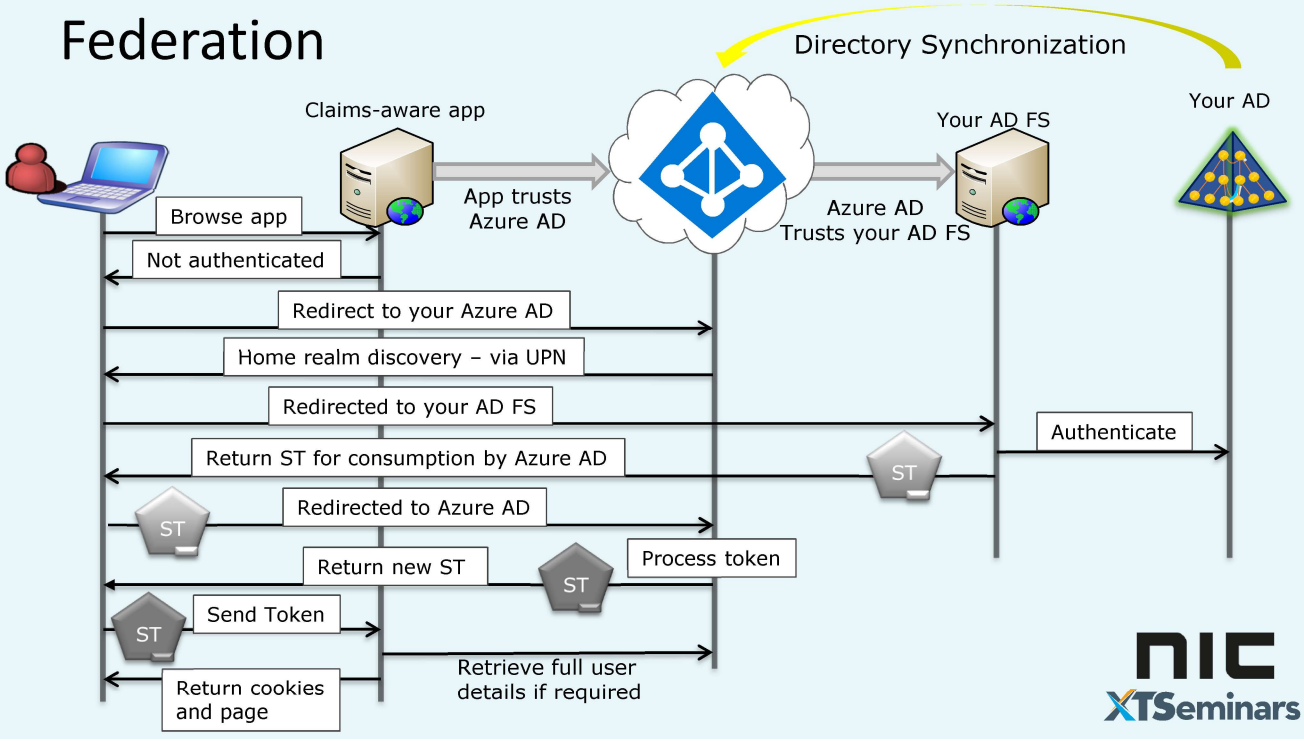
XTSeminars

On-premises user sign-in to Azure AD



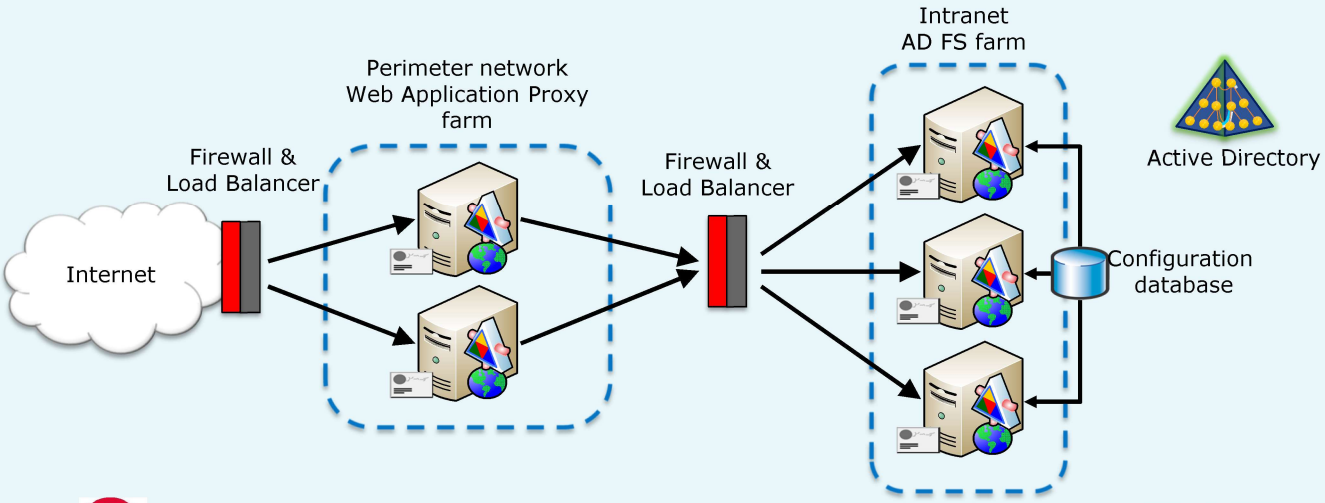
XTSeminars

Federation



XTSeminars

Federation at what cost?



Now fully supported as a WAP replacement

XTSeminars

To federate or not? The facts…

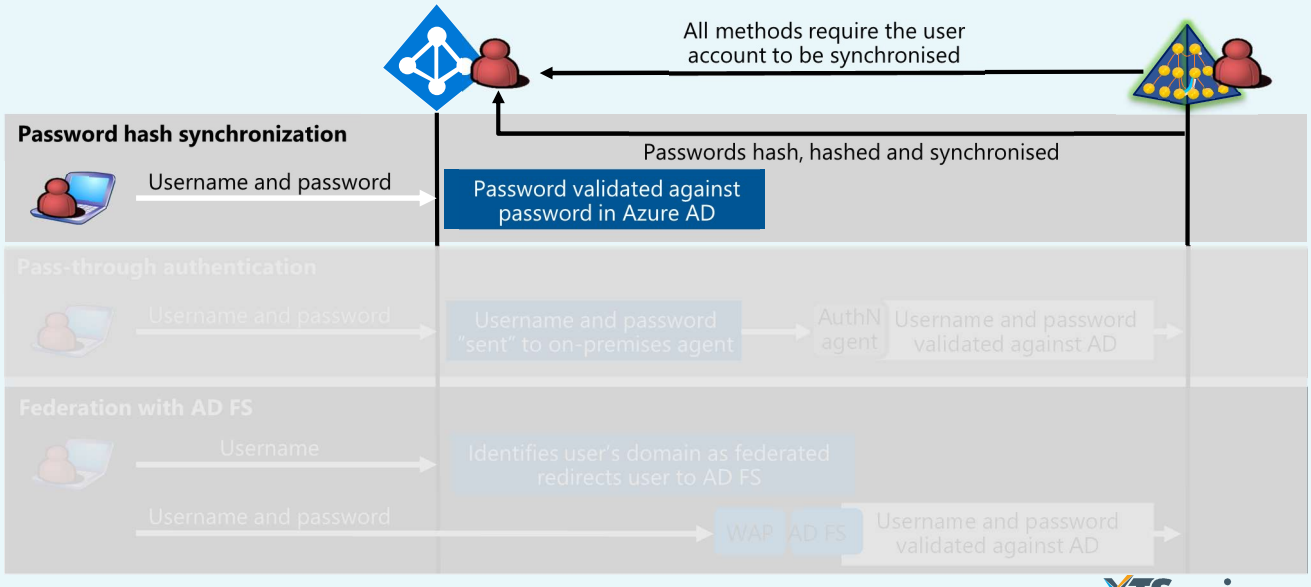
- Federation gives you
  - SSO via on premises AD credentials
    - Seamlessly authenticate to AD FS when the client is attached to the corporate network
      - Now supported by Seamless SSO for PHS and PTA
  - Passwords remain on-premises
    - Now supported via PTA
  - On-premises authentication policies
    - Now supported via PTA
  - On-premises authentication methods (multi-factor)
  - Conditional access via AD FS
    - Capabilities++ provided by Azure AD
- Federation requires
  - On-premises AD FS infrastructure with high-availability
  - High-availability for the company's Internet connection
    - Remote workers will not be able to authenticate to Azure AD If the link is down
  - Planned recovery from the loss of AD FS availability

XTSeminars

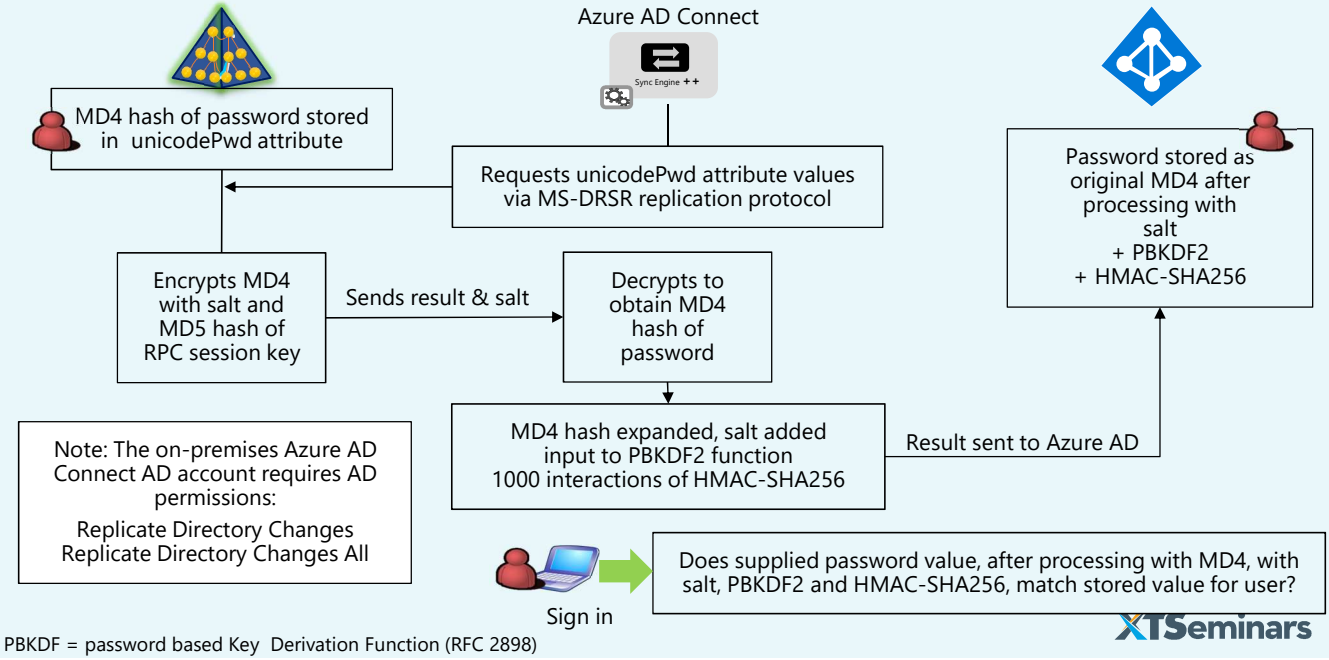
To federate or not? More facts…

- Federation may require manual certificate rollover
  - Auto renewal possible for most configurations (AD FS auto certificate rollover enabled)
- Federation doesn't give you
  - Cloud authentication scalability
  - Identity Protection
    - Requires P2 license
- PHS & PTA
  - Cloud authentication
  - Cloud scalability
  - Identity protect

On-premises user sign-in to Azure AD



Password synchronization



PBKDF = password based Key Derivation Function (RFC 2898)

XTSeminars

Password synchronization facts…

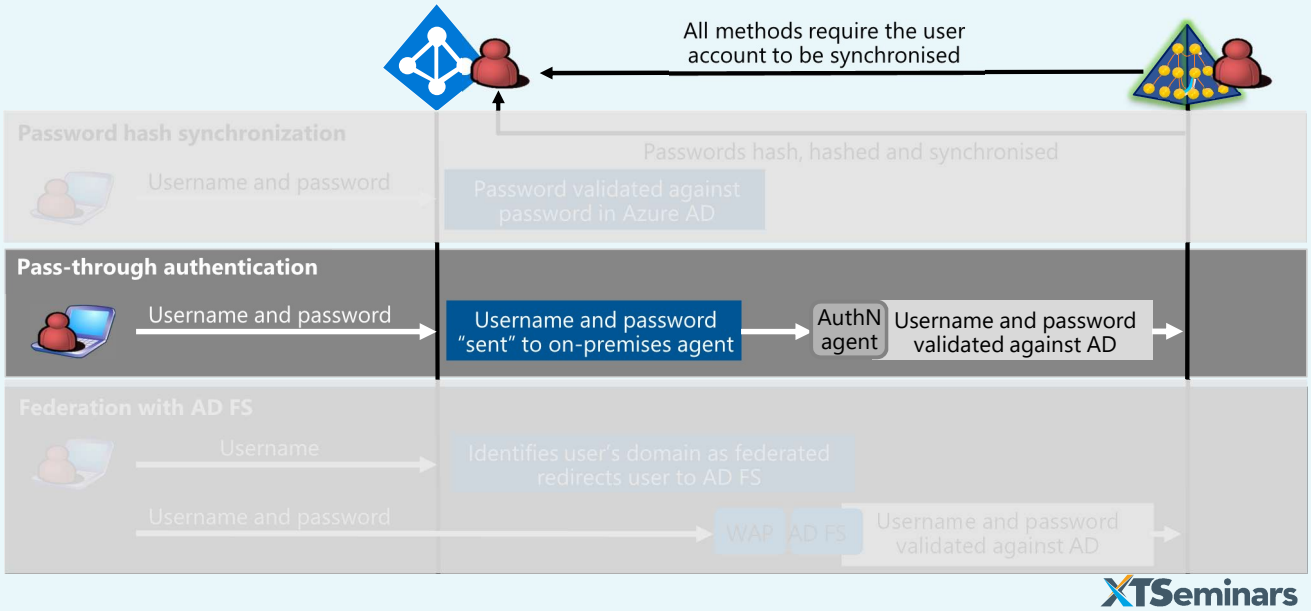
- On-premises password complexity applies to synchronized users
  - If an administrator changes the cloud password using PowerShell the Azure AD password policy applies
- An locked out on-premises AD account can still be active in the cloud
  - The cloud password for a PHS user is set to never expire
- A disabled on-premises AD account will not be reflected in Azure AD until the next sync cycle
  - Potentially 30 mins delay
- PHS can be used in addition to federation and used as a fall-back

XTSeminars

Demo…

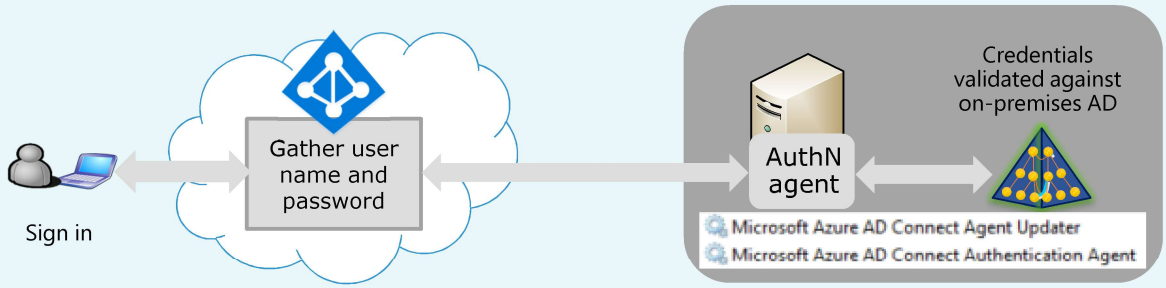
Password hash synchronization

On-premises user sign-in to Azure AD



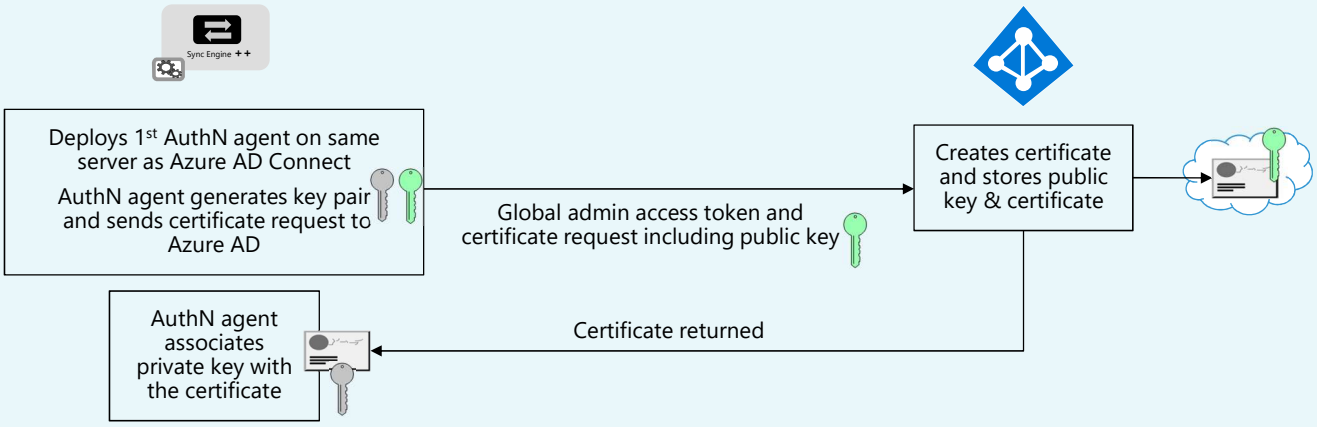
XTSeminars

Pass-through authentication



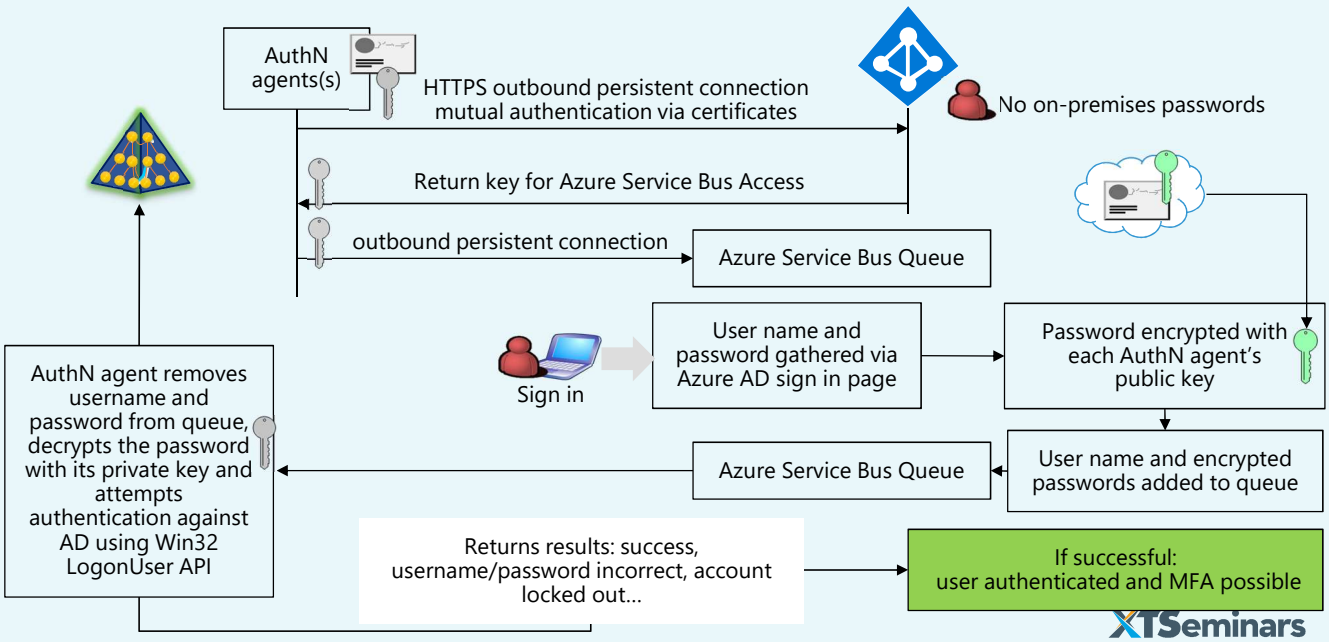
- The pass-through authentication agent (AuthN agent) only requires outbound firewall ports
  - Port 80 and 443
- Multiple agents can be deployed for fault tolerance and performance
  - Three agents should provide required performance
- All communications via mutually authenticated HTTPS

Pass-through authentication installation



- Each agent has its own unique certificate and private key
  - Azure AD periodically triggers the renewal of certificates and keys

Pass-through authentication in action



Account lockout

- Azure AD Smart Lockout protects against brute-force attacks and on-premises account lockout
- Locks account in Azure AD
  - Lockout Threshold – default 10 failed attempts
  - Lockout Duration – default 60 seconds
    - Automatically increases with a continuing attack
- Machine intelligence algorithms attempt to distinguish between genuine users and attackers
  - Factors include past sign-in behaviour, user's devices and browsers
  - Lockout Threshold automatically adjusted

XTSeminars

Protecting on-premises account lockout

- Smart Lockout (SL) threshold must be less than on-premises AD lockout threshold
  - Recommended AD threshold two or three times higher than SL threshold
- SL duration should be longer than AD lockout duration
- Smart Lockout is included with all versions of Azure AD
- The Smart Lockout values can only be changes by an administrator with a P2 license
  - Programmatically set via graph API

https://graph.microsoft.com/beta/<tenantID>/settings


```
{
 "templateId": "5cf42378-d67d-4f36-ba46-e8b86229381d",
 "values": [
  {
   "name": "LockoutDurationInSeconds",
   "value": "120"
  },
  {
   "name": "LockoutThreshold",
   "value": "15"
  },
  {
   "name" : "BannedPasswordList",
   "value": ""
  },
  {
   "name" : "EnableBannedPasswordCheck",
   "value": "false" } ]
}
```


Pass-through authentication the facts…

- No on premises passwords in the cloud
- All on-premises password policies operational
- Account lockout/disabled operational
- Does not support on-premises MFA
  - Azure AD MFA supported
- Works with Alternate ID
- Does not provide SSO for on-premises credentials
  - Requires Seamless SSO
- Requires high-availability for the company's Internet connection
  - Remote workers will not be able to authenticate to Azure AD If the link is down
- Currently does not support legacy auth
  - Example Office 2010

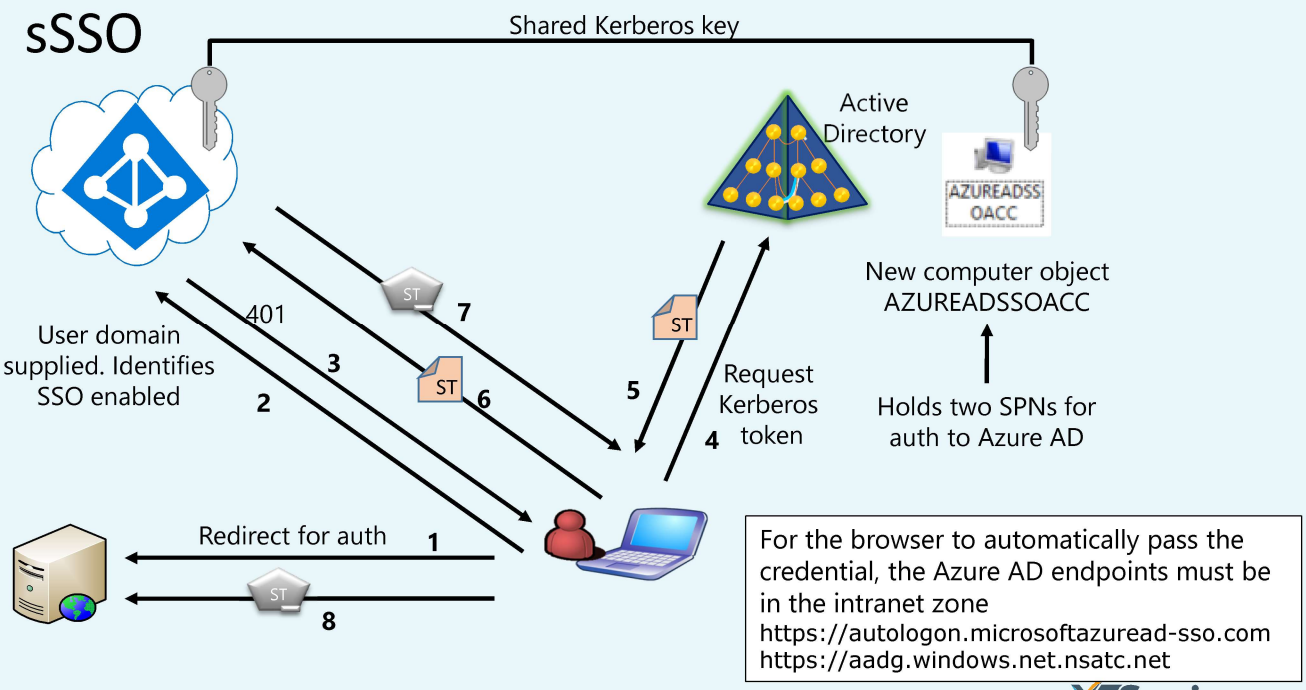
Demo…

Pass-through authentication

What's in this session

Seamless SSO, the facts…

- Works with pass-through authentication or password hash sync
- Users only need to type their name to authenticate to Azure AD
  - It is possible for applications to pass a domain_hint for seamless SSO
    - Access panel - myapps.microsoft.com/*example.com*
  - Supports Windows 7 and above
    - Windows 10 Edge not currently supported
  - Machine must be domain joined and have access to a DC
    - On corporate network or via remote access technology
  - Authenticates to Azure AD with a Kerberos token
  - Available with all versions of Azure AD
  - Supports Alternate ID
  - Support for multiple browsers and OSs
    - Including Safari and Mac



Kerberos authentication

- Seamless SSO can be configured with PTA or PHS
- If the user is connected to the corporate AD domain and sSSO succeeds, the authentication to Azure AD is Kerberos
- If the user is not connected to the corporate AD domain, authentication will fall-back to select authentication method (PTA or PHS)
- If an incompatible or mis-configured browser is detected, authentication will fall-back to select authentication method (PTA or PHS)

XTSeminars

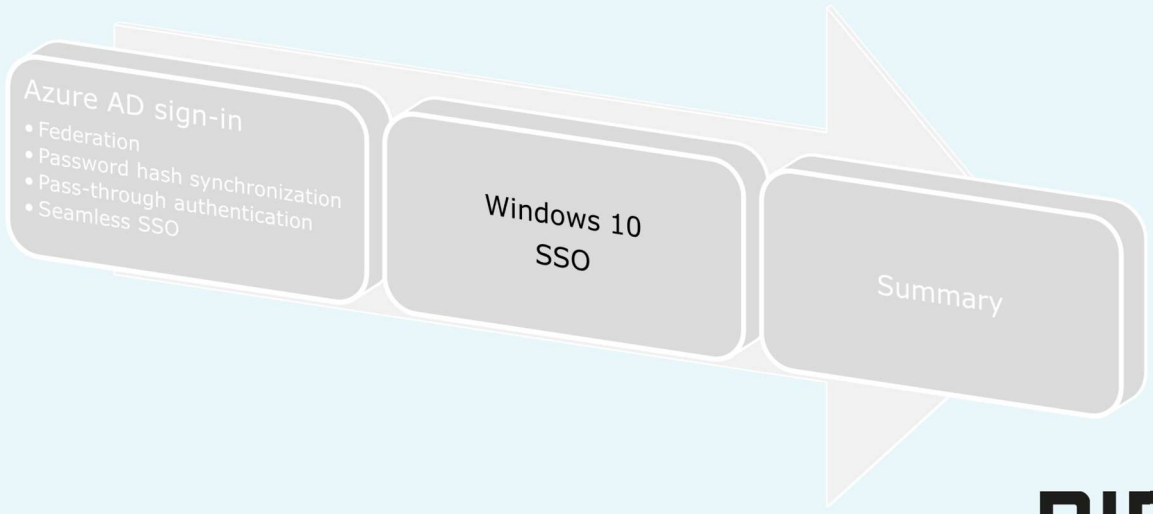
Kerberos Key

- The security of your on-premises authentication relies on the integrity of the Kerberos key
  - Recommended to roll the key every 30 days
- For details of managing key rolling see:
  - https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-sso-faq
- Automatic key rollover is on the roadmap!

Demo…

Seamless SSO

What's in this session



Windows 10 and AD users

- Hybrid Azure AD Join
  - AD Domain Join with automatic Azure AD registration
  - All the benefits of Group Policy / SCCM / Intune
- When users sign-in to their device they get a
  - Kerberos token for on-premises AD and Primary Refresh Token (PRT) for Azure AD access
- Single sign on to all Azure AD authenticated resources
  - No requirement to have access to a DC
- Conditional access policies can be based on the user's device
- Windows Hello for Business can be used for authentication

What's in this session

Feature summary	PTA + sSSO	PHS + sSSO	ADFS
Authentication against credentials held on-premises	Yes	No	Yes
Single-Sign-On	Yes	Yes	Yes
Passwords remain on premises	Yes	Salted hash synced	Yes
On-premises MFA solution	No	No	Yes
Azure AD MFA	Yes	Yes	Yes
On-premises password policies	Yes	Partial	Yes
On-premises account enable/disable	Yes	Delayed (30 mins)	Yes
On-premises password lockout	Yes	No	Yes
Conditional access	Yes++	Yes++	Yes
Credentials captured from user via Azure AD UI	Yes	Yes	No
Protection against on-premise account lockout	Smart Lockout	N/A	Extranet Lockout
Cost of implementation	Medium	Low	High
Scalability/fault tolerance	Cloud scalability	Cloud scalability	Complex
AuthN **fails** for remote workers if the on-premises Internet connection is down. Requires HA solution.	Yes	No	Yes
On-going maintenance for authentication	Automated	None	SSL certificate management
Azure AD Connect Health monitoring	Not integrated	Limited	Yes
Azure AD Identity Protection (requires P2 license)	Yes	Yes	No

Recommendations

- New customers:
  - Use cloud authentication (PTA or PHS)
    - Leverage conditional access and Azure AD MFA
  - Existing customers with AD FS
    - Keep AD FS for authentication if it meets all your requirements
    - If using AD FS for authentication to apps, switch to Azure AD for authentication to apps
- Enable Seamless SSO if your using PTA or PHS
  - Simple to deploy
  - Immediately enhances the sign-in experience for your users
  - Implement domain_hint for custom apps

So where next?

5-Day Hands-On Masterclass with John Craddock

Microsoft Identity solutions with Azure Active Directory, on-premises AD FS and AD

38 hands-on labs

10% Discount if you book by this Friday for:
Oslo : April 23 – 27 or
Oslo : August 27 - 31

Talk to the Crayon team or email info@niccomf.com

http://www.xtseminars.co.uk/masterclass

Consulting services on request

John Craddock
Infrastructure and security Architect
XTSeminars Ltd

Johncra@xtseminars.co.uk
@john_craddock

John has designed and implemented computing systems ranging from high-speed industrial controllers through to distributed IT systems with a focus on security and high-availability. A key player in many IT projects for industry leaders including Microsoft, the UK Government and multi-nationals that require optimized IT systems. Developed technical training courses that have been published worldwide, co-authored a highly successful book on Microsoft Active Directory Internals, presents regularly at major international conferences including TechEd, IT Forum and European summits. John can be engaged as a consultant or booked for speaking engagements through XTSeminars. www.xtseminars.co.uk

NIC XTSeminars

Resources

Slides and demos from the conference will be available at github.com/nordicinfrastructureconference/2018 (bit.ly/2y7JhA3)

NIC