Office 365 and Azure Active Directory Identities In-depth

Jethro Seghers
Program Director
SkySync
Agenda

• Introduction Identities
• Different forms of authentication
• Azure Active Directory Premium
• QA
Today’s identity challenges
Users signed-in to Azure AD have SSO to all applications.

Management portal(s) → Authenticate to
Powershell → Authenticate to
GRAPH APIs → Authenticate to

Synchronise users from your AD DS

Your tenant
Your data

Azure subscriptions → Authenticate to
Office365 → Authenticate to
Your apps → Authenticate to
Partner apps → Authenticate to
Application gallery → Authenticate to
## Different Identities

### 1. MS Online IDs
- **Appropriate for**
  - Smaller organizations without AD on-premise

- **Pros**
  - No servers required on-premise

- **Cons**
  - No SSO
  - 2 sets of credentials to manage with differing password policies
  - Users and groups mastered in the cloud

### 2. MS Online IDs + AADConnect
- **Appropriate for**
  - Orgs with AD on-premise

- **Pros**
  - No servers required on-premise
  - Users and groups mastered on-premise
  - Enables co-existence scenarios
  - Several SSO options

- **Cons**
  - Single server deployment (?)

### 3. Federated IDs + AADConnect
- **Appropriate for**
  - Larger enterprise organizations with AD on-premise

- **Pros**
  - SSO with corporate cred
  - Full control over authentication
  - Support for non-AD systems

- **Cons**
  - High availability server deployments required
Identity architecture: Identity options

1. Microsoft Online IDs
2. Microsoft Online IDs + AADConnect
3. Federated IDs + AADConnect
What is AADConnect?

“...is a Directory Synchronization engine based on Forefront Identity Manager (FIM) that will synchronize a subset of your on-premise Active Directory with Windows Azure Active Directory (Office 365).”
On-premises: Synchronise users, groups and devices. Requires immutable ID. Enable write-back for passwords, devices and groups.

Azure AD:
Continuously evolving product
Automatic upgrades are possible
Set-ADSyncAutoUpgrade

AD account to access AD
AD account should only have the privileges necessary to perform required tasks
Sync Engine ++
Service account to run Azure AD Connect
SQL
Azure AD account to access Azure AD
SQL Server 2012 Express LocalDB or SQL Server 2008 or higher
How does AADConnect work?
Demo: AAD Connect
AD Connect replaces earlier tools, upgrades are possible
DirSync
Azure AD Sync
FIM and the Azure AD Connector
++ more than just a synchronization engine
Manages user sign-in options
Write-back for password, devices and groups
Tools to support AD FS
  - Simple UI experience to update AD FS SSL certificates
  - Fix trust
  - Login testing
Azure AD Connect Health agent, reports status to the Azure AD Connect Health Portal
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites
• One-stop shop for viewing the health of your identity infrastructure
  • Azure AD Connect
  • AD FS
  • On-premises AD
• Agents installed on identity infrastructure components
  • Monitoring and alerts
  • Email notification of critical alerts
  • Trends in performance data
  • Usage reports
• Requires a P1 license
Username and password validated against AD

**Password hash synchronization**

Username and password

Password validated against password in Azure AD

**Pass-through authentication**

Username and password

Username and password “sent” to on-premises agent

AuthN agent validated against AD

**Federation with AD FS**

Username

Identifies user’s domain as federated

Redirects user to AD FS

Username and password validated against AD
User attributes are synchronized using Identity Synchronization services including a password hash, Authentication is completed against Azure Active Directory.
Identity Synchronization tools, **Authentication is passed back through federation** and completed against **Windows Server Active Directory**.

User attributes are synchronized using Identity Synchronization tools, **Authentication is passed back through federation** and completed against **Windows Server Active Directory**.
User attributes are synchronized using Identity Synchronization tools, **Authentication is completed against Windows Server Active Directory using the Passthrough Agent**.
All methods require the user account to be synchronised

**Password hash synchronization**
- Username and password
- Password validated against password in Azure AD
- Passwords hash, hashed and synchronised

**Pass-through authentication**
- Username and password
- Username and password "sent" to on-premises agent
- AuthN agent
- Username and password validated against AD

**Federation with AD FS**
- Username
- Identifies user’s domain as federated
- Redirects user to AD FS
- Username and password validated against AD
Process token

Home realm discovery – via UPN

Redirected to your AD FS

Return ST for consumption by Azure AD

Return new ST

Claims-aware app

Your AD FS

Your AD

Authenticate

Directory Synchronization

App trusts Azure AD

Azure AD Trusts your AD FS

Browse app

Not authenticated

Redirect to your Azure AD

Home realm discovery – via UPN

Redirected to your AD FS

Redirected to Azure AD

Return ST for consumption by Azure AD

Redirected to Azure AD

Return new ST

Process token

Send Token

Retrieve full user details if required

Return cookies and page
Active Directory Firewall & Load Balancer
Perimeter network Web Application Proxy farm
Firewall & Load Balancer
Intranet AD FS farm
Configuration database
Internet
Firewall & Load Balancer
Active Directory
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
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

**PTA**
Simple deployment of agents
Automatic update of on-premises agents
Automatic rollover of certificates
Requires high-availability for the company’s Internet connection
Username and password validated against AD

Password hash synchronization

Username and password

Passwords hash, hashed and synchronised

Password validated against password in Azure AD

All methods require the user account to be synchronised

Pass-through authentication

Username and password

Username and password "sent" to on-premises agent

AuthN agent

Username and password validated against AD

Federation with AD FS

Username

Identifies user's domain as federated
redirects user to AD FS

WAP AD FS

Username and password validated against AD
Sends result & salt

Requests `unicodePwd` attribute values via MS-DRSR replication protocol

Encrypts MD4 with salt and MD5 hash of RPC session key

Sends result & salt

Decrypts to obtain MD4 hash of password

MD4 hash expanded, salt added input to PBKDF2 function

1000 interactions of HMAC-SHA256

Result sent to Azure AD

Password stored as original MD4 after processing with salt + PBKDF2 + HMAC-SHA256

Note: The on-premises Azure AD Connect AD account requires AD permissions:
- Replicate Directory Changes
- Replicate Directory Changes All

Does supplied password value, after processing with MD4, with salt, PBKDF2 and HMAC-SHA256, match stored value for user?

PBKDF = password based Key Derivation Function (RFC 2898)
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
All methods require the user account to be synchronised.

**Password hash synchronization**
- Username and password
- Password validated against password in Azure AD
- Passwords hash, hashed and synchronised

**Pass-through authentication**
- Username and password
- Username and password “sent” to on-premises agent
- Username and password validated against AD
- AuthN agent

**Federation with AD FS**
- Username
- Identifies user’s domain as federated
- Redirects user to AD FS
- Username and password validated against AD

WAP, AD FS
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
Each agent has its own unique certificate and private key. Azure AD periodically triggers the renewal of certificates and keys.
HTTPS outbound persistent connection
mutual authentication via certificates

Return key for Azure Service Bus Access

outbound persistent connection

Azure Service Bus Queue

User name and encrypted password added to queue

Password encrypted with each AuthN agent’s public key

User name and password gathered via Azure AD sign in page

Sign in

AuthN agent removes username and password from queue, decrypts the password with its private key and attempts authentication against AD using Win32 LogonUser API

Returns results: success, username/password incorrect, account locked out...

If successful: user authenticated and MFA possible

No on-premises passwords
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
AAD Premium introduction: Demo
Q&A