



Hybrid Identity: Choosing the Right Authentication Method

Choosing the Right Hybrid Identity Authentication: Real-World Breakdown

Breaking down three authentication methods for hybrid identity management, plus Single Sign-On (SSO).



Password Hash Sync



Pass-Through Auth



AD FS



Single Sign-On

Password Hash Sync | Pass-Through Auth | Federation



Perparim Abdullahu
SC-300 in Progress


Why Authentication Matters



Hybrid environments require secure, efficient sign-in methods.
Choosing the right method impacts:


- **Security**
- **Compliance**
- **User Experience**
- **Operational Overhead**

Method 1 – Password Hash Synchronization (PHS)

- **Microsoft's Recommended Approach**
- Syncs password **hashes** (not plaintext) to Microsoft Entra ID
- Users can log in from anywhere—even if on-prem is offline
- **Extra benefit:** Microsoft monitors dark web for stolen hashes
-  *Compliance concern: Some industries (e.g. healthcare) may not allow password hash sync*




Method 2 – Pass-Through Authentication (PTA)

- Password stays **on-prem**, never stored in Azure
- Uses **PTA agent** to validate credentials
- Easier setup than federation
- Good for compliance-focused environments
-  *If on-prem is down, cloud sign-in fails for remote users*



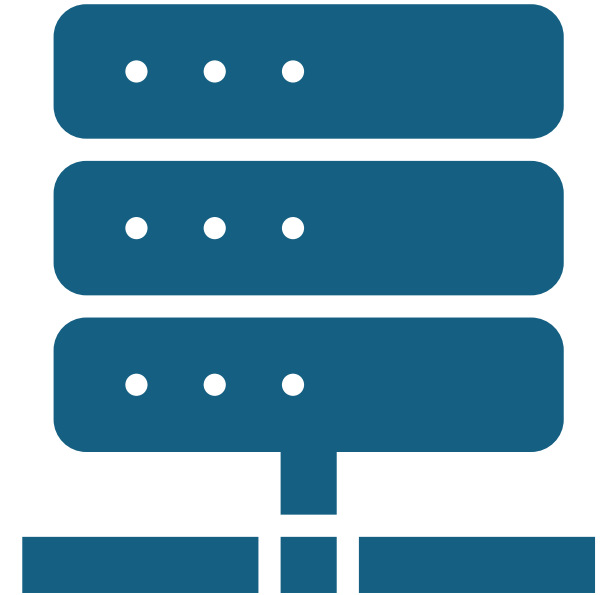
Method 3 – Federated Authentication (ADFS)

- For **large enterprises** with advanced auth needs
- Supports **smart cards, third-party MFA**, legacy systems
- Requires:
 - 2 ADFS servers (internal)
 - 2 ADFS proxies (DMZ)
-  *Costly, complex, high-maintenance—but powerful*



Flexibility & Seamless SSO

- Azure AD Connect setup isn't permanent—you can switch later
- **Seamless SSO** = automatic sign-in from domain-joined PCs
 - No second login prompt
 - Works best with PHS
- 💡 Tip: Seamless SSO improves UX without extra setup








What Should You Choose?

Ask yourself:

- Do you need 3rd-party MFA? → Federation
- Do you need compliance w/o cloud hashes? → PTA
- Want easiest, most flexible setup? → PHS
- Want zero login prompts? → Enable Seamless SSO
- ☒ *Balance security, compliance, and user experience*



Summary

-  **PHS** – Easiest & Recommended
-  **PTA** – Great for compliance, no cloud hashes
-  **Federation** – Powerful but complex
-  Seamless SSO enhances user experience
-  Choose what fits your org's size, policy & security model