

- For Hybrid Identity Scenarios

Choosing the Right Azure AD Authentication Method for Hybrid Identity

- Perparim Abdullahu – AZ-305 Certified | SC-300 in Progress

Why This Matters

- When syncing on-prem AD with Azure AD, how you authenticate users matters. Here are the 3 main hybrid identity options — and how to choose the right one.




Password Hash Synchronization (PHS)

✓ Most popular and Microsoft-recommended

- Hash of the on-prem password is synced to Azure AD
- ✓ Easy setup via Azure AD Connect
- ✓ Supports cloud sign-in even if on-prem is down
- ✗ May not meet strict compliance





Pass-Through Authentication (PTA)

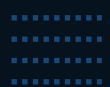
For when hash sync isn't allowed

- Password checked against on-prem AD via secure agent
-  Microsoft never stores password
-  Requires on-prem connectivity
-  Remote users can't log in if network is down

Federated Authentication (AD FS)

Best for large orgs or 3rd-party MFA

- Auth handled by your AD FS server
-  Microsoft never sees passwords
-  Supports smartcards, custom MFA
-  Complex to deploy & maintain
-  Still depends on on-prem availability



Visual Summary



| Method | Microsoft Knows Password? |
|--------|---------------------------|
| PHS | Hash Only |
| PTA | No |
| AD FS | No |

| On-Prem Required? |
|-------------------|
| No |
| Yes |
| Yes |

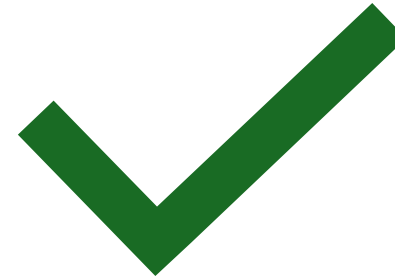
| Recommended For |
|-------------------------|
| Most orgs |
| Compliance-focused orgs |
| Large/Custom MFA orgs |

My Choice in Labs



In my hybrid identity lab, I chose **Password Hash Sync (PHS)** because:

- ✓ It's easy to set up
- ✓ Supports remote users
- ✓ Doesn't require on-prem to be online



I'd recommend PHS unless compliance or 3rd-party auth requires otherwise.

Final Takeaway

