

Securing a Hybrid Active Directory Environment

Derek Melber

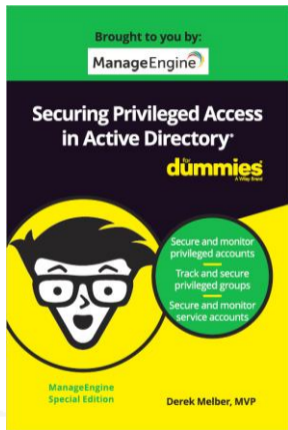
derek@manageengine.com

About Your Speaker



About Derek Melber

- Derek Melber
 - Chief Technology Evangelist
 - MVP (AD and Group Policy)
 - derek@manageengine.com
- Online Resources
 - ManageEngine Active Directory Blog
 - Security Hardening Site
 - Download free Dummies book
- 2019 World Tour



Agenda

- What is hybrid?
- History of password management
- Hybrid password management environment
- Hybrid AD: Password Sync
- Hybrid AD: Single Sign On
- Hybrid AD: Self-service password reset

WHAT IS HYBRID?

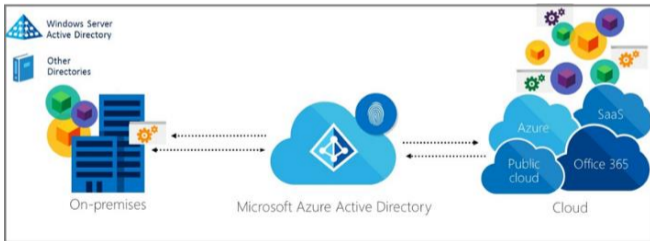


What is Hybrid (for our definition)

- On-prem Active Directory

AND

- Azure Active Directory (AAD)



According to Microsoft

Hybrid cloud is more common than you may think

67% of survey respondents were already using hybrid cloud or considering it as a future option.



67%

According to Reality

- Over 500 attendees in Microsoft Server session
 - How many will of you will be one of these in 5 years:
 - ON-prem only: 25%
 - Cloud only: 0%
 - Hybrid: 75%



HISTORY OF PASSWORD MANAGEMENT

History of password management

- Of course... on-prem Active Directory password management is all we have had
- Key factors
 - No need for password sync... everything was on-prem AD
 - Users changed password from Ctrl-Alt-Del
 - Password was only needed for on-prem, as all apps local
 - No need for single sign on... all apps local
 - Did not have any self-service password reset option



HYBRID PASSWORD MANAGEMENT ENVIRONMENT

Hybrid password management environment

- Too many passwords
- Password change in one system fails to update in another system
- Too many sign ons...on-prem, AAD/O365, cloud app(s)
- Self-service password reset for all aspects of life... just not at work!



HYBRID AD: PASSWORD SYNC

Hybrid AD: Password Sync

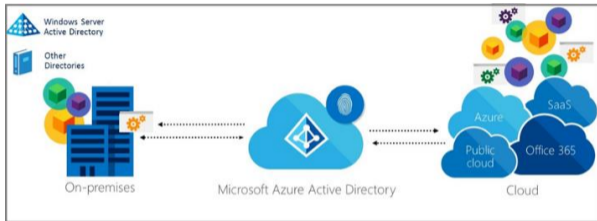
- Users have many usernames and passwords
 - On-prem AD
 - AAD/O365
 - Salesforce
 - IBM/AS400
 - Etc.

Hybrid AD: Password Sync

- When user changes password on-prem, why not changed everywhere?



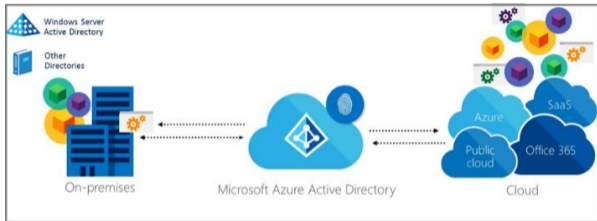
Hybrid AD: Password Sync



Option 1:

- Change password on-prem
- AD Connect sync with AAD
- AAD sync with cloud apps
- Why configure two locations to sync “from”?

Hybrid AD: Password Sync



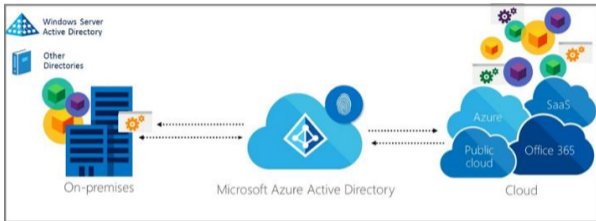
Option 2:

- Change password in AAD
- AD Connect sync with on-prem AD
- AAD sync with cloud apps
- Do users know how to change password in AAD?
- What are limitations of password changes in ADD?

Hybrid AD: Password Sync

- Azure AD portal password limitations
 - Allowed characters: aA1\$
 - **Disallowed characters:** Unicode and spaces (Yes, NO SPACES!)
 - **Password length:** 8 to 16 characters (Yes, 16 char maximum!)
 - 3 of 4 allowed characters required
 - Maximum password age: 90 days
 - Password expiration notification: 14 days
 - **Password history** for changes: Last password
 - **Password history** for reset: No history
 - Lockout threshold: 10
 - Lockout duration: 1 min

Hybrid AD: Password Sync



Option 3:

- Change password in on-prem AD
- ADSSP sync password with AAD and all cloud apps
- Users use same Ctrl-Alt-Del password change they are used to
- Increase passwords with Password Enforcer
- User is not confused as to why password change on-prem does not update AAD/Cloud

Hybrid AD: Password Sync

The screenshot shows the management console for Password Sync/Single Sign On. At the top, there is a header with the title "Password Sync/Single Sign On" and a subtitle "Integrate the various components to get a complete solution for your AD environment." To the right of the header are two buttons: "Account Linking" and "+ New Custom App". Below the header is a search bar and a dropdown menu showing "Password Sync(15)". A red warning banner states: "Important : Install the Password Sync Agent to synchronize native password changes and resets. [Learn more](#)". The main content area displays a grid of application tiles, each with a logo and a name: IBM /AS400 System, HP UX Directory Server, Google Apps, Oracle E-Business Suite, Oracle Database, Office 365 / Azure, Salesforce, Zoho, and Zendesk.

Password Sync/Single Sign On
Integrate the various components to get a complete solution for your AD environment.

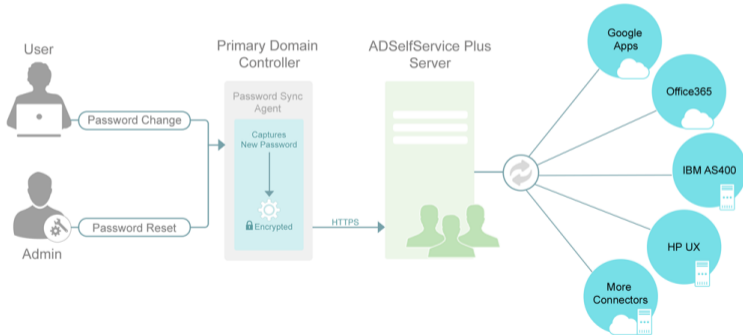
Account Linking + New Custom App

Search: Password Sync(15)

Important : Install the Password Sync Agent to synchronize native password changes and resets. [Learn more](#)

 IBM /AS400 System	 HP UX Directory Server	 Google Apps
 Oracle E-Business Suite	 Oracle Database	 Office 365 / Azure
 Salesforce	 Zoho	 Zendesk

Hybrid AD: Password Sync





HYBRID AD: SINGLE SIGN ON (SSO)

Hybrid AD: Single Sign On

- Must sign on to every application, every time!
 - On-prem
 - Office 365
 - Salesforce
 - Dropbox
 - Etc.

Hybrid AD: SSO

- Once user logs into on-prem AD... access to cloud apps!



Hybrid AD: Single Sign On

The screenshot shows a web-based management console for Password Sync/Single Sign On. At the top, there is a header with the title "Password Sync/Single Sign On" and a subtitle "Integrate the various components to get a complete solution for your AD environment". To the right of the header are two buttons: "Account Linking" and "New Custom App". Below the header is a search bar and a dropdown menu showing "Single Sign On(110)". A red warning banner states: "Important : Install the Password Sync Agent to synchronize native password changes and resets. [Learn more](#)". The main content area displays a grid of application tiles for integration, each with a logo and a name: Google Apps, Office 365 / Azure, Salesforce, Zoho, Zendesk, Dropbox, PagerDuty, PlanMyleave, and Mingle.

Password Sync/Single Sign On
Integrate the various components to get a complete solution for your AD environment

Account Linking New Custom App

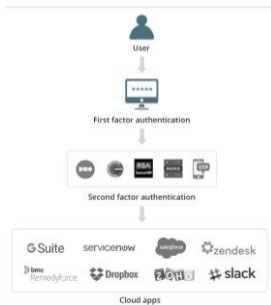
Search Single Sign On(110)

Important : Install the Password Sync Agent to synchronize native password changes and resets. [Learn more](#)

 Google Apps	 Office 365 / Azure	 Salesforce
 Zoho	 Zendesk	 Dropbox
 PagerDuty	 PlanMyleave	 Mingle

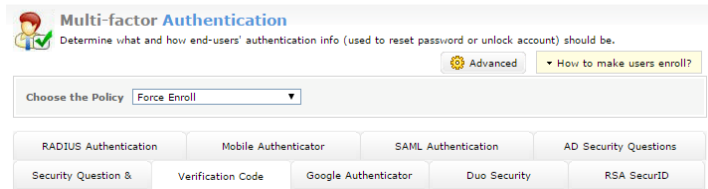
Hybrid AD: SSO

- Use TFA to secure access to some or all apps




Hybrid AD: Single Sign On

- Benefits of ADSelfService Plus
 - One click access to applications through portal
 - Secure access to cloud apps with TFA
 - Use on-prem AD user account as foundation for all access
 - Policy based access control (OUs and groups)
 - Add your custom app through SAML



Multi-factor Authentication

Determine what and how end-users' authentication info (used to reset password or unlock account) should be.

 Advanced ▾ How to make users enroll?

Choose the Policy

RADIUS Authentication	Mobile Authenticator	SAML Authentication	AD Security Questions	
Security Question &	Verification Code	Google Authenticator	Duo Security	RSA SecurID



HYBRID AD: SELF-SERVICE PASSWORD RESET

Hybrid AD: Self-service Password Reset

- Users wonder why they must call the corporate HD to reset password
- Users don't call any other HD to reset password in their world
 - Users are already trained on how to reset their own password
 - You only need to have them enroll in a system
- Self-service password reset options
 - Microsoft AAD
 - Third party solution

Hybrid AD: Self-service Password Reset

- Microsoft provides Azure AD Self-service Password Reset
 - Users must learn how to get to AAD SSPR interface
 - Consider they don't do this often.. How will they remember?

Microsoft

Get back into your account

Who are you?

To recover your account, begin by entering your user ID and the characters in the picture or audio below.

User ID:

Example: user@contoso.onmicrosoft.com or user@contoso.com



🔊

🔊

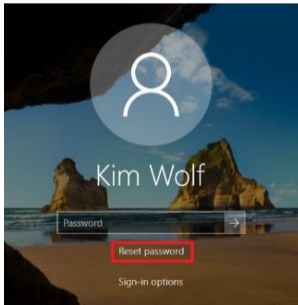
Enter the characters in the picture or the words in the audio.

Next

Cancel

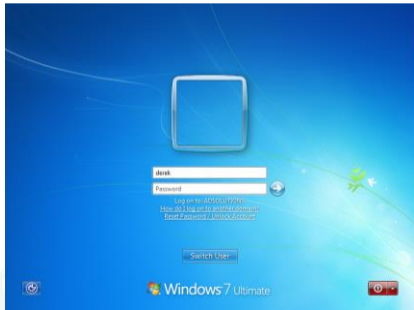
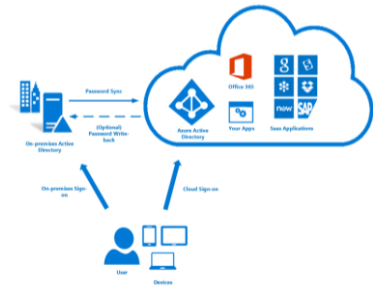
Hybrid AD: Self-service Password Reset

- Microsoft provides “Password Reset” option from GINA



Hybrid AD: Self-service Password Reset

- What if AD is not available?



Hybrid AD: Self-service Password Reset

- Microsoft Self-service password reset limitations

For Hybrid Domain Joined scenarios, the SSPR workflow will successfully complete without needing an Active Directory domain controller. If a user completes the password reset process when communication to an Active Directory domain controller is not available, like when working remotely, the user will not be able to sign in to the device until the device can communicate with a domain controller and update the cached credential. **Connectivity with a domain controller is required to use the new password for the first time.**

Hybrid AD: Self-service Password Reset

- ADSelfService Plus
 - Easy for user – from login **GINA**
 - Reset from **on-prem**
 - Reset from **on the road**
 - Password is **not limited** to AAD password requirements
 - User can **see password requirements** in GUI
 - If user is roaming, **local cache can be updated** with VPN solution



The screenshot shows the ADSelfService Plus interface. At the top, the logo 'ADSelfService Plus' is displayed. Below it is a dialog box titled 'Reset Your Password' with a key icon. The dialog contains the instruction 'Please provide your user name and domain name.' and two input fields: 'Domain User Name' with a text box and '(Example : Jsmith)' to its right, and 'Domain Name' with a dropdown menu showing 'ADSOLUTIONS'. At the bottom of the dialog are 'Continue' and 'Cancel' buttons.

Summary

- What is hybrid?
- History of password management
- Hybrid password management environment
- Hybrid AD: Password Sync
- Hybrid AD: Single Sign On
- Hybrid AD: Self-service password reset

ManageEngine

Thank you!

Derek Melber

derek@manageengine.com

