Convert your hybrid Azure AD joined devices to Azure AD joined devices

Sandy Zeng

Cloudway

Twitter: @sandy_tsang

MVP – Enterprise Mobility

Panu Saukko

ProTrainIT

Twitter: @panusaukko

MVP – Enterprise Mobility

Purpose of the session

- Convert hybrid Azure Active Directory joined (HAADJ) devices to Azure Active Directory joined (AADJ) devices
  - “Remove” AD from the HAADJ devices without re-installing the OS
  - From a customer case

Not supported by Microsoft

Current state and target goal

Current state

- Devices are HAADJ
- Devices are co-managed
  - Pretty common scenario when moving from AD/ConfigMgr → cloud-only environment (AAD/Intune)

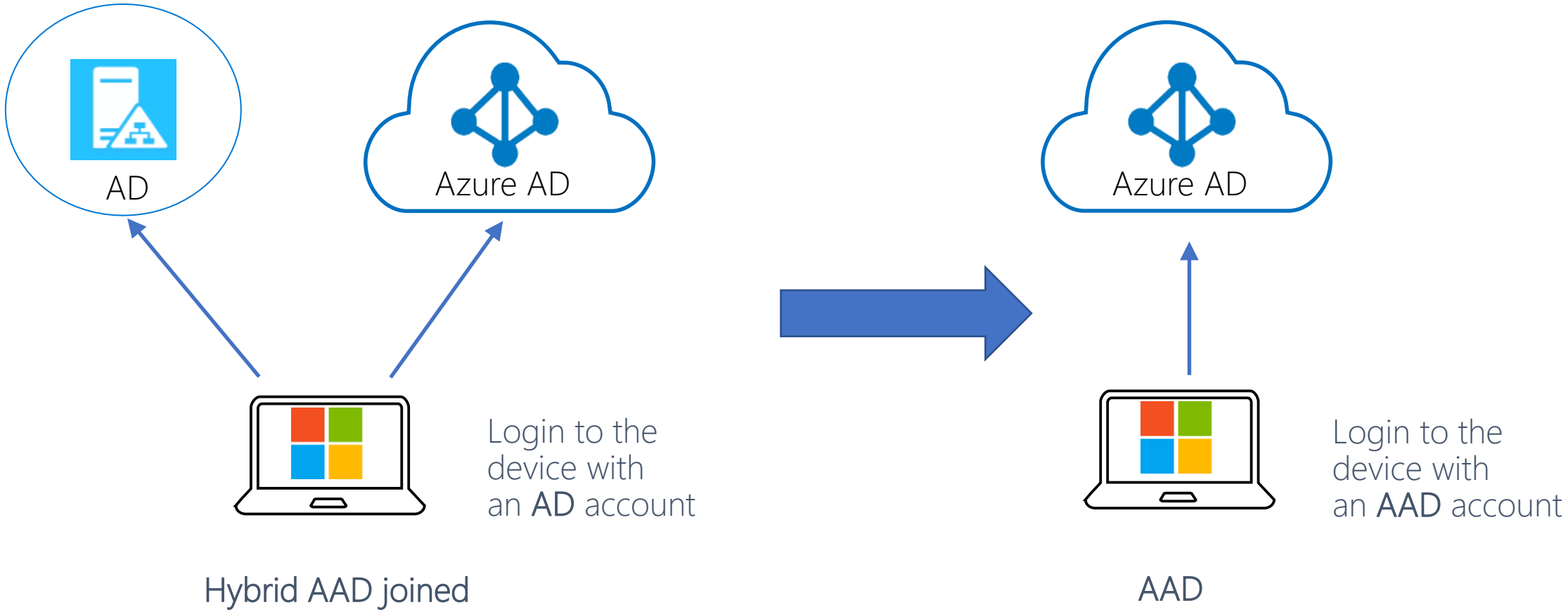
Target goal

- Convert from HAADJ to AADJ without re-installing the OS
- Stay as co-managed. Consider move to Intune only
- Restore primary user after the convert from HAAJ to AADJ

Solution Requirements

- A service account to remove device from AD and exclude the device from syncing back to AAD
- Provisioning package to join the device to AAD
- Azure Function App use Managed Identity, with Microsoft Graph permission
- Use ConfigMgr task sequences.
  - It is easy to create a list of tasks with error control/scheduling/troubleshooting
  - Possible to do without ConfigMgr, but requires more complex scripts
- The device should be in on-prem network

HAADJ vs AADJ



Back to basics - Hybrid Azure AD join

- Azure AD Connect Sync device OU to tenant
- Configure Azure AD connect SCP or use Targeted method with registry
- Azure AD register (dsregcmd.exe /join /debug)
- MDM enrollment
  - GPO. Use registry with user credential
  - Or Co-management. Use auto enrollment with device credential or user credential

How to “Reverse”

Hybrid Azure AD join	Undo Hybrid Azure AD join
1. Azure AD Connect Sync device OU to tenant 2. Configure Azure AD connect SCP or use Targeted method with registry 3. Azure AD register (dsregcmd.exe /join /debug) 4. MDM enrollment • GPO. Use registry with user credential • or Co-management. Use auto enrollment with device credential or user credential	1. Gets device primary user (Azure Function App) 2. Delete from Intune (Azure Function App) • Retire device, remove MDM from device • Unregister Azure AD (same as dsregcmd.exe /leave /debug) 3. Unjoin Active Directory 4. Move device to another un-synced OU

Demo

ConfigMgr Task Sequence

- TS Varibles
  - Set Variable UnjoinAdUserName
  - Set Variable UnjoinAdUserPassword
  - Set VariableTargetOU
  - Set Task Sequence Variable DeprovisionUrl
  - Set Task Sequence Variable Set Primary User
  - Set Task Sequence Variable OSDDoNotLogCommand
- Deprovision
  - Retired from Intune
  - Move OU
  - Unjoin AD
- Copy PPKG
- Restart
  - Add Do No Restart Text
  - Restart Computer
- Provisioning
  - Install PPKG
  - Rest Primary User
  - Remove Last Logon User
  - Save bitlocker key and resume bitlocker
  - Add Preferred Aad Tenant Domain Name
  - Restart Computer

Migration-001-Deprovision

Migration-002-SetPrimaryUser

Azure Function App

- Functions “Migration-001-Deprovision”
  - Get primary user

  GET https://graph.microsoft.com/beta/devicemanagement/manageddevices/{ManagedDeviceID}/Users?$Select=Id,userPrincipalName
  - Delete Intune device

  DELETE https://graph.microsoft.com/beta/deviceManagement/managedDevices/{ManagedDeviceID}

Functions “Migration-002-SetPrimaryUser”

- Set primary user

POST https://graph.microsoft.com/beta/deviceManagement/managedDevices(‘{ManagedDeviceID}')/users/$ref

Body JSON format

{@odata.id: https://graph.microsoft.com/beta/users/{userId}}

Install provision package with PowerShell


```powershell
#Apply provisiong package
$PackageInstall = (Install-ProvisioningPackage -PackagePath "C:\Windows\Temp\AAD Join.ppkg" -ForceInstall -QuietInstall | Select-Object -ExpandProperty Result) | Select-Object -ExpandProperty ProvxmlResults

#Stop auto restart device process
shutdown /a

#Check provisioning install result
if (($PackageInstall.LastResult -eq "Success") -or ($PackageInstall.LastResult -eq $null))
{
    # Write log entry and exit with sucess
    Write-Output "Provisioning complete - Results: $($PackageInstall.LastResult). Result message: $($PackageInstall.Message) "
}
else {
    # Write log entry and exit with failure
    Write-Output "Provisioning failed - Results: $($PackageInstall.LastResult). Result message: $($PackageInstall.Message) "
}
```

Remove Last Logon User


```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI" /v LastLoggedOnDisplayName /f

reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI" /v LastLoggedOnSAMUser /f

reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI" /v LastLoggedOnUser /f

reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI" /v LastLoggedOnUserSID /f

reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI" /v SelectedUserSID /f
```

Preferred AAD Tenant Domain Name

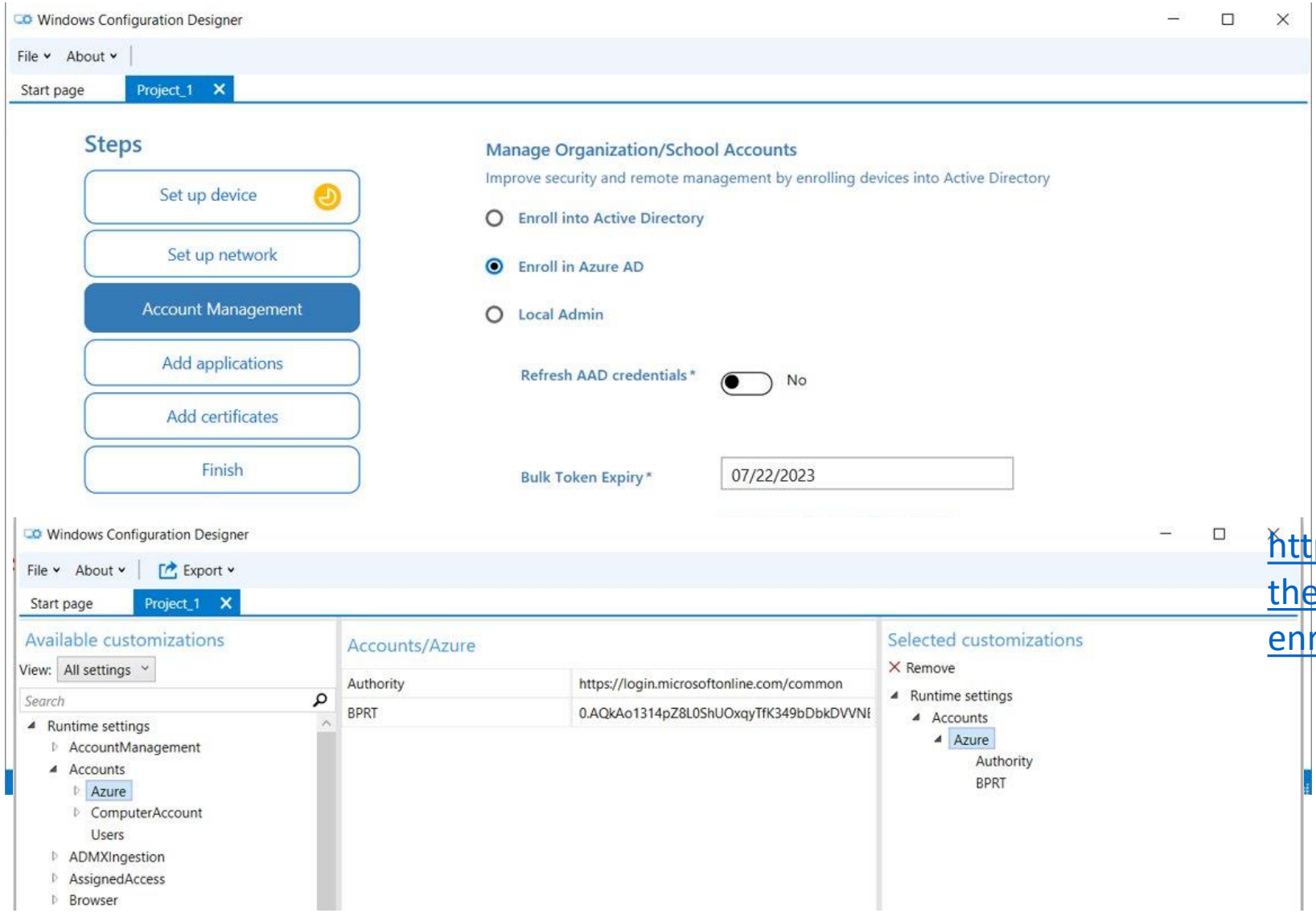
Using MDM WMI Bridge

Need to run as a system account

```powershell
$namespaceName = "root\cimv2\mdm\dmmap"
$className = "MDM_Policy_Config01_Authentication02"

# Create a new instance for MDM_Policy_Config01_Authentication02
try
{
    $obj = Get-CimInstance -Namespace $namespaceName -ClassName $className -Filter "ParentID='./Vendor/MSFT/Policy/Config' and InstanceID='Authentication'"
    if(!$obj) {
        #IMPORTANT: change smsboot.com to your own domain name
        New-CimInstance -Namespace $namespaceName -ClassName $className -Property @{ParentID="./Vendor/MSFT/Policy/Config";InstanceID="Authentication";PreferredAadTenantDomainName='smsboot.com'}
    }
}
catch [Exception]
{
    write-output $_ | out-string
}
```

Provision package



Bulk token expires after 180d

First time needs GA rights

Use DEM account to create a token

https://oofhours.com/2023/02/14/simplify-the-process-of-generating-an-aad-bulk-enrollment-provisioning-package/

Provision packages and Windows 11 22H2?

Provisioning packages might not work as expected

Status	Originating update	History
Resolved KB5020044	N/A	Resolved: 2023-01-06, 16:58 PT Opened: 2022-10-05, 14:17 PT

[Resolved issues in Windows 11, version 22H2 | Microsoft Learn]

Other things to consider

- The user will get a new profile
  - Old profiles still exists on the device
  - Disk space?
- Are using Bitlocker?
  - Need to store Bitlocker keys to AAD
- When the devices is removed from AD → No more GPOs
  - Ensure the needed settings are coming from Intune policies
- Local user group memberships
  - Admin rights?
- Machine based certificates?
  - No more GPO based certificate autoenrollment

Summary

- It is possible to convert HAADJ devices to AADJ without OS reinstallation
  - Not supported by Microsoft!
  - The process works: Tested in real life ☺

Thank You!