Active Directory Intune, Autopilot and BitLocker

Quick Start Guide

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

20 Enterprise Ste 100

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Legend

! **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ℹ **IMPORTANT**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

Active Directory Intune, Autopilot and BitLocker Quick Start Guide
Updated - October 2024

Contents

Introduction

On Demand Migration for Active Directory (ODMAD) supports Microsoft Entra ID Join device migration for devices running Windows 10 or Windows 11 while preserving the User Profiles and File/Folder Security Permissions.

ODMAD successfully migrates these devices to the target Microsoft Entra ID using the default ODMAD settings, including migrating devices that are already Intune-enrolled and devices that were originally provisioned using Autopilot. In addition to migrating the devices to Microsoft Entra ID, a best practice is to also clear previous Autopilot and Intune settings to allow successful Intune enrollment and management in the target.

This step-by-step guide walks through how to perform Intune managed device migration between two Microsoft Entra ID (Cloud Only) tenants.

This guide is a supplementary document to the Active Directory Entra-Join Quick Start Guide.

Topics

This guide covers the following topics:

- Requirements
- Intune/Autopilot Workstation Cutover High-Level Process
- High level Custom Task Explanation
- Implementation Process
- Intune Cutover Run Book

Requirements

General

- Client is licensed for On Demand Migration Active Directory and Directory Sync
- One Global Administrator Account for each Microsoft 365 tenant

  Accounts

  Microsoft Entra ID Application Account
- An account with Global Administrator Role is required to grant permissions and establish connection when adding a Cloud Environment.

  Microsoft Entra ID PowerShell Accounts
- Three (3) PowerShell accounts are automatically created to read and update objects in the cloud. To do this an OAuth token is used from the account used to add the Cloud Environment.
- These PowerShell accounts do not require any Microsoft 365 licenses.

Intune/Autopilot Workstation Cutover High-Level Process

The high-level process no longer requires the modification of the Default Microsoft Entra ID Cutover action in ODMAD. However, if BitLockerBackup is required for the migration, there is an additional task that needs to be added which will be noted below:

- AutoPilot Cleanup – Default Task, removes the Autopilot registry keys from the workstation. This should be done after the workstation has been removed from Enrolled Devices in the source tenant.
- BT-DownloadReACLConfig – Default Task
- BT-ReACLPrepareWin10Profiles – Default Task
- BitlockerBackupToEntraID (Only required if source workstations are BitLocker Enabled) – If the workstation is BitLocker enabled in the source, the Recovery key is not automatically transferred to the target Microsoft Entra ID. This task creates a PowerShell script on the workstation and creates a Scheduled Task that will run the script after the user has logged on post migration. The script will escrow the existing recovery key from workstation and write it to the target Microsoft Entra ID account.
- CleanupLocalAdministratorsGroup (Optional) – If the source user was an Administrator on the machine, the Re-ACL process will put the target user in the Administrators group. This task will remove users from the Local Administrator Group.
- BT-EntraIDCutover – Default Task

High level Custom Task Explanation

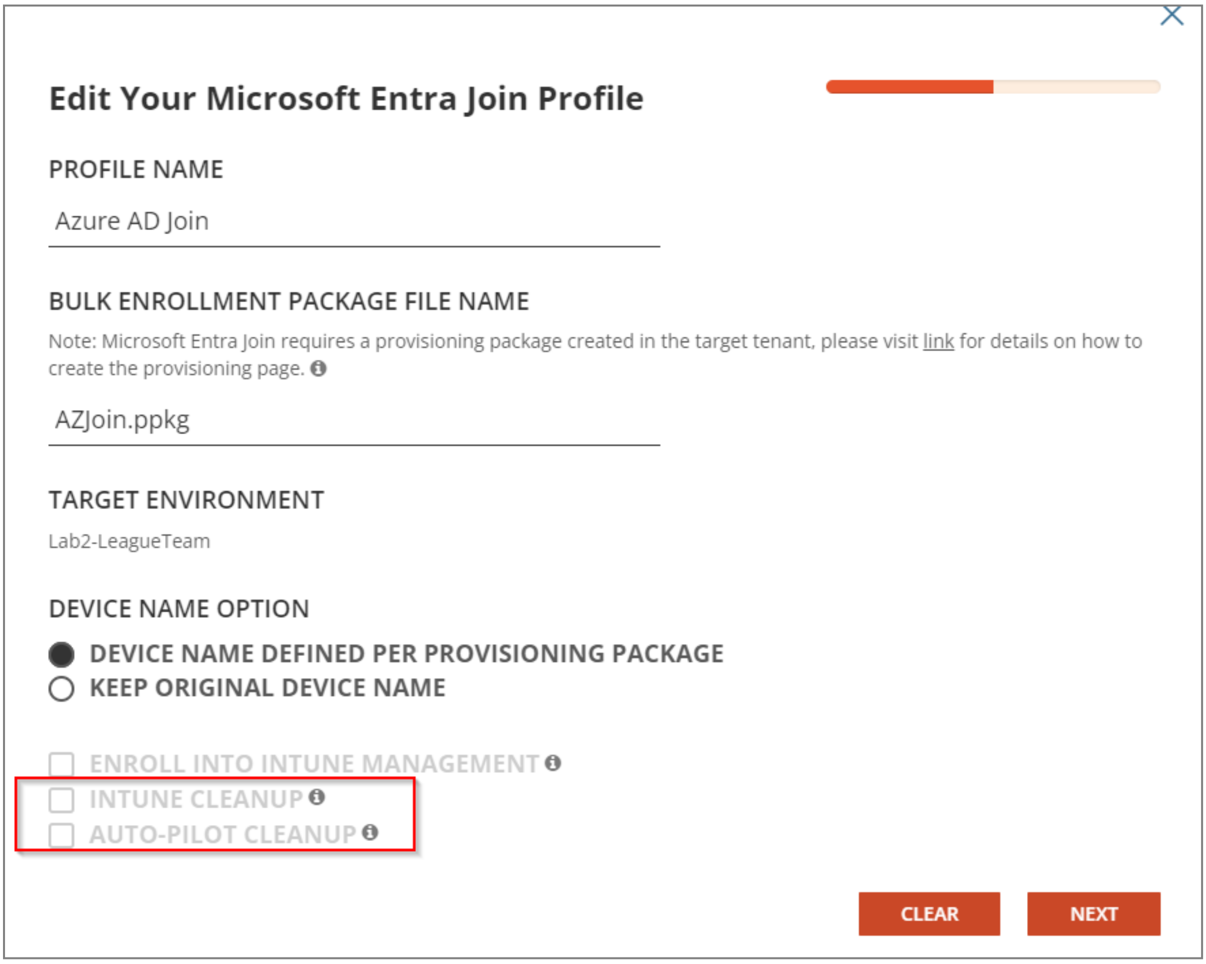
Autopilot Cleanup

This task must be submitted by the migration administrator for the auto-pilot device to remove the autopilot object in Entra ID.

To allow enrolling the workstation into the target Intune, it is important to remove the source Auto-Pilot Enrollment information. Otherwise, the workstation thinks that it is already part of an Intune/Auto-Pilot Enrollment and will not try to enroll in the target. To accomplish this, Auto-Pilot Cleanup option must be selected in the Entra ID Join Profile.

Intune Registry Cleanup

To allow enrolling the workstation into the target Intune, it is important to remove the source Intune Enrollment information. Otherwise, the workstation thinks that it is already part of an Intune Enrollment and will not try to enroll in the target. To accomplish this, Intune Cleanup option must be selected in the Entra ID Join Profile.



Edit Your Microsoft Entra Join Profile

PROFILE NAME

Azure AD Join

BULK ENROLLMENT PACKAGE FILE NAME

Note: Microsoft Entra Join requires a provisioning package created in the target tenant, please visit link for details on how to create the provisioning page.

AZJoin.ppkg

TARGET ENVIRONMENT

Lab2-LeagueTeam

DEVICE NAME OPTION

● DEVICE NAME DEFINED PER PROVISIONING PACKAGE

○ KEEP ORIGINAL DEVICE NAME

□ ENROLL INTO INTUNE MANAGEMENT

□ INTUNE CLEANUP

□ AUTO-PILOT CLEANUP

SetUserEmailValues

When the machine enrolls in the target Intune, it will look for an Intune Licensed user in M365 using the UserEmail value found in the workstation registry. By default, this value is set to the Bulk Enrollment user, which does not have the relevant license, and prevents the Intune service from running correctly.

The product performs this automatically during Entra ID Device Join when the Enroll into Intune Management option is selected in EntraID Device Join Profile. The product will update the UserEmail value in the following registry key, setting it to the UPN of the logged-on target user.

- HKLM:\System\CurrentControlSet\Control\CloudDomainJoin\JoinInfo

BitlockerBackupToEntraID (Optional)

When a machine is BitLocker enabled in the source Environment, the key is stored in the source Microsoft Entra ID. During the Workstation migration process the BitLocker key is not automatically migrated into the target Environment. To ensure that the recovery key is stored in the target tenant, this task will escrow the BitLocker key from the workstation and push into the target tenant post migration.

This script creates a separate PowerShell script on the workstation called BackupBitlockerKeyToADD.ps1 in the ODMAD agent folder and creates a Scheduled Task to execute BackupBitlockerKeyToADD.ps1 when the first target user logs on.

When the BackupBitlockerKeyToADD script runs during the first login post-migration, it will escrow the BitLocker recovery keys from the machine and store them in the Microsoft Entra ID object of the logged-on user and become viewable in the target Intune tenant.

The script will also create a log file in the ODM agent Files folder and then perform cleanup to remove the Scheduled Task and remove the script itself.

BackupBitlockerKeytoAAD.txt

```
Param (
)

$output = New-Object BinaryTree.ADM.Agent.PSHelpers.PSOutput


$ScriptName = "BackupBitlockerKeyToADD.ps1"

$BacktoAAD = @"

Try{
   `$ODMADService = Get-Service -Name ODMActiveDirectory
   }
Catch{
     Write-Output "Error Retrieving Service Status...Terminating with error:
`$(`$Error)"
     Exit 1
     }
If(`$ODMADService){
    Write-Output "ODM AD Agent Service Found...Finding ODM AD Agent Service Path"
    `$ODMADServicePath = (Get-ItemProperty -Path
HKLM:SYSTEM\CurrentControlSet\Services\ODMActiveDirectory).ImagePath
    `$ODMAgentPath = Split-Path `$ODMADServicePath
    `$ODMAgentPath = `$ODMAgentPath.Trim("``"")
    Write-Output "ODM AD Service Path: `$(`$ODMAgentPath)"
}
Else{
    Write-Output "No ODM Agent Service Found...Terminating"
    Exit 1
    }

`$TranscriptFile = "`$(`$ODMAgentPath)\Files\PowerShell-`$(Get-Date -f yyyyMMdd-HHMM)-
BackupBitlockerKeyToAAD.log"
Start-Transcript -Path `$TranscriptFile

`$DriveLetter = `$env:SystemDrive

#endregion declarations

#region functions

function Test-Bitlocker (`$BitlockerDrive) {
    #Tests the drive for existing Bitlocker keyprotectors
```

BackupBitlockerKeytoAAD.txt

```
    try {
        Get-BitLockerVolume -MountPoint `$BitlockerDrive -ErrorAction Stop
    } catch {
        Write-Output "Bitlocker was not found protecting the `$BitlockerDrive drive.
Terminating script!"
        exit 0
    }
}

function Get-KeyProtectorId (`$BitlockerDrive) {
    #fetches the key protector ID of the drive
    `$BitLockerVolume = Get-BitLockerVolume -MountPoint `$BitlockerDrive
    `$KeyProtector = `$BitLockerVolume.KeyProtector | Where-Object {
`$_.KeyProtectorType -eq 'RecoveryPassword' }
    return `$KeyProtector.KeyProtectorId
}

function Invoke-BitlockerEscrow (`$BitlockerDrive,`$BitlockerKey) {
    #Escrow the key into Azure AD
    try {
        BackupToAAD-BitLockerKeyProtector -MountPoint `$BitlockerDrive -KeyProtectorId
`$BitlockerKey -ErrorAction SilentlyContinue
        Write-Output "Attempted to escrow key in Azure AD - Please verify manually!"
        exit 0
    } catch {
        Write-Error "Error Occurred"
        exit 1
    }
}

#endregion functions

#region execute

Test-Bitlocker -BitlockerDrive `$DriveLetter
`$KeyProtectorId = Get-KeyProtectorId -BitlockerDrive `$DriveLetter
Invoke-BitlockerEscrow -BitlockerDrive `$DriveLetter -BitlockerKey `$KeyProtectorId

#endregion execute


Remove-Item -path "`$ODMAgentPath\$($ScriptName)" -Force

Unregister-ScheduledTask -TaskName "$($TaskName)" -Confirm:`$false

Stop-Transcript

"@

#$output = New-Object BinaryTree.ADM.Agent.PSHelpers.PSOutput

### Get ODMAD Agent Information to determine path
```

BackupBitlockerKeytoAAD.txt

```
Try{
   $ODMADService = Get-Service -Name ODMActiveDirectory -ErrorAction SilentlyContinue
   }
Catch{
    Write-Output "Error Retrieving Service Status...Terminating with error: $($Error)"
    Exit 1
    }
If($ODMADService){
    Write-Output "ODM AD Agent Service Found...Finding ODM AD Agent Service Path"
    $ODMADServicePath = (Get-ItemProperty -Path
HKLM:SYSTEM\CurrentControlSet\Services\ODMActiveDirectory).ImagePath
    $ODMAgentPath = Split-Path $ODMADServicePath
    $ODMAgentPath = $ODMAgentPath.Trim("`"")
    Write-Output "ODM AD Service Path: $($ODMAgentPath)"
}
Else{
    Write-Output "No ODM Agent Service Found...Terminating"
    Exit 1
    }

$AgentPath = "$ODMAgentPath\"
$ScriptFullName = $AgentPath+$ScriptName
If(!(Test-Path $ScriptFullName)) {
    New-item -path $ODMAgentPath -Name $ScriptName -Type "File" -Value $BacktoAAD
}

# Create Scheduled Task
$TaskName = "Backup Bitlocker Key"
$Argument = "-ExecutionPolicy Bypass -File `"$($ODMAgentPath)\$($ScriptName)`""
$Action = New-ScheduledTaskAction -Execute "PowerShell.exe" -Argument $Argument
$Settings = New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries
$Principal = New-ScheduledTaskPrincipal -UserId "LOCALSERVICE" -LogonType
ServiceAccount
$Trigger = New-ScheduledTaskTrigger -Atlogon
$Trigger.Delay = "PT20M"
$ScheduledTask = New-ScheduledTask -Action $Action -Trigger $Trigger -Settings
$Settings
# Register Scheduled Task
Register-ScheduledTask -TaskName $TaskName -InputObject $ScheduledTask -User "NT
AUTHORITY\SYSTEM" -Force

return ($output)
```

SetPrimaryUser (Optional)

The Primary User value is automatically set in the target Microsoft Entra ID when performing a Microsoft Entra ID join. The product also provides the ability to set this value again via a default system action “Set Intune Primary User”. The default system action will set the last logon target user as the device Primary Intune User.

Implementation Process

Refer to the below steps to configure the Optional BitlockerBackupToEntraID task to the custom EntraID Cutover action we are about to create.

1. Copy the Default EntraIDCutover Action

1. In ODMAD using Select CONFIGURATIONS from the main ODMAD Menu.
2. Select ACTIONS.
3. In the ACTIONS section select click SHOW SYSTEM.
4. Find the EntraIDCutoverAction and select it.
5. Click COPY, which will open the Edit a Custom Action dialog window. Configure the action as follows:
    a. ACTION NAME: IntuneMicrosoftEntraIDCutover
    b. ACTION DISPLAY NAME: Intune Microsoft Entra ID Cutover
    c. DESCRIPTION: Process to join an Intune/Autopilot workstation to an Microsoft Entra ID
    d. ACTION TARGET: Computer
    e. ACTION TYPE: Microsoft Entra ID Cutover
6. Click the SAVE button to continue.

2. Add BitlockerBackupToEntraID Task (Optional: Only required if source workstations are Bitlockered)

1. Scroll down to the TASKS section of the Action window and click NEW.
2. The ADD A Custom Task window will appear. Configure this as follows:
    a. TASK NAME: BitlockerBackupToEntraID
    b. DESCRIPTION: Backups the Bitlocker key from the Workstation to Entra ID user that logged on to the workstation
    c. TASK TYPE: PowerShell Script
3. Click NEXT to Continue.
4. Copy the BackupBitlockerToAAD Script into the SCRIPT Section.
   Note: There is no need to click the LOAD SCRIPT FRAMWORK button as this is included in the PS1 file.
   BackupBitlockerKeytoAAD.txt
5. Leave all other settings as default and click the SAVE button.

6. Select the Task just created and select the IntuneMicrosoftEntraIDCutover Action that was created earlier. Click the ADD TO button to add this task to the action.

7. Scroll up the ACTIONS section and expand the IntuneMicrosoftEntraIDCutover Action. The task just added will appear as the last step of the action, click+hold on the task and drag to correct position in the script (after the SetUserEmailValues task, but before the BT-EntraIDCutover task). The change will be saved automatically.

3. Add CleanupLocalAdministratorsGroup Task (Optional)

1. Scroll down to the TASKS section of the Action window and click NEW.

2. The ADD A Custom Task window will appear. Configure this as follows:

   a. TASK NAME: CleanupLocalAdministratorsGroup

   b. DESCRIPTION: Removes Microsoft Entra ID Domain users from the local Administrators group before cutover.

   c. TASK TYPE: PowerShell Script

3. Click NEXT to Continue.

4. Copy the CleanupLocalAdministratorsGroup Script into the SCRIPT Section.

   Note: There is no need to click the LOAD SCRIPT FRAMWORK button as this is included in the PS1 file.

   CleanUp Local Administrators Group.txt

5. Leave all other settings as default and click the SAVE button.

6. Select the Task just created and select the IntuneMicrosoftEntraIDCutover Action that was created earlier. Click the ADD TO button to add this task to the action.

7. Scroll up the ACTIONS section and expand the IntuneMicrosoftEntraIDCutover Action. The task just added will appear as the last step of the action, click+hold on the task and drag to correct position in the script (after the SetUserEmailValues task, but before the BT-EntraIDCutover task). The change will be saved automatically.

Intune Cutover Run Book

This runbook assumes that the computer had been read in to On Demand and the workstation has the agent installed, configured, and registered.

1. Run Re-ACL Process

1. In On Demand, navigate to Devices and Servers.

2. Select the Device and from the drop-down menu select Re-ACL.

3. Select the Re-ACL profile and follow the on-screen prompts.

2. Run Cutover Process

2a. Remove Workstation from Source Autopilot

The Autopilot Clean action must be completed and On Demand Migration Active Directory will automatically remove the serial number from the source tenant.

1. In On Demand, navigate to Devices and Servers.
2. Select the Device(s) to be cutover and from the drop-down menu select “Autopilot Cleanup”.
3. Once the job is completed, move to the next step.

2b. Cutover the Device using ODMAD

1. In On Demand, navigate to Devices and Servers.
2. Select the Device(s) to be cutover and from the drop-down menu select Intune Microsoft Entra ID Cutover.
3. Select the Microsoft Entra ID Cutover Profile and follow the on-screen prompts.

About us

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product