

On Demand Migration Active Directory Entra-Join

## **Quick Start Guide**



© 2025 Quest Software Inc.

**ALL RIGHTS RESERVED.**

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

Quest Software Inc.

Attn: LEGAL Dept

20 Enterprise, Suite 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**

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are property of their respective owners.

**Legend**

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

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

# Contents

<b>Introduction</b> .....	<b>4</b>
Topics .....	4
Requirements .....	4
Environment Preparation .....	6
Provisioning Package Preparation .....	6
<b>Device Migration</b> .....	<b>10</b>
On Demand Migration Directory Sync .....	10
Setting up the Directory Sync Local Environment .....	10
Setting up the Directory Sync Cloud Environment .....	12
Configure Directory Sync Template.....	13
Configure Directory Sync Workflow .....	14
Running Directory Sync Workflow and validating the sync results .....	15
On Demand Migration Active Directory Project .....	16
Install the local agent on the workstation .....	16
Setup the Microsoft Entra Bulk Enrollment Repository and Microsoft Entra ID Join Migration Profile.....	18
Perform Device Migration.....	21
Validate Device Post Microsoft Entra ID Join .....	24
<b>Frequently Asked Questions</b> .....	<b>27</b>
Can I use configure Wi-Fi access point for my devices to use post Microsoft Entra ID Join?..	27
I cannot connect to my devices via Remote Desktop Service post Microsoft Entra ID Join. ..	28
What is the Microsoft Entra ID NetBIOS name for my Microsoft Entra ID Users? .....	28
Can I provision a local administrator for my devices during Microsoft Entra ID Join process?	28
Can I provision additional applications and adding a certificate for my devices during Microsoft Entra ID Join process?.....	29
My device is Microsoft Entra ID Joined, it is prompting me to setup MFA and Windows Hello, is this normal? .....	29
After my user devices are Microsoft Entra ID Joined to the target tenant, how can users switch their Microsoft Apps such as OneDrive, Teams, and Outlook to start using target tenant account?.....	29
Is there a way that I can use On Demand Migration Active Directory to migrate my devices if they are Microsoft Entra ID Join only in the source? .....	30
Can I migrate to and from GCC/GCCH tenants?.....	30
After Cutover, why is the Windows screen flickering or displaying a black screen on some devices? .....	31
<b>About us</b> .....	<b>33</b>

# Introduction

On Demand Migration Active Directory supports device migrations to Microsoft Entra ID from Domain Joined, Hybrid Domain Joined, and Entra Joined workstations running Windows 10 or Windows 11 while preserving the User Profiles and File/Folder Security Permissions.

This step-by-step guide walks you through how to configure a Project to perform device migration to Microsoft Entra ID using [On Demand Migration for Active Directory](#). For device migrations using other On Demand products, please see the guide for your product: [On Demand Migration Active Directory Express](#) or [On Demand Migration Entra ID for Devices](#).

## Topics

This guide covers the following topics:

- Microsoft Entra ID Device Join Requirements
- Environment preparation
- Prepare the Provisioning Package
- Configure and synchronize your objects between source On-Premises Active Directory and target Microsoft Entra Tenant
- Configure Device Migration Project
- Perform Device Microsoft Entra ID Join migration
- Validate the device post Microsoft Entra ID Join
- Frequently Asked Questions

## Requirements

### General

- Client is licensed for On Demand Migration Active Directory and Directory Sync
- Client is licensed for On Demand Migration Azure Device Migration Add-on
- One Global Administrator Account for each Microsoft 365 tenant
- One Domain Administrator Account for each On-Premises Active Directory attached to the tenant
- One dedicated server to install the Directory Sync agent
- Permissions to download and install Directory Sync agent



**Important Tip:** Local Account and dedicated server are only needed if the environment is an On-Premises Active Directory or in a Hybrid Tenant setup.

## Hardware

The local agent must meet the following minimum hardware requirements:

- At least one (1) Windows Server 2012 R2, 2016 or 2019
- Additional Windows servers may be deployed; limit of 5.
- CPU: 4 Cores
- Memory: 4GB Free
- Disk: 40GB Free Disk Space excluding Operating System



**Important Tip:** Do not install local agents on AD domain controllers in a production environment.

## Software

The local agent must meet the following minimum software requirements:

- Windows Server 2012 R2, 2016 or 2019
- .NET 4.7.2. NOTE: .NET will automatically be installed if needed.
- TLS 1.2 or higher

## Domain and Forest Functional Levels

All AD Functional Levels supported by Microsoft for a Microsoft Windows Server operating system listed below are supported for migration from/to Domain controllers running on that same Operating System. For example, Windows Server 2016 functional levels are supported on Windows Server 2022, Windows Server 2019, and Windows Server 2016. For full details see Microsoft's documentation of Active Directory Domain Services Functional Levels in Windows Server on Microsoft Learn.

- NOTE: Windows Server 2003 functional levels are supported only on Windows Server 2016, Windows Server 2012 R2, and Windows Server 2012. That is, Microsoft does not support Windows Server 2003 functional levels on Windows Server 2019 or Windows Server 2022.
- NOTE: Microsoft's lifecycle for Windows Server 2012 ends extended support on October 10, 2023. Customers should be planning to move their Domain Controllers off of Windows Server 2012 and Windows Server 2012 R2 by that date.

## Network

- Directory Sync web interface uses TCP port 443 (HTTPS).
- Agent web connections use port 443 to Directory Sync host application.
- DCs use TCP ports 139, 389 (UDP), 445, and 3268.
- SID History functionality uses TCP ports 135, 137-139, 389 (UDP), 445, 1027, 3268, and 49152-65535. (Optional)

## Accounts

Local Active Directory Account (Optional, required for Hybrid Tenant)

- Agent installer will prompt for a domain account with permission to read and write on-premises Active Directory.
- An agent intended to sync all domains in a forest must have rights to all domains and objects used in workflows.

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.

## Environment Preparation

This section will review the environment setup that will be used to perform Microsoft Entra ID Device Join. To facilitate the migration, please confirm you have the following:

- A source environment that is either on premise Active Directory or a Hybrid Microsoft Entra tenant including a local on-premises Active Directory with Microsoft Entra Connect configured.
- A source environment that is Microsoft Entra ID only tenant.
- A target environment that is either an Microsoft Entra ID Only tenant or is a Hybrid Microsoft Entra tenant including a local on-premises Active Directory with Microsoft Entra Connect configured.
- A file share that is accessible by the workstation, the file share will be used to store the provisioning package which is needed to perform the Microsoft Entra ID Join. Later in this guide, we will review how to create the provisioning package using Windows Configuration Designer (WCD).
- A Windows Workstation running Windows 10 (Build 1709 or later), or Windows 11.

*Device Microsoft Entra ID Join status*

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant	Registered	Activity
Lab1-W10AZ	Yes	Windows	10.0.19044.1889	Hybrid Azure AD joined	N/A	None	N/A	8/26/2022, 7:40 PM	N/A

*Microsoft Entra ID Portal Device View*



**Important Tip:** For additional detail on how to configure an Hybrid Microsoft Entra ID Join device, please refer to this Microsoft Article at [Configure Microsoft Entra hybrid join - Microsoft Entra | Microsoft Docs](#)

## Provisioning Package Preparation

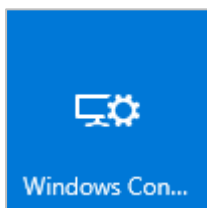
This section will explain how to create a provisioning package for Windows Workstation running Windows 10 (Build 1709 or later), or Windows 11 using Windows Configuration Designer. Additional detailed instructions can also be found at this Microsoft Article [Bulk enrollment for Windows devices - Microsoft Intune | Microsoft Docs](#).

1. Download the Windows Configuration Designer (WCD) from the Microsoft Store.

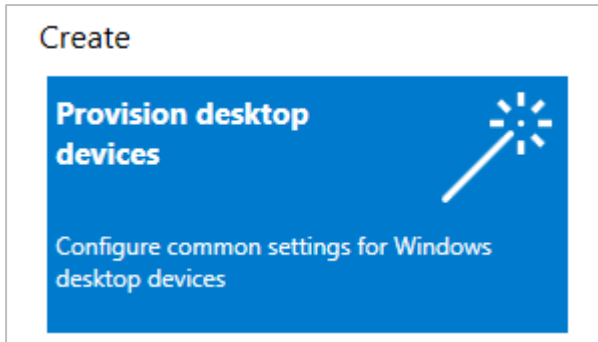


**Important Tip:** Windows Configuration Designer(WCD) should be downloaded and installed on the workstation used by the migration administrator to prepare the enrollment package. It does not need to be installed on the workstations that are being migrated.

2. Launch the Windows Configuration Designer by clicking on the icon on the start menu.



3. Create a new package by clicking on the Provision desktop devices icon.



4. Provide a project name and click *Finish*.

A "New project" dialog box titled "Enter project details". It has a close button (X) in the top right corner. The "Name:" field contains "Microsoft Entra ID Device Join QS Guide". The "Project folder:" field contains "C:\Users\LYu02\OneDrive - Quest\Documents\Windows Imaging and Configuration Designer (W" and a "Browse..." button. The "Description:" field is empty. A "Finish" button is at the bottom right.

5. Specify a computer name using the on-screen instructions. Leave all other settings with default. Click *Next*.

A "Steps" configuration screen with a sidebar on the left containing buttons for "Set up device", "Set up network", "Account Management", "Add applications", "Add certificates", and "Finish". The main area is titled "Device name" and contains instructions: "Enter a unique value with maximum 63-character length to use for the DNS computer name of the device. For help generating a unique name, you can use %RAND%x% to generate x number of random digits in the name. x must be a number less than 63. You can use %SERIAL% to generate the name with the computer's serial number embedded, if the serial number exceeds the character limit, it will be truncated from the beginning of the serial name sequence." Below this, there are example values: "Contoso-%SERIAL%", "Fabrikam-%RAND%5%", and "A2JoinQSGuide%Rand3%", with the last one highlighted by a red box. A note states: "This setting is only supported in Windows 10 version 2004 and later releases. To change the computer name on earlier releases use the ComputerName setting under Accounts -> ComputerAccount in the Advanced View." Below that is the "Enter product key" section with a text input field. The "Configure devices for shared use" section has a toggle switch set to "No", highlighted by a red box. The "Remove pre-installed software" section also has a toggle switch set to "No", highlighted by a red box. At the bottom, there are links for "Link to advanced editor", "Learn more", and "Next".

6. Disable the Wi-Fi setting if devices will have a wired network connection, or you may enter a Wi-Fi SSID in your environment, Click *Next*.

**Set up network**  
 Connect devices to a Wi-Fi network

Off

Make sure you have a wired network (Ethernet) connected to your device

7. Perform the following in Account Management section, click *Next* when completed:
  - Select “Enroll in Azure AD” option.
  - Click on the “Get Bulk Token” link to generate a token that will be used for device join. You will be prompted by Microsoft 365 to enter your tenant credential.



**Important Tip:** Your account must have a specific Azure AD (Microsoft Entra ID) role assignment to create a bulk enrollment token. Reference the Microsoft documentation for details on which roles have access and how to assign them [Bulk enrollment for Windows devices - Microsoft Intune | Microsoft Docs](#).

- Optionally you can also specify a local administrator account and password. This account will be created on the device.

**Manage Organization/School Accounts**  
 Improve security and remote management by enrolling devices into Active Directory

Enroll into Active Directory

Enroll in Azure AD

Local Admin

Bulk Token Expiry\*

Bulk AAD Token\* Bulk Token Fetched Successfully

Optional: Create a local administrator account

User name

Password



**Important Tip:** If you do not have any local administrator account configured on the device, it is recommended that you create this optional local administrator account as your source Active Directory Admin account will not work after device migration.

8. Leave the default setting for Add Application section and click *Next*.
9. Leave the default setting for Add certificates section and click *Next*.
10. Review the package setting and click *Create*.



### Steps

- Set up device
✔
- Set up network
✔
- Account Management
✔
- Add applications
✔
- Add certificates
✔
- Finish

### Summary

**Set up device**

Share devices: No

Remove pre-installed software: No

Enter device name: AzJoinQSGuide%Rand:3%

**Network settings**

Network: Wired

**Account Management**

Bulk Token Expiry Date: "2023-02-23T00:27:24.023Z"

Local admin user name: QSGuide

Local admin user password: \*\*\*\*\*

**Add applications**

**Add certificates**

**Protect your package**

Protect the contents of your package by specifying a password. The password length must be 8-16 characters.

No

You are ready to create the package!

Create

11. Store the package file in a Shared Folder which is accessible by the Workstation for later use. (The Share Folder UNC path will need to be defined later in On Demand Migration Active Directory)

# Device Migration

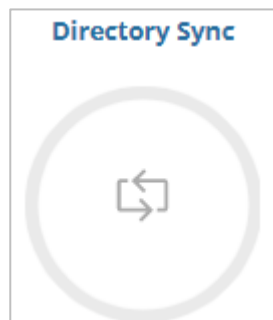
## On Demand Migration Directory Sync

This section explains how to setup Directory Sync between Local On-Premises Active Directory and an Microsoft Entra tenant using On Demand Migration Directory Sync. During project setup, an Office 365 Global Administrator account is initially required to add Microsoft Entra tenant to the project.

### Setting up the Directory Sync Local Environment

Follow these steps to setup the Directory Sync Environments.

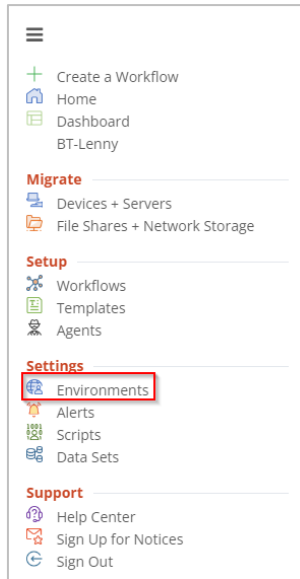
1. Log in to [On Demand](#).
2. Navigate to *Migration*.
3. Select an existing migration project.
4. Click on Directory Sync from the Project Dashboard.



5. Once the On Demand Migration Directory Sync module is loaded, click on the Directory Sync icon in the main dash view.



6. Click *Environments* in the left navigation menu to display the environment page.



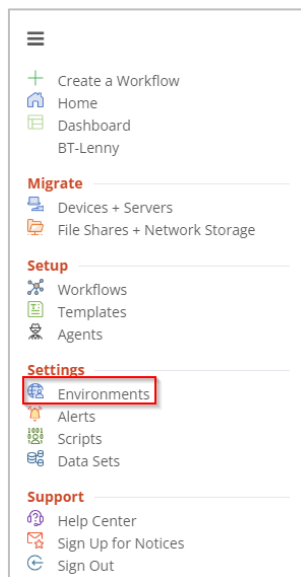
7. Click the *New* button.
8. Click *Local* as the environment type, Click *Next*.
9. Name the environment, Click *Next*.
10. Name the local agent, Click *Next*.
11. Note the agent registration URL and registration Key for later use, click *Finish*.
12. Install the agent in the Windows Server that is joined to the local AD domain.
  - a. Launch the On Demand Migration Directory Sync Agent installation in the target workstation or server.
  - b. Accept the license agreement and click on *next*.
  - c. Enter the target active directory environment information by providing the following and click *next*.
    - Domain Name
    - Global Catalog Server
    - Username
    - Password
  - d. Enter the On Demand Migration Directory Sync Registration URL and Agent Registration Key information and click *next*.
  - e. In the *siDHistory* Migration section, you may skip this step as *siDHistory* is not in-scope for this project.

*Note, Refer to On Demand Migration Active Directory Online Help Center for detailed information about agent installation and set-up requirements.*

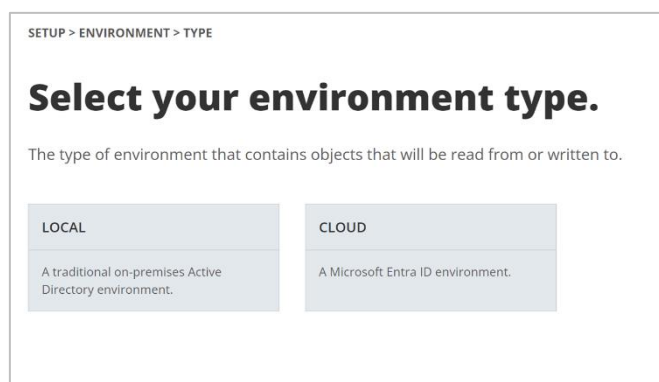
13. Once the agent is installed and the environment is discovered, click on the *Setting* button to access the local AD environment setting page.
14. Click on the *Organization Unit* tab and define the OU filter based on your project scope. In this case, we should include the following:
  - a. Users and Groups objects in-scope of the migration
  - b. Devices in-scope of the migration
15. Click on the *Filters* tab and define any LDAP filter based on your project scope.
16. Click *Save*.

# Setting up the Directory Sync Cloud Environment

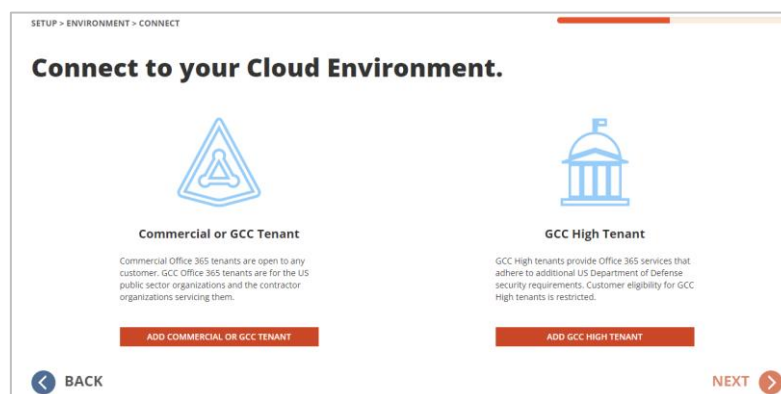
1. Click *Environments* in the left navigation menu to display the environment page.



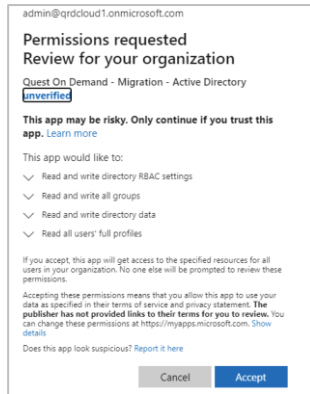
2. Click *New* to open the environment wizard.
3. Select *Cloud* and click *Next*.



4. Type the name of the cloud environment and click *Next*.
5. Click on *Add Commercial or GCC tenant*.



6. Enter the tenant Admin Credential and accept the consents.



7. Click *Next*.
8. Configure the cloud environment filter group and click *Next*.
9. Select the “Include Objects Synchronized with a Local Active Directory via Microsoft Entra Connect” option if you wish to include Hybrid Objects. For the purpose of this guide, we will leave this option unchecked and click *Next*.
10. Review the environment summary and click *Finish*.

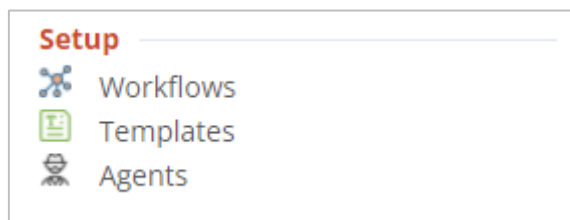


**Important Tip:** When migrating devices between two Microsoft Entra tenants without Local On-Premise Active Directory, please add both source and target tenant as Cloud environments.

## Configure Directory Sync Template

This section provides a step-by-step guide on how to configure the Directory Sync Template.

1. Log in to *On Demand*.
2. Navigate to *Migration*, select the project, and click on *Directory Sync*.
3. Click the *Directory Sync* icon.
4. Click the *Templates* link via the hamburger menu.



5. Click *New* and bring up the Template Wizard.
6. Enter the name and description for the template and click *Next*.
7. Select Local for source environment type and click *Next*.
8. Select Cloud for target environment type and click *Next*.
9. Configure the Users Synchronization options and click *Next*. For the purpose of this guide, use the default options.
10. Configure the Groups Synchronization options and click *Next*. For the purpose of this guide, use the default options.
11. Configure the Contact Synchronization options, click *Next*. For the purpose of this guide, use the default options.
12. Specify the default user password and click *Next*.
13. Configure the Attribute mappings, click *Next*. For the purpose of this guide, use the default options.

14. Review the template summary and click *Finish*.



**Important Tip:** If you do not wish to create objects in your target environment, please choose “Skip” or “Do Not Create” option for each object type.

## Configure Directory Sync Workflow

This section provides a step-by-step guide on how to deploy and configure the Directory Sync Workflow.

1. Log in to [On Demand](#).
2. Navigate to *Migration*, select the project, and click on *Directory Sync*.
3. Click on the *Directory Sync* icon.
4. Click on *New* under *Workflow* and bring up the workflow wizard.
5. Enter the workflow name and click *Next*.
6. Select the environments and click *Next*, for the purpose of this guide, please select the Local and Cloud environments added in the above step.
7. Select *One Way Sync* and click *Next*.
8. The workflow wizard will have four(4) workflow tasks pre-selected, they are Read, Match, Stage and Write. We will need to configure all 4 tasks.
  - a. Read – Select the environments from which you wish to read the objects.
  - b. Match – This is the step where you will decide how to match existing objects across your Microsoft Entra ID directories. Matching is conducted by pairing sets of attributes to find corresponding objects. Your two (2) environments may already have some attributes that can be used to find similar objects between the different directories, or you may need to populate some to ensure accurate matching. For a successful Directory Synchronization, it is most important that existing objects are correctly matched.

For the purpose of this guide, DisplayName and Name will be used for matching.

**2. Match Objects**

Configure your matching criteria by selecting up to five attributes below. ⓘ

LAB1-LOCAL ↔ DEMO3

<b>SOURCE ENVIRONMENT</b> Lab1-Local	↔	<b>TARGET ENVIRONMENT</b> Demo3
<b>SOURCE ATTRIBUTES</b> name displayName	↔	<b>TARGET ATTRIBUTES</b> Name DisplayName

MATCH ACROSS ALL OBJECT TYPES  
Objects are matched even if they are of different object types such as users and contacts.

ADD ANOTHER PAIR

OK CANCEL

- c. Stage – Configure how objects are synced using the sync template. The Stage data step is required and if you do not wish to create any objects in the target environment, you may modify the template option and select “Skip” or “Do Not Create” for each object type.
  - i. Select the Sync Template, click *Next*.
  - ii. Select the source environment, click *Next*.
  - iii. Select the target environment, click *Next*.
  - iv. Choose the target domain name, click *Next*.
  - v. Select the Source Organizational Units, for the purpose of this guide, select the OUs you have defined in the Local Environment which contains your in-scope Users, Groups and Devices. Click *Next*.

- vi. Configure any Stage Data filters by double-clicking the OUs. It is highly recommended to setup a filter to limit the scope when performing a test on the first sync as part of the validation. click *Next*.
  - vii. Review the stage data summary and click *Finish*.
  - d. Write – Specify the environment you want the changes to be applied to and click *Next*. This task can be removed from the workflow if you do not need to create any objects in the target environment.
9. Configure the Sync Interval. For the purpose of this guide, select *Manually* and click *Next*.
  10. Configure the Sync Alert. For the purpose of this guide, we do not want to setup any alerts. Click *Skip*.
  11. Review the workflow summary and click *Finish*.

## Running Directory Sync Workflow and validating the sync results

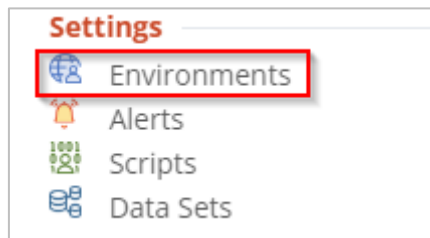
This section provides a step-by-step guide on how to synchronize the objects between source and target environment using the workflow created in this guide.

1. Log in to *On Demand*.
2. Navigate to *Migration*, select the project, and click on *Directory Sync*.
3. Click on the *Directory Sync* icon.
4. Select the workflow created and click *Run* button.
5. Allow the workflow run to complete.
6. Select the workflow created and click *Run* button again.



**Important Tip:** This step is needed to ensure all the objects created in the target tenant will be matched to the source objects.

7. Click the *Environments* link via the hamburger menu.



8. Select the Local On-Premises AD environment and click on *Details*.

Name	Type	Workflows	Agents	Discovery	Last Discovery	Next Discovery	Last Reconcile
Demo3	Cloud	5	OK	Discovered	08/29/2022 3:36 PM		
Demo2	Cloud	5	OK	Discovered	08/29/2022 3:35 PM		
Demo1	Cloud	1	OK	Discovered	08/29/2022 9:43 AM		08/29/2022 10:35 AM
Lab1-Local	Local	3	OK	Discovered	08/26/2022 5:02 PM		08/29/2022 10:18 AM
Lab2-Local	Local	4	OK	Discovered	07/11/2022 10:01 AM		07/21/2022 5:51 PM
Demo3	Cloud	0	OK	Discovered	08/29/2022 9:43 AM		
Demo2	Cloud	0	OK	Discovered	08/29/2022 9:43 AM		

NEW
PASSWORD LOGS
DISCOVERY LOGS
DISCOVER
DETAILS
SETTINGS
DELETE

9. Confirm source devices are discovered, users and groups have matching objects in the target environment.

ID	Name	Email	Distinguished Name Source	Distinguished Name Target	Match Status	Deleted
5a0248d2-256e-415e-af40-57d02cb13c1b	Lab1ODMAD1		CN=Lab1ODMAD1,OU=Lab1ODMAZObjects,...	CN=Lab1ODMAD1,OU=M365x16494329.on...	Matched	No
cc3898eb-64cc-49fb-93ca-5b58c8e7a04c	Lab1ODMAD2		CN=Lab1ODMAD2,OU=Lab1ODMAZObjects,...	CN=Lab1ODMAD2,OU=M365x16494329.on...	Matched	No
4b2f0dc7-8944-44ae-bee3-afd27aedbb1b	Lab1ODMAD3		CN=Lab1ODMAD3,OU=Lab1ODMAZObjects,...	CN=Lab1ODMAD3,OU=M365x16494329.on...	Matched	No

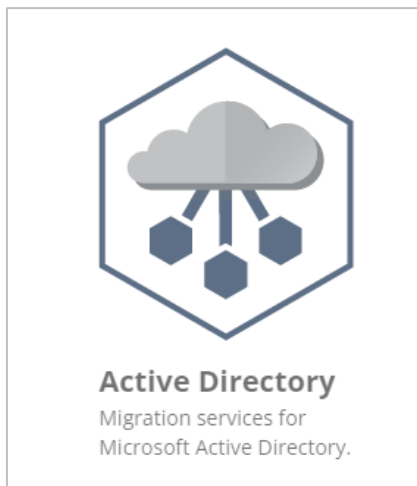
Buttons: REFRESH, SELECT ALL, UNMATCH, EXPORT

# On Demand Migration Active Directory Project

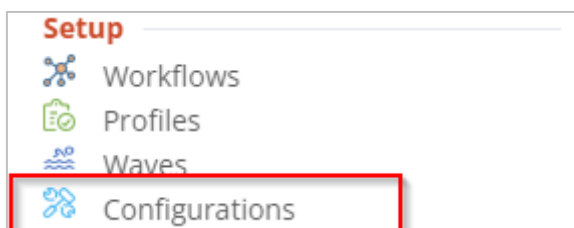
This section provides a step-by-step guide on how to configure Active Directory Migration configurations and migrating the source device to target Microsoft Entra ID only tenant.

## Install the local agent on the workstation

1. Log in to *On Demand*.
2. Navigate to *Migration*, select the project, and click on *Active Directory*.
3. Click on the *Active Directory* icon.



4. Via the hamburger menu, click on *Configurations*.





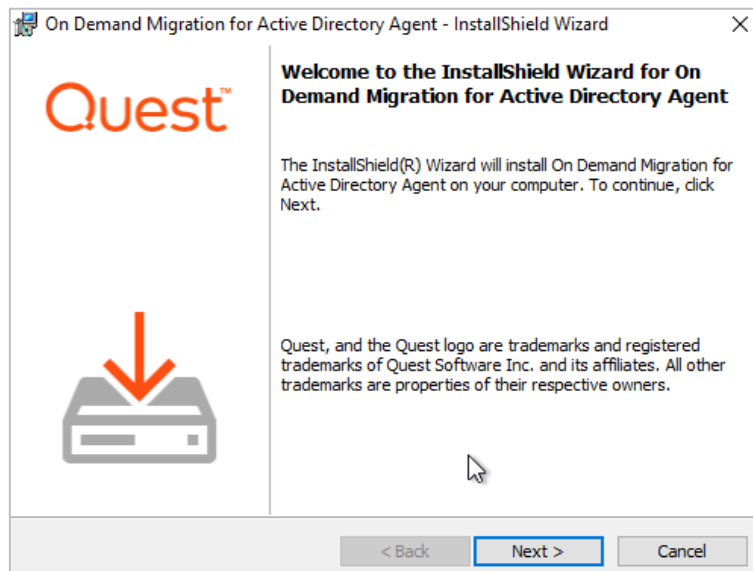
5. Download the latest device agent and note the Service URL and Auth Key for later use.

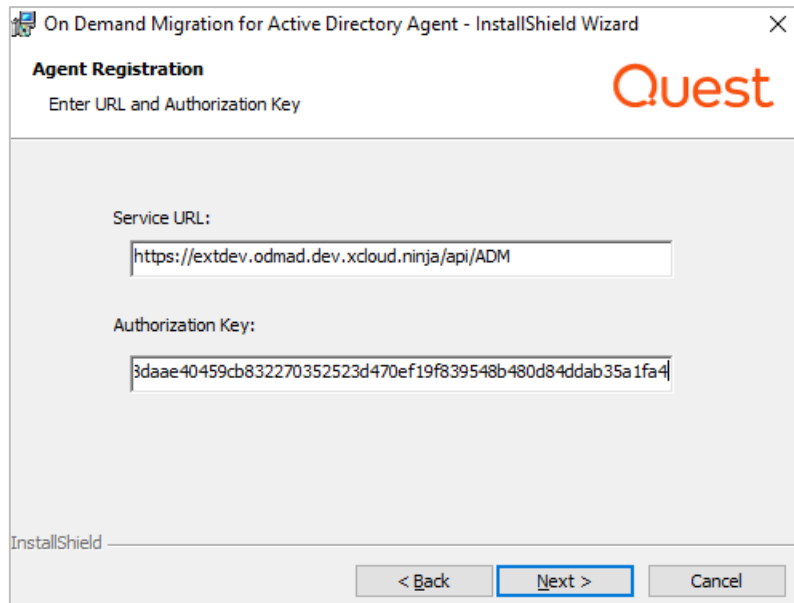
ACTIONS	<b>DOWNLOADS</b>
<b>DOWNLOADS</b>	
REPOSITORIES	
VARIABLES	

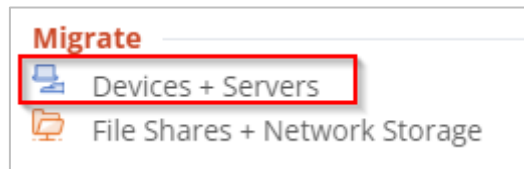
<b>DOWNLOADS</b>	
<b>MAPPING FILES</b>	
Select a Target environment to download user and group mapping files used during Device/Share ReACL. ⓘ	DEMO1 <input type="button" value="DOWNLOAD"/>
<b>DEVICE AGENT</b>	
Select a version of the device agent to download. ⓘ	20.12.8.9999 (LATEST) <input type="button" value="DOWNLOAD"/>
Service URL https://extdev.odmad.dev.xcloud.ninja/api/ADM	<input type="button" value="Copy"/>
Auth Key 5d915498daae40459cb832270352523d470ef19f839548b480d84ddb35a1fa4	<input type="button" value="Copy"/>
Perform automatic agent upgrades when a new agent version is available?	<input type="button" value="ENABLE"/> <input type="button" value="DISABLE"/>
<b>SQL RE-PERMISSION TOOL</b>	
Download the SQL Re-Permission Tool.	<input type="button" value="DOWNLOAD"/>

6. Copy the agent installation file onto the workstation and run the installer. The installer will prompt you to enter the Service URL and Auth Key noted in the previous step. Follow the installer wizard to complete the installation process.

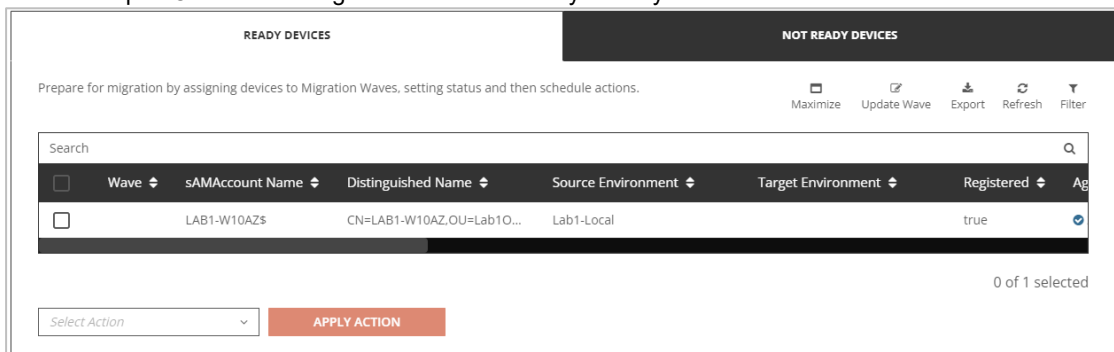




7. After the agent installation completes, you should see the device under the Ready Devices tab via *Devices + Servers* in the Hamburger Menu.

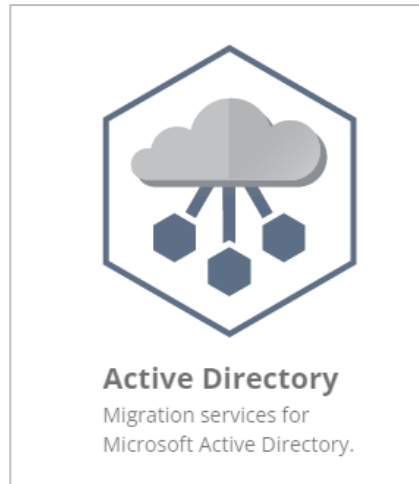


Note: by default, when the agent is first installed, it may take up to 4 hours for the agent to be registered and show up in On Demand Migration Active Directory “Ready Devices” view.

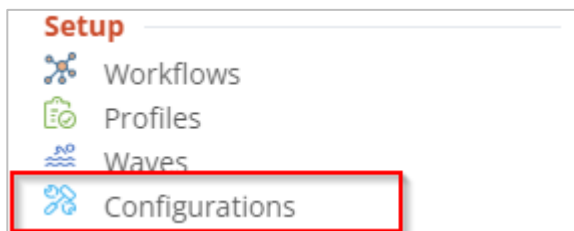


## Setup the Microsoft Entra Bulk Enrollment Repository and Microsoft Entra ID Join Migration Profile

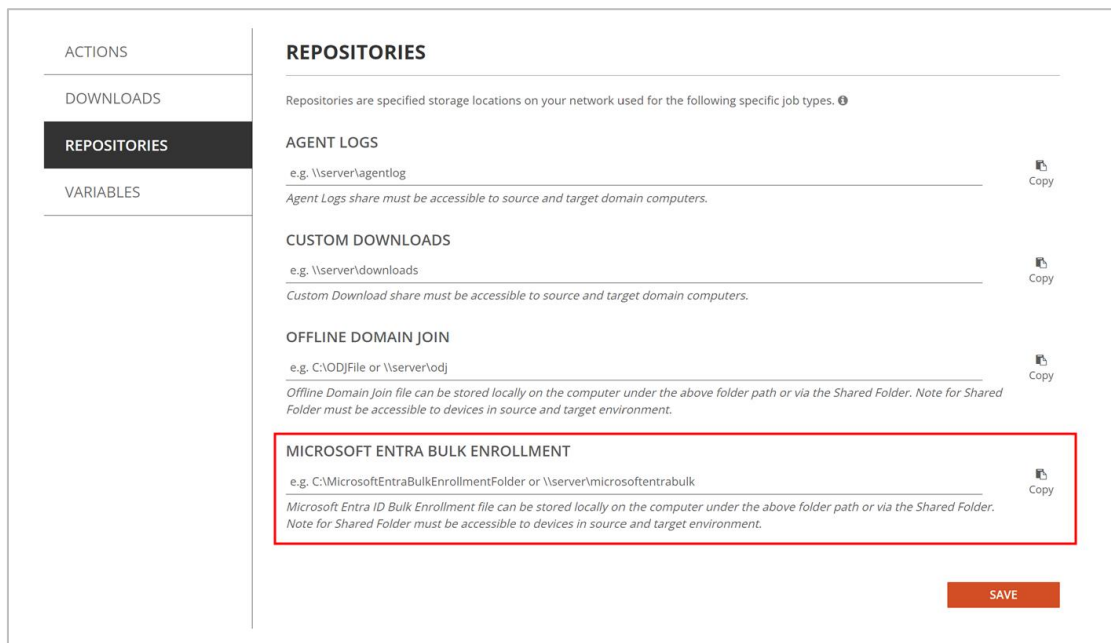
1. Log in to *On Demand*.
2. Navigate to *Migration*, select the project, and click on *Active Directory*.
3. Click on the *Active Directory* icon.



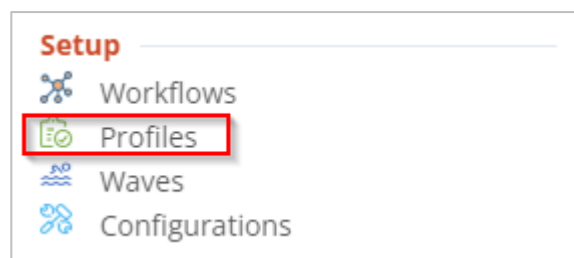
4. Via the hamburger menu, click on *Configurations*.



5. Click on *Repositories* and fill in the Provisioning Package Local Path or Shared Folder's UNC Path under *Microsoft Entra Bulk Enrollment*. Click *Save*.



6. Via the hamburger menu, click on *Profiles*.



7. Click on *Microsoft Entra Join* tab, and click on *Add* to create a new *Microsoft Entra Join Profile*.

8. Enter the following information in the profile and click Save.
  - a. Name of the Profile
  - b. Provisioning Package File Name
  - c. Source Domain Credential
  - d. Specify the target Microsoft Entra tenant
  - e. Choose an option to either preserve the computer name or use the name defined in the provisioning package.

✕

### Add Your Microsoft Entra Join Profile

**PROFILE NAME**  
Entra Join

---

**BULK ENROLLMENT PACKAGE FILE NAME**  
Enter file name

---

**TARGET ENVIRONMENT**  
Select Environment ▾

**DEVICE NAME OPTION**

**DEVICE NAME DEFINED PER PROVISIONING PACKAGE**

**KEEP ORIGINAL DEVICE NAME**

CLEAR NEXT

- f. Click Next
- g. Enter the Source Domain Credential information including the Domain FQDN. Note, if the source device is an Microsoft Entra Join Cloud Only device, you may uncheck the “Active Directory Joined or Microsoft Entra Hybrid Joined” option.

For Preflight check validation, choose this option if the source device is a remote workstation that does not have access to Local On-Premise Active Directory.

To add a new user to the local admin group, select the Create Local Admin option and enter a Username and Password for the new user.

### Add Your Microsoft Entra ID Join Profile

SOURCE DIRECTORY IS ACTIVE DIRECTORY JOINED OR HYBRID MICROSOFT ENTRA ID JOINED

**SOURCE DOMAIN CREDENTIALS**  
 FQDN OF DOMAIN (E.G. FABRIKAM.COM)  
 Enter Domain \_\_\_\_\_

USERNAME (E.G. FABRIKAM\USERNAME OR USERNAME@FABRIKAM.COM)  
 Enter Username \_\_\_\_\_

PASSWORD  
 Enter Password \_\_\_\_\_

**PREFLIGHT CHECK VALIDATION**  
 SKIP SOURCE LOCAL ACTIVE DIRECTORY VALIDATION

---

CREATE LOCAL ADMIN

**CREDENTIALS**  
 USERNAME  
 LocalAdmin \_\_\_\_\_

PASSWORD  
 ..... \_\_\_\_\_

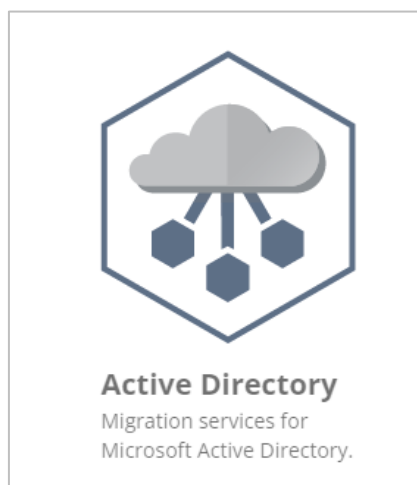
BACK
SAVE PROFILE

h. Click Save Profile

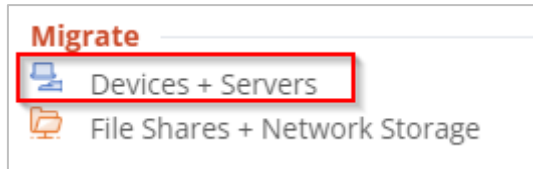
## Perform Device Migration

This section provides a step-by-step guide on how to perform the Device Migration to Microsoft Entra ID Join including Device ReACLing, and Device Cutover.

1. Log in to [On Demand](#).
2. Navigate to *Migration*, select the project, and click on *Active Directory*.
3. Click on the *Active Directory* icon.

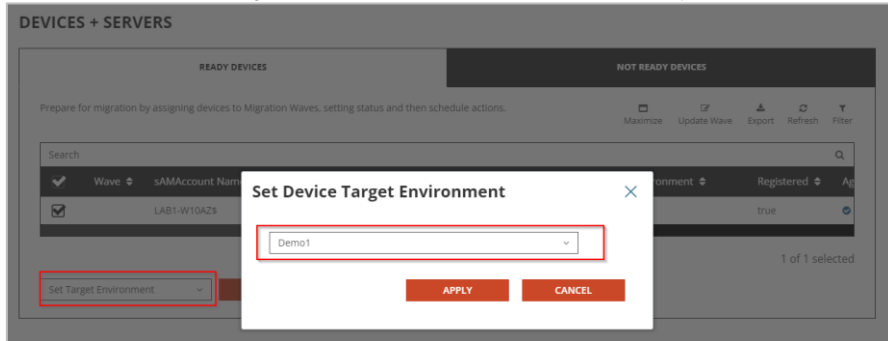


4. Via the hamburger menu, click on *Devices + Servers*.



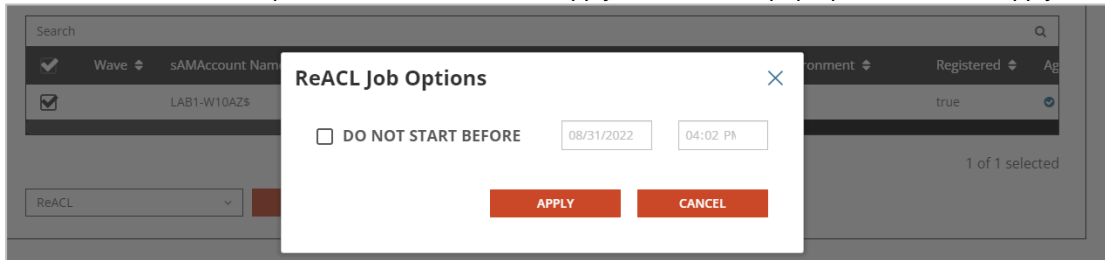
5. First, we will define the target environment for the device.

Select the device, select *Set Target Environment* from the drop-down action menu, click *Apply Action*. In the pop-up window, select the target Microsoft Entra tenant and click *Apply*.

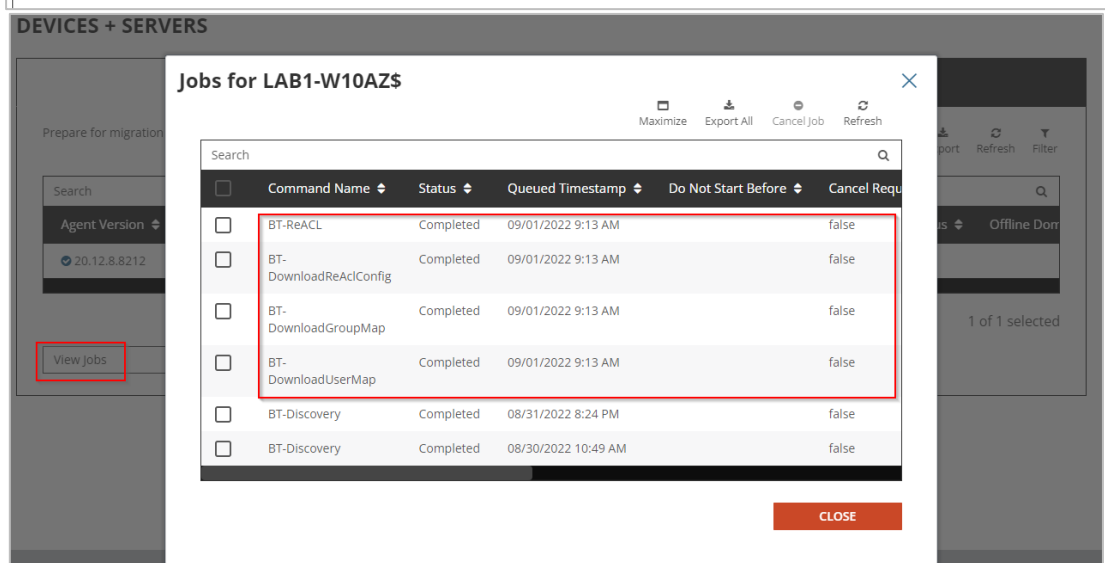
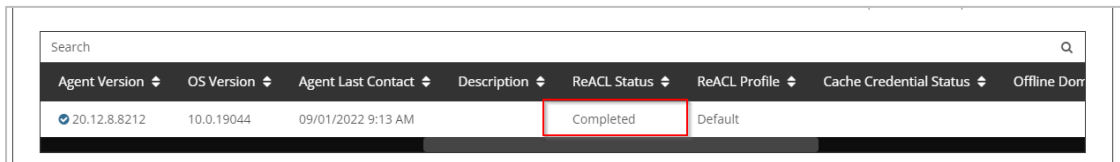


6. Next, we will perform the Device ReACL in preparation for Microsoft Entra ID Join cutover.

Select *ReACL* via the drop-down action menu, click *Apply Action*. In the pop-up window, click *Apply*.



7. The Device will receive the ReACL job shortly and complete the processing. You may check the job status via the ReACL Status or select *View Jobs* action from the drop-down menu.



8. Next, we will perform the Microsoft Entra ID Join device cutover.

Select *Microsoft Entra ID Cutover* via the drop-down action menu, click *Apply Action*. In the pop-up window, select the Microsoft Entra ID Profile configured earlier and click *Apply*.

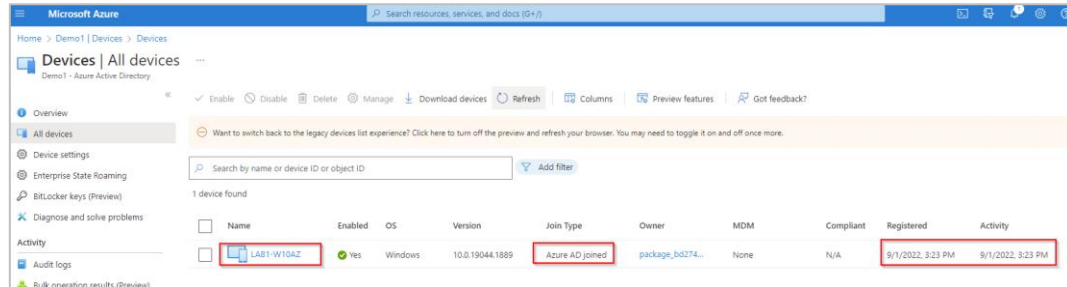
- The Device will receive the Microsoft Entra ID Cutover job request shortly and perform the reboot to complete the Microsoft Entra ID device join. You may check the job status via the Microsoft Entra ID Cutover Status or select *View Jobs* action from the drop-down menu.

Command Name	Status	Queued Timestamp	Do Not Start Before	Cancel
BT-AzureADCutover	Completed	09/01/2022 3:13 PM		false
BT-ReACLPrepareWin10Profiles	Completed	09/01/2022 3:13 PM		false
BT-DownloadReAcConfig	Completed	09/01/2022 3:13 PM		false
BT-AzureADCutoverPreflight	Completed	09/01/2022 3:13 PM		false
BT-ReACL	Completed	09/01/2022 9:13 AM		false
BT-DownloadReAcConfig	Completed	09/01/2022 9:13 AM		false
BT-DownloadGroupMap	Completed	09/01/2022 9:13 AM		false
BT-DownloadUserMap	Completed	09/01/2022 9:13 AM		false
BT-Discovery	Completed	08/31/2022 8:24 PM		false
BT-Discovery	Completed	08/30/2022 10:49 AM		false

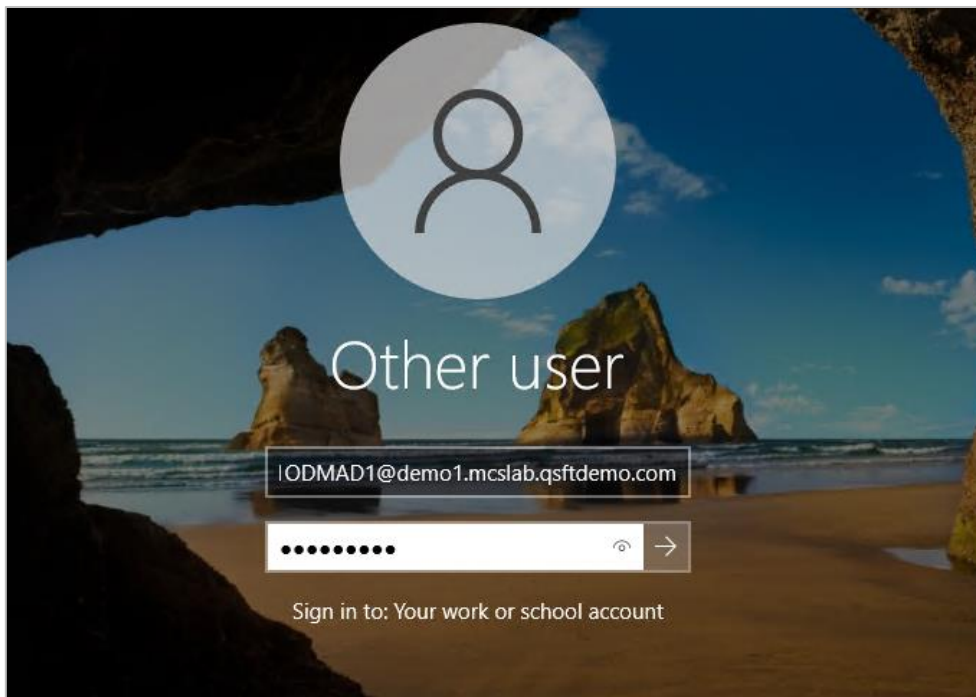
# Validate Device Post Microsoft Entra ID Join

This section provides a step-by-step guide on how to validate the device after it is Microsoft Entra ID Joined to the target tenant.

1. Log into target Microsoft Entra ID Admin Center, via the Device view and verify the device is Microsoft Entra ID Joined.

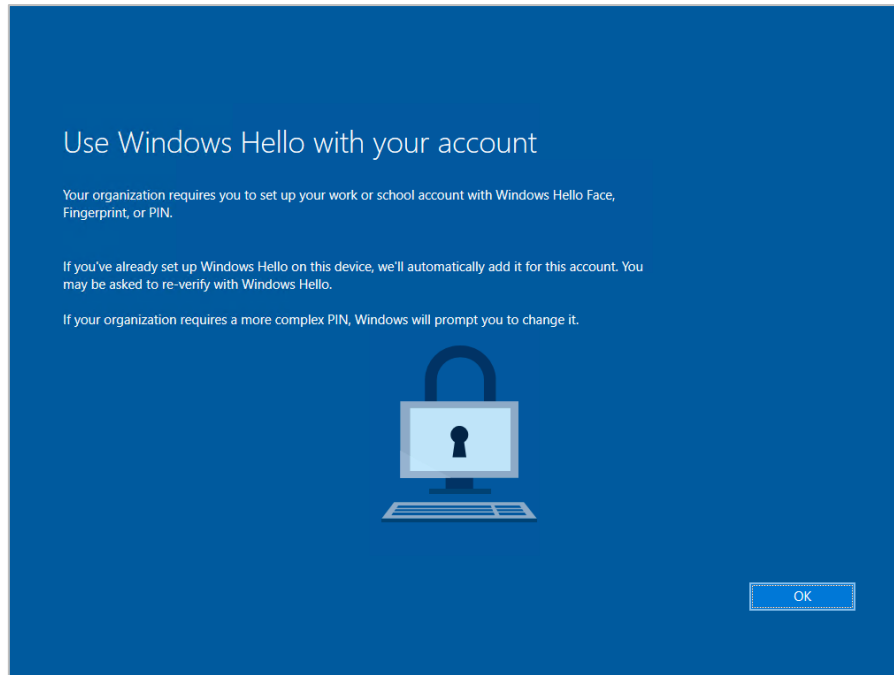


2. Log in to the workstation using your account UPN in the target Microsoft Entra ID.

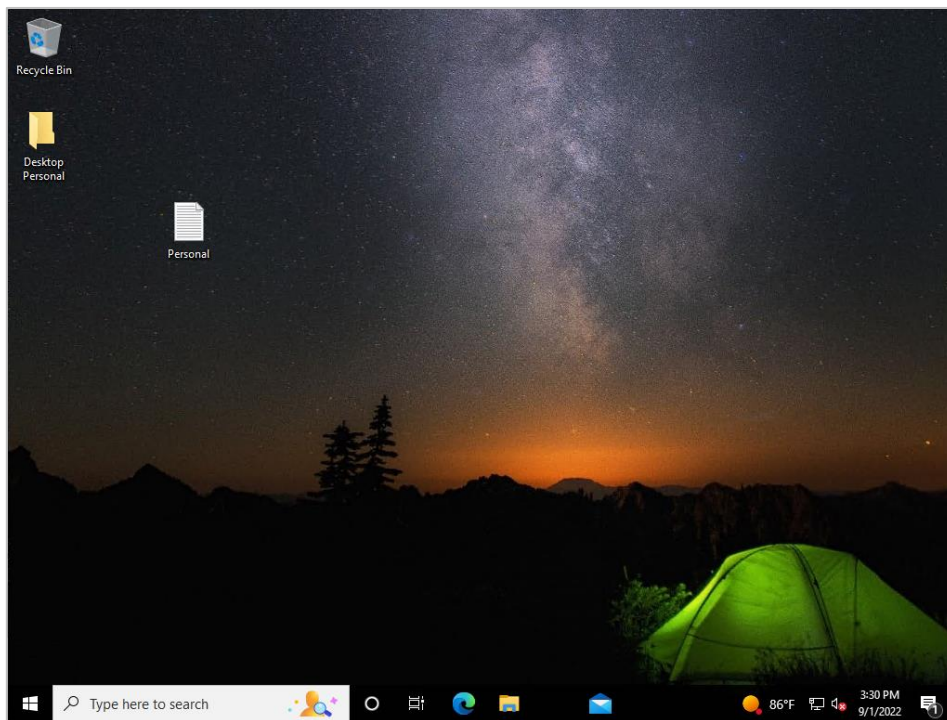


3. Windows may prompt you to setup Windows Hello or MFA, depending on your tenant's policy. Follow the on-screen instructions.

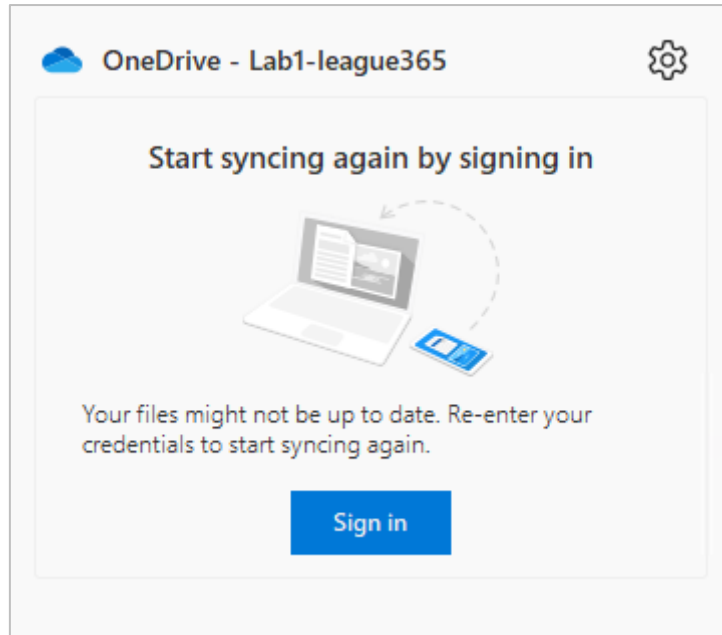




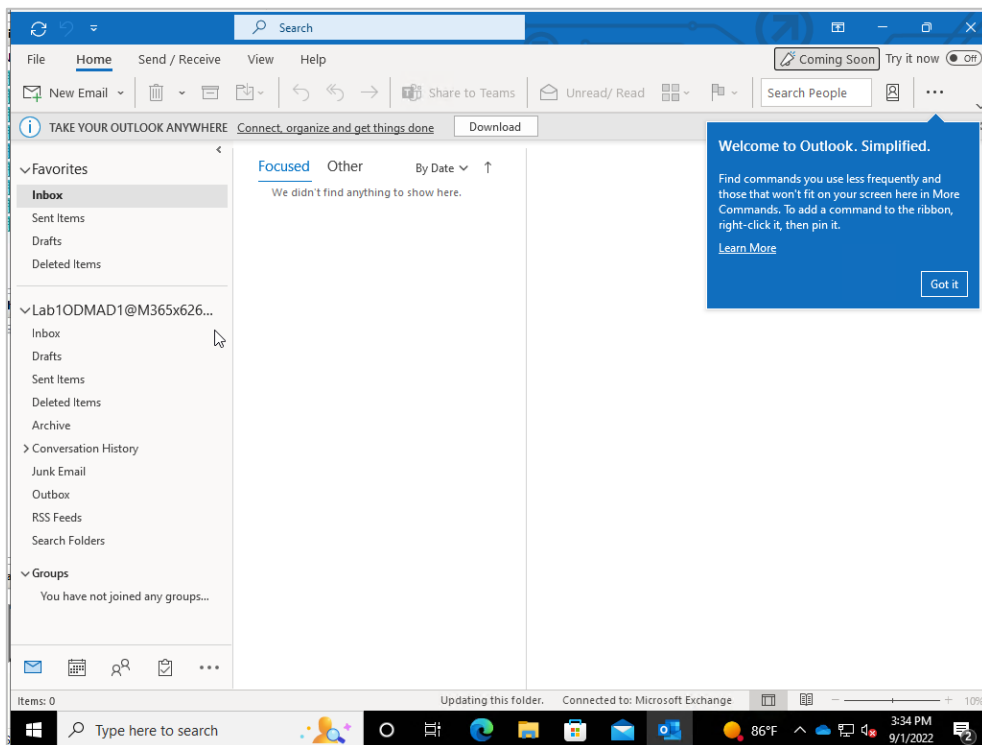
4. Windows will complete the login process. Verify the user profile remains the same as the source user.



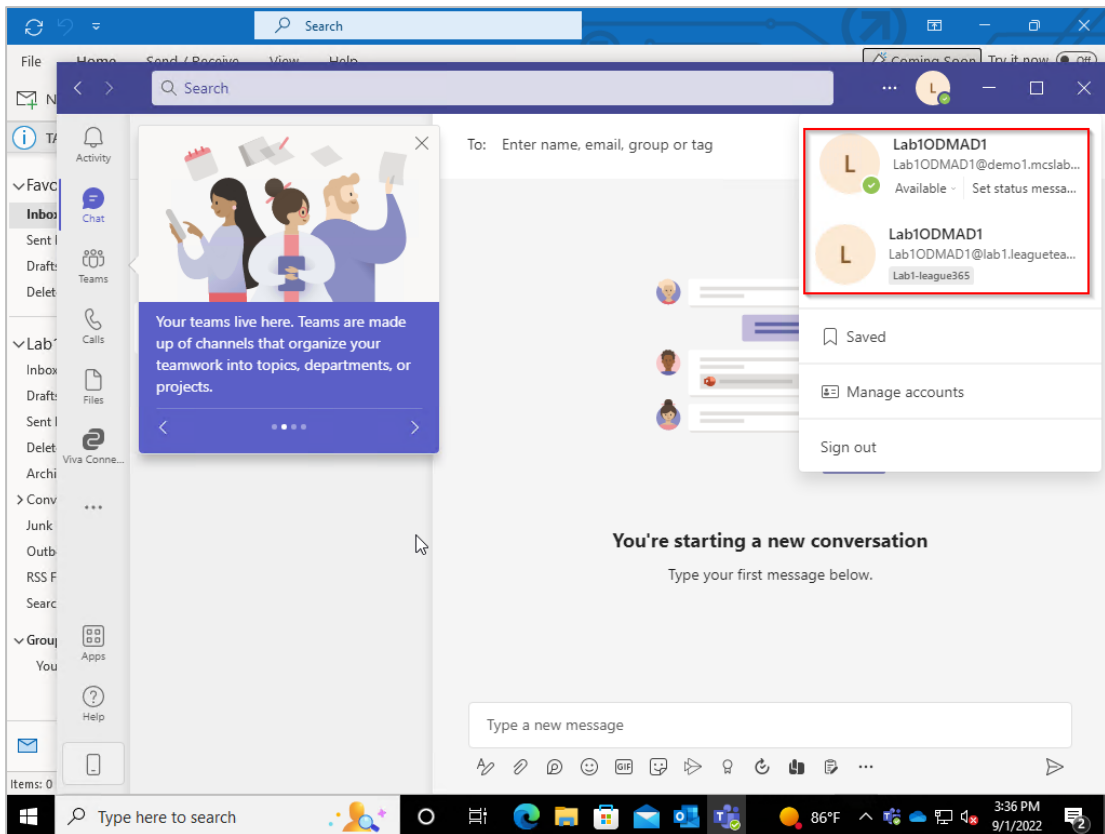
5. In the System Tray, locate the OneDrive icon, right click, and Click *Sign in*.



6. OneDrive will prompt you to enter the account credential. Follow the on-screen instructions and complete the sign in process.
7. Open Outlook and follow the on-screen instructions when Outlook prompts you to enter the account credential. Outlook should start once the credential is authenticated.



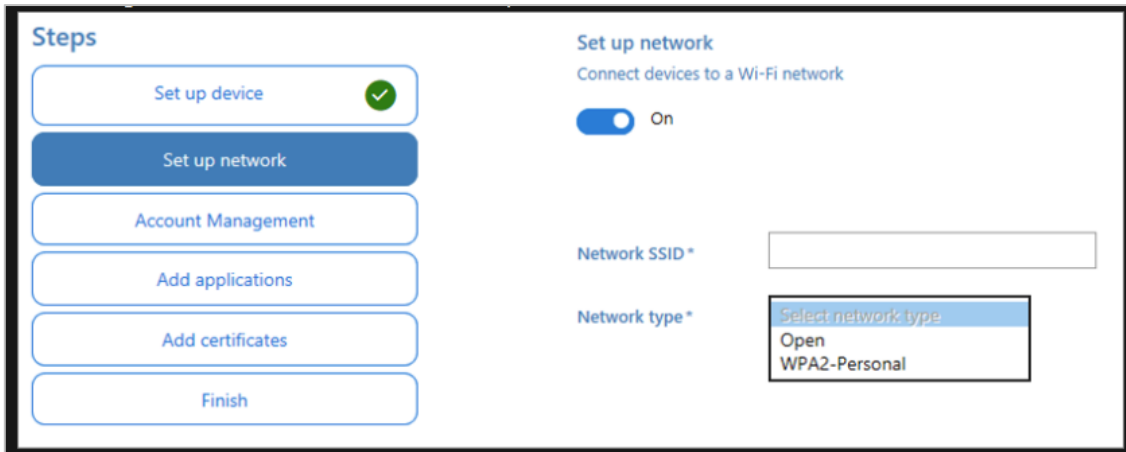
8. Launch the Teams client. Because your device is Microsoft Entra ID Joined, the target Teams account will be automatically added, while the original source account should also be retained.



## Frequently Asked Questions

### Can I use configure Wi-Fi access point for my devices to use post Microsoft Entra ID Join?

Device Wi-Fi access point can be configured via the Microsoft Entra ID Join Provisioning Package. Additional detail can be found at this [Link](#).



## I cannot connect to my devices via Remote Desktop Service post Microsoft Entra ID Join.

Remote Desktop Connection file may have to be modified in order to connect to Microsoft Entra ID Join device via RDP. The following settings need to be changed in the RDP file.

- authentication level:i:2
- enablecredsspssupport:i:0
- username:s:Lab1ODMAD1@demo1.mcslab.qsftdemo.com
- domain:s:AzureAD

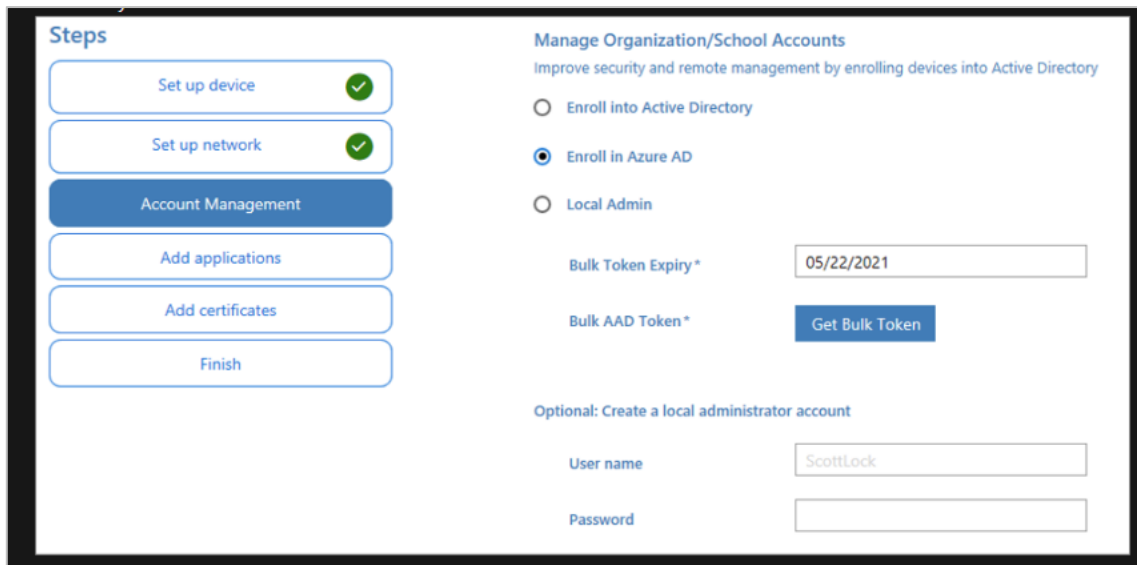
Additional information and instruction can be found at this Microsoft Soft Link [Remote Desktop Connection for credentials - Windows Server | Microsoft Docs](#)

## What is the Microsoft Entra ID NetBIOS name for my Microsoft Entra ID Users?

For Microsoft Entra ID Devices, the default NetBIOS name is AzureAD. For Hybrid Microsoft Entra ID Join devices, the NetBIOS name can be configured using the On-Premises Active Directory's NetBIOS name.

## Can I provision a local administrator for my devices during Microsoft Entra ID Join process?

For Microsoft Entra ID Devices, an optional local administrator account can be configured via the Microsoft Entra ID Join Provisioning Package. Additional detail can be found at this [Link](#).



## Can I provision additional applications and adding a certificate for my devices during Microsoft Entra ID Join process?

For Microsoft Entra ID Devices, applications and certificate account can be configured via the Microsoft Entra ID Join Provisioning Package. Additional detail can be found at this [Link](#).

## My device is Microsoft Entra ID Joined, it is prompting me to setup MFA and Windows Hello, is this normal?

Yes, it is normal for users to receive MFA and/or Windows Hello setup prompt if the organization has policy in place which requires users to configure these security settings.

## After my user devices are Microsoft Entra ID Joined to the target tenant, how can users switch their Microsoft Apps such as OneDrive, Teams, and

# Outlook to start using target tenant account?

On Demand Migration Desktop Update Agent provides an automated solution to help end-users switch their desktop applications to their new target M365 accounts. Additional Detail and Help related to Desktop Update Agent can be found at [On Demand Migration Current - Desktop Update Agent User Guide \(quest.com\)](#).

# Is there a way that I can use On Demand Migration Active Directory to migrate my devices if they are Microsoft Entra ID Join only in the source?

Support for devices that are Microsoft Entra ID Joined (Cloud Only, Not Hybrid Microsoft Entra ID Joined) in the source and wants to Microsoft Entra ID Join to a target tenant is supported. Please ensure to include devices in the source environment's object filter and the following attribute is part of your template mapping if an existing template is used.

MAPPING

Below is a list of your mapped attributes. Double-click a mapping entry to modify.

Target	Type	Source	Target Object Type
DeviceCategory	Basic	DeviceCategory	All
DeviceId	Basic	DeviceId	All
DeviceMetadata	Basic	DeviceMetadata	All
DeviceVersion	Basic	DeviceVersion	All

NEW ADVANCED SELECT ALL EXPORT ALL REMOVE SAVE

# Can I migrate to and from GCC/GCCH tenants?

Active Directory supports GCC and GCCH as target environments, in addition to Commercial tenants. Only Commercial and GCC are supported as source environments. To enable GCC/GCCH Device Migration, please contact Quest Support for additional configuration described in the following article: [Update GCC/GCCH tenant object's RID value for ReACL](#). This configuration is required for successfully switching the user profile during cutover.

# After Cutover, why is the Windows screen flickering or displaying a black screen on some devices?

After a successful cutover and when the target user logs onto to the device, Windows is unusable. For a Windows 10 device, the windows task bar just flickers. For a Windows 11 device, the screen is black but after about 10 minutes, the windows task bar is displayed but does not function correctly.

This is only occurring in the unique situation where the On Premise user object is being synced to the source tenant user object using Entra Connect and then the same On Premise user object is then synced to the target tenant user object also using Entra Connect.

In this situation the following registry keys are locking the profile to the source tenant account and these keys must be removed before logging on with the target account.

HKLM:\Software\Microsoft\IdentityStore\Cache - subfolders  
And  
HKLM:\Software\Microsoft\IdentityStore\LogonCache - subfolders:

1 - This can be done manually on the device.

1. Download and extract PSEXEC.
2. Open a cmd prompt as admin.
3. Change location to folder where PSEXEC have been extracted and run  
"psexec -s -i cmd.exe"  
It will open a new cmd with system admin permission and run regedit:  
This will open a cmd prompt as a local system account
4. Run regedit from this new window.
5. Perform the registry removal as mentioned above.
6. Reboot device.

2 - Create a custom task in On Demand Migration Active Directory that will run PowerShell scripts to remove these registry keys.

This custom task can be added to a custom Entra Cutover action or be added to a new Action and run as required.

The following are SAMPLE scripts to remove these registry keys.

Note that these scripts are provided as-is for example purposes only, and you may need to modify them to work for your specific project.

If required to be amended, this will need to be done by you or with assistance from Quest's Professional Services Team.

## DeleteCache Script

```

# Define the registry path
$registryPath = "HKLM:\Software\Microsoft\IdentityStore\Cache"

# Check if the registry path exists
if (Test-Path $registryPath) {
    # Get all subkeys of the specified registry path
    $subkeys = Get-ChildItem -Path $registryPath

    # Loop through each subkey and delete it
    foreach ($subkey in $subkeys) {
        try {
            Remove-Item -Path $subkey.PSPath -Recurse -Force
            Write-Output "Deleted: $($subkey.PSPath)"
        } catch {
            Write-Output "Failed to delete: $($subkey.PSPath)"
        }
    }
} else {
    Write-Output "Registry path does not exist: $registryPath"
}

```

### DeleteLogonCache Script

```

# Define the registry path
$registryPath = "HKLM:\Software\Microsoft\IdentityStore\LogonCache"

# Check if the registry path exists
if (Test-Path $registryPath) {
    # Get all subkeys of the specified registry path
    $subkeys = Get-ChildItem -Path $registryPath

    # Loop through each subkey and delete it
    foreach ($subkey in $subkeys) {
        try {
            Remove-Item -Path $subkey.PSPath -Recurse -Force
            Write-Output "Deleted: $($subkey.PSPath)"
        } catch {
            Write-Output "Failed to delete: $($subkey.PSPath)"
        }
    }
} else {
    Write-Output "Registry path does not exist: $registryPath"
}

```



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](http://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.