On Demand Migration Active Directory Entra-Join

Quick Start Guide

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.**

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

On Demand Migration Active Directory Entra-Join – Quick Start Guide
Updated – January 2025

Contents

Introduction 4

Topics 4

Requirements 4

Environment Preparation 6

Provisioning Package Preparation 6

Device Migration 10

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

Frequently Asked Questions 27

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

After Cutover, why is the Windows screen flickering or displaying a black screen on some devices? 30

About us 33

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

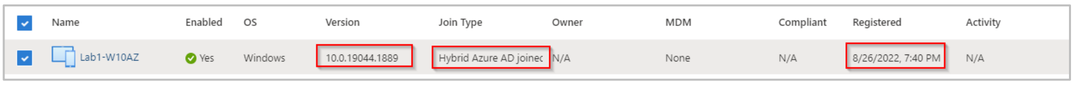
- Three (3) PowerShell accounts are automatically created to read and update objects in the cloud. To do this, an OAuth token is used from the account used to add the Cloud Environment.
- These PowerShell accounts do not require any Microsoft 365 licenses.

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 Connectconfigured.
- 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 Connectconfigured.
- 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 joinec	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

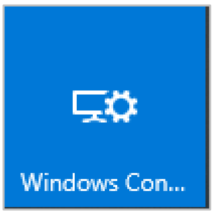
Provisioning Package Preparation

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.

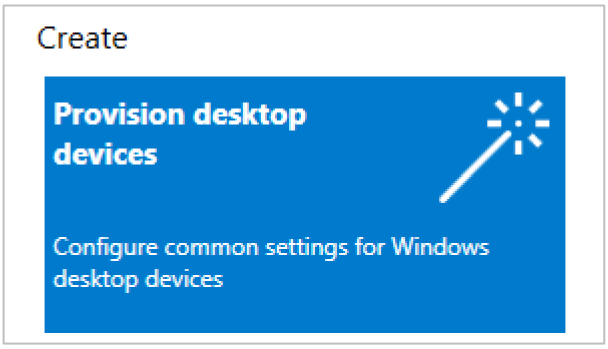
1. Download the Windows Configuration Designer (WCD) from the Microsoft Store.

   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.

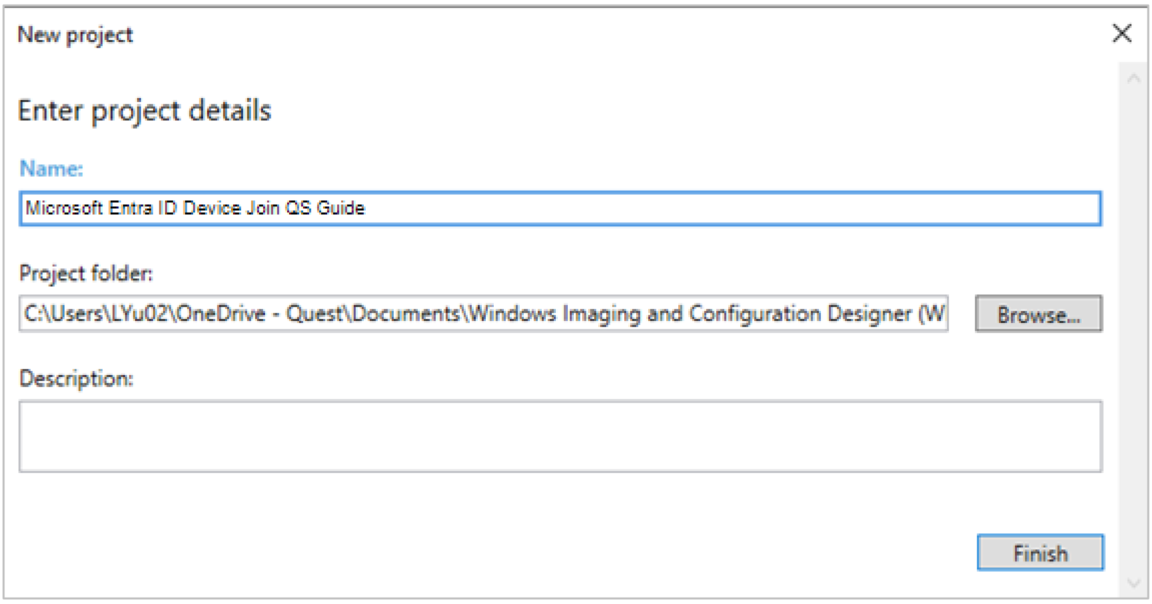


Create

Provision desktop devices

Configure common settings for Windows desktop devices

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



New project

Enter project details

Name:

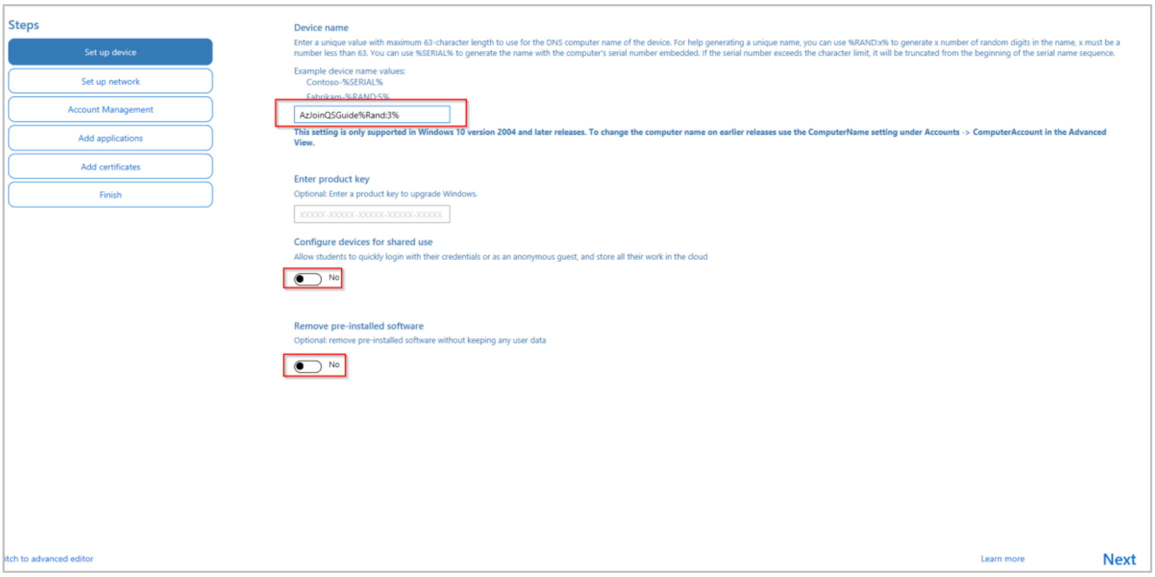
Microsoft Entra ID Device Join QS Guide

Project folder:

C:\Users\LYu02\OneDrive - Quest\Documents\Windows Imaging and Configuration Designer (W

Description:

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



Device name

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.

Example device name values:
Contoso-%SERIAL%
Fabrikam-%RAND:5%

AzJoinQSGuide%Rand:3%

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.

Enter product key

Optional: Enter a product key to upgrade Windows.

XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Configure devices for shared use

Allow students to quickly login with their credentials or as an anonymous guest, and store all their work in the cloud

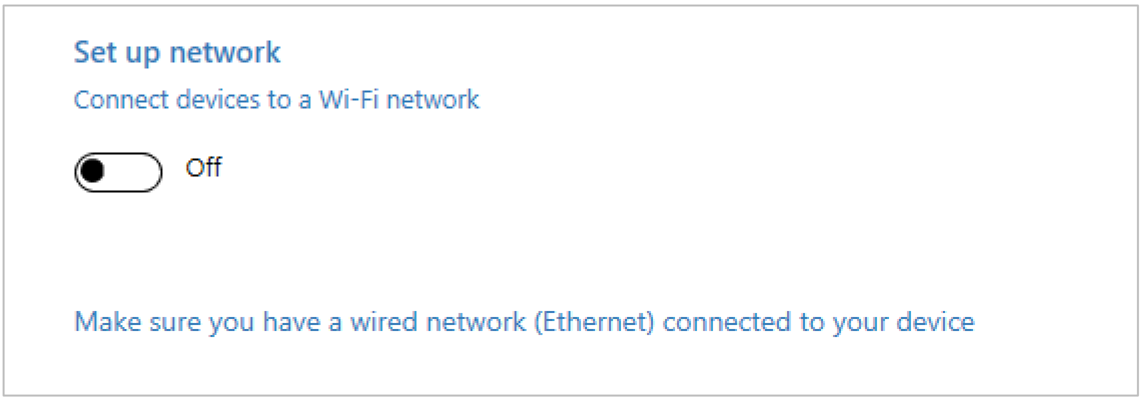
No

Remove pre-installed software

Optional: remove pre-installed software without keeping any user data

No

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

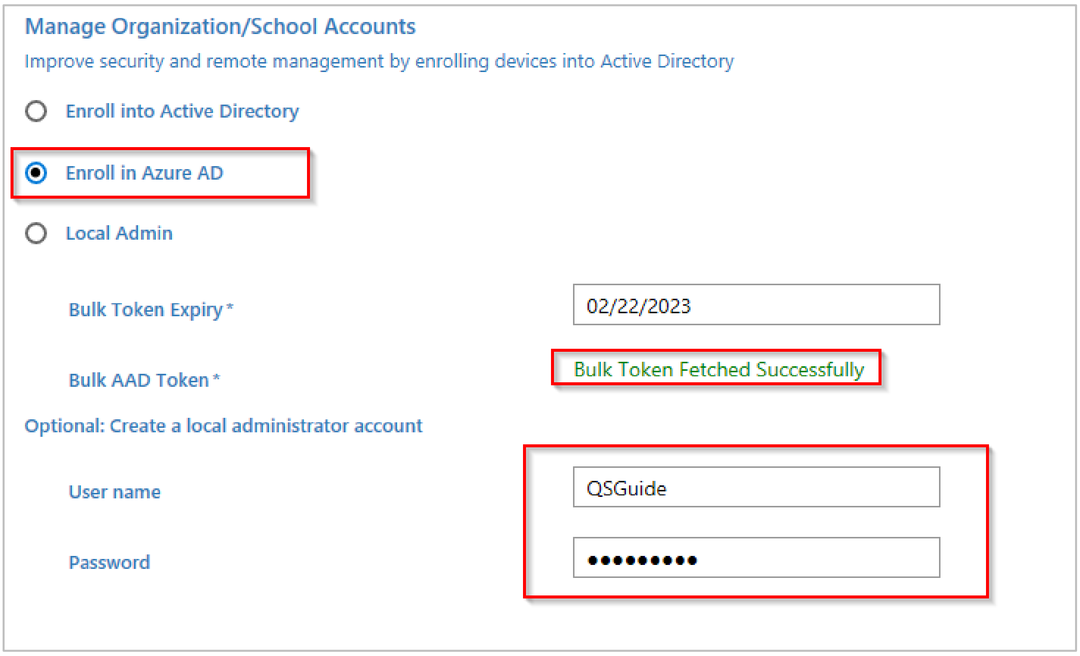
Connect devices to a Wi-Fi network

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

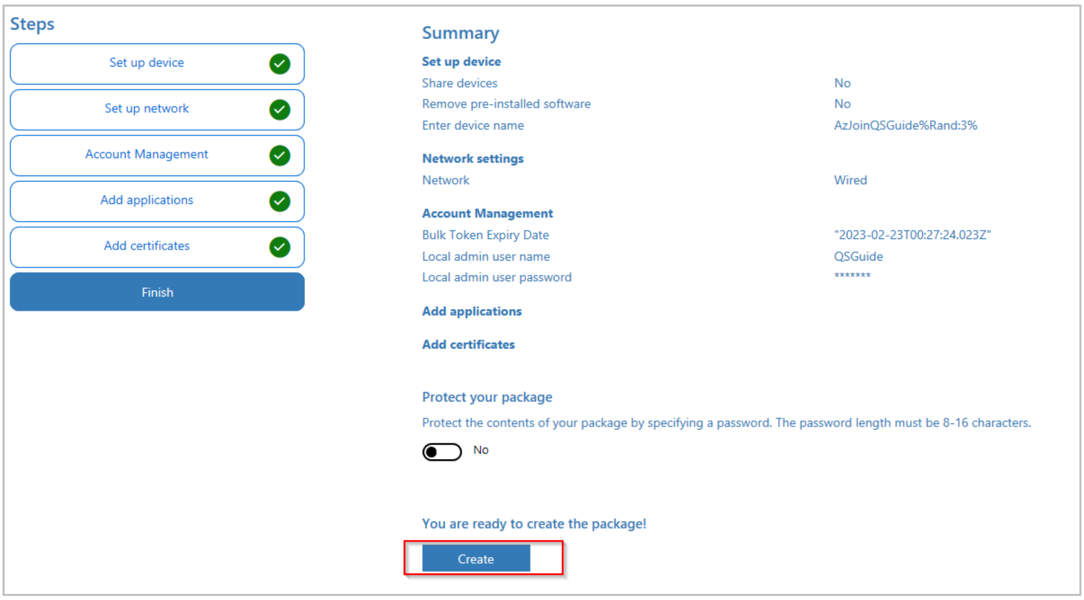
Bulk Token Expiry *	02/22/2023
Bulk AAD Token *	Bulk Token Fetched Successfully

Optional: Create a local administrator account

User name	QSGuide
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 ✓

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!

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

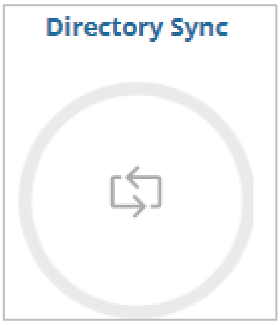
On Demand Migration Directory Sync

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.

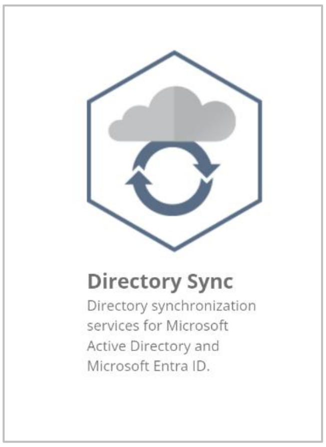
Setting up the Directory Sync Local Environment

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.



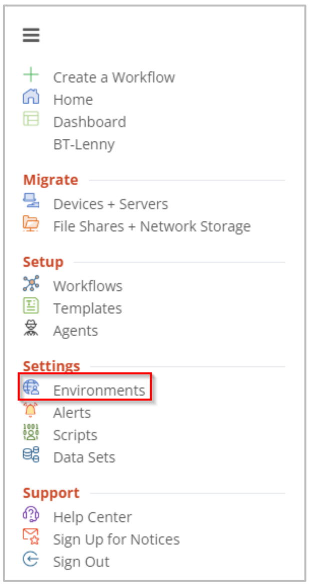
5. Once the On Demand Migration Directory Sync module is loaded, click on the Directory Sync icon in the main dash view.



Directory Sync

Directory synchronization services for Microsoft Active Directory and Microsoft Entra ID.

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

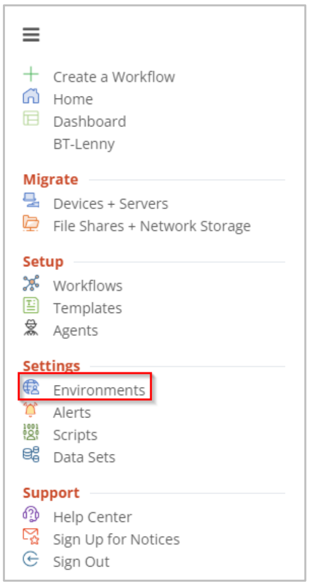


7. Click the *New* button.
8. Click *Local* as the environment type, Click *Next*.
9. Name the environment, Click *Next*.
10. Name the local agent, Click *Next*.
11. Note the agent registration URL and registration Key for later use, click *Finish*.
12. Install the agent in the Windows Server that is 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.

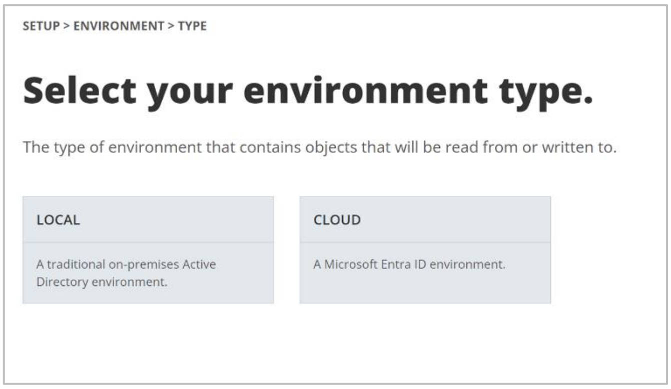
    Note, Refer to On Demand Migration Active Directory Online Help Center *for* detailed information about agent *installation and set-up requirements.*
13. Once the agent is installed and the environment is discovered, click on the *Setting* button to access the local AD environment setting page.
14. Click 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*.



SETUP > ENVIRONMENT > TYPE

Select your environment type.

The type of environment that contains objects that will be read from or written to.

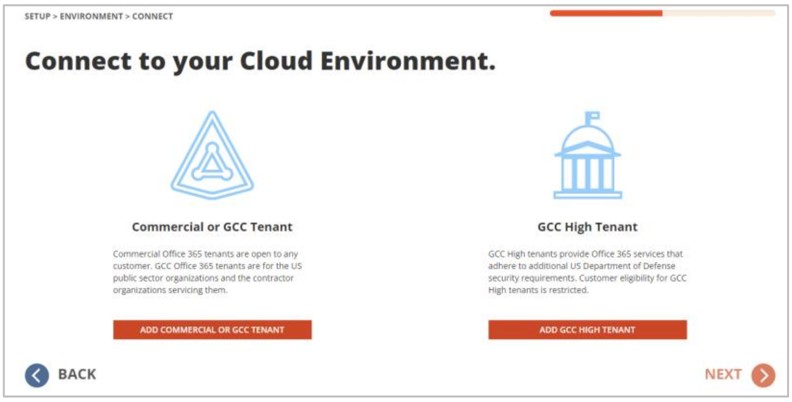
LOCAL

A traditional on-premises Active Directory environment.

CLOUD

A Microsoft Entra ID environment.

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



SETUP > ENVIRONMENT > CONNECT

Connect to your Cloud Environment.

Commercial or GCC Tenant

Commercial Office 365 tenants are open to any customer. GCC Office 365 tenants are for the US public sector organizations and the contractor organizations servicing them.

ADD COMMERCIAL OR GCC TENANT

GCC High Tenant

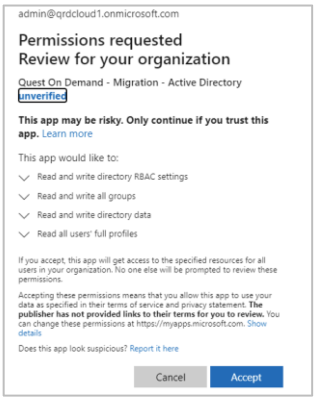
GCC High tenants provide Office 365 services that adhere to additional US Department of Defense security requirements. Customer eligibility for GCC High tenants is restricted.

ADD GCC HIGH TENANT

BACK

NEXT

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



admin@qrdcloud1.onmicrosoft.com

Permissions requested
Review for your organization

Quest On Demand - Migration - Active Directory
unverified

This app may be risky. Only continue if you trust this app. Learn more

This app would like to:

- Read and write directory RBAC settings
- Read and write all groups
- Read and write directory data
- Read all users' full profiles

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

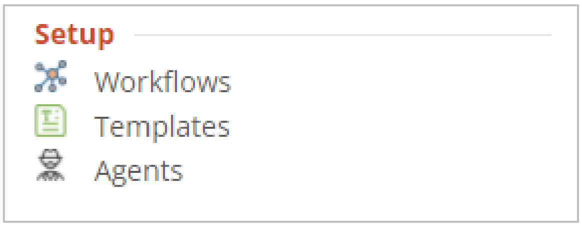
7. Click *Next*.
8. Configure the cloud environment filter group and click *Next*.
9. Select the "Include Objects Synchronized with a Local Active Directory via Microsoft Entra Connect option if you wish to include Hybrid Objects. For the purpose of this guide, we will leave this option unchecked and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

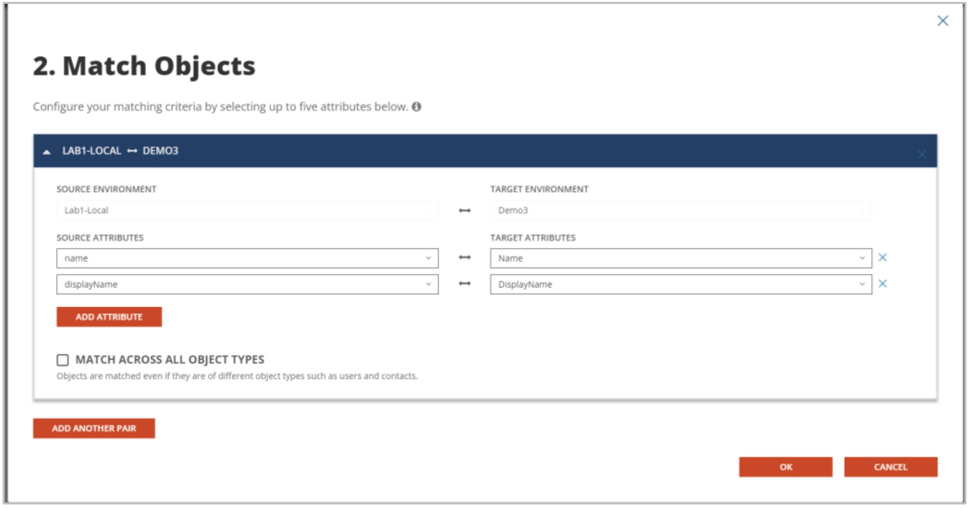
Important Tip: If you do not wish to create objects in your target environment, please choose “Skip” or “Do Not Create” option for each object type.

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

SOURCE ENVIRONMENT: Lab1-Local ⟷ TARGET ENVIRONMENT: Demo3

SOURCE ATTRIBUTES		TARGET ATTRIBUTES
name	⟷	Name
displayName	⟷	DisplayName

□ MATCH ACROSS ALL OBJECT TYPES

Objects are matched even if they are of different object types such as users and contacts.

    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.*

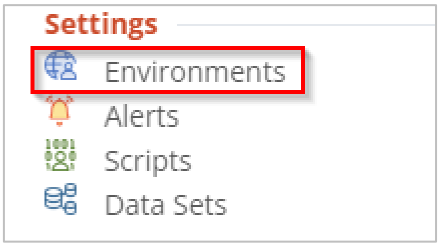
Running Directory Sync Workflow and validating the sync results

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.

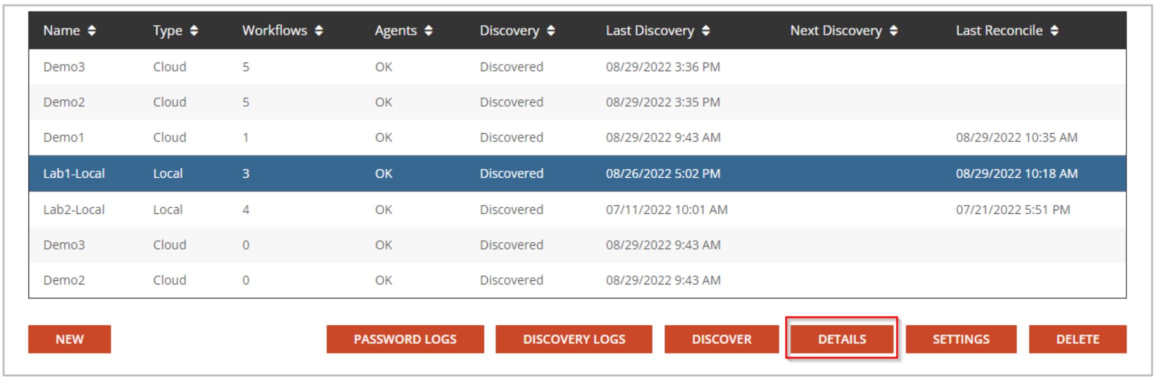
1. Log in to *On Demand.*
2. Navigate to *Migration,* select the project, and click on *Directory Sync.*
3. Click on the *Directory Sync* icon.
4. Select the workflow created and click *Run* button.
5. Allow the workflow run to complete.
6. Select the workflow created and click *Run* button again.

    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.

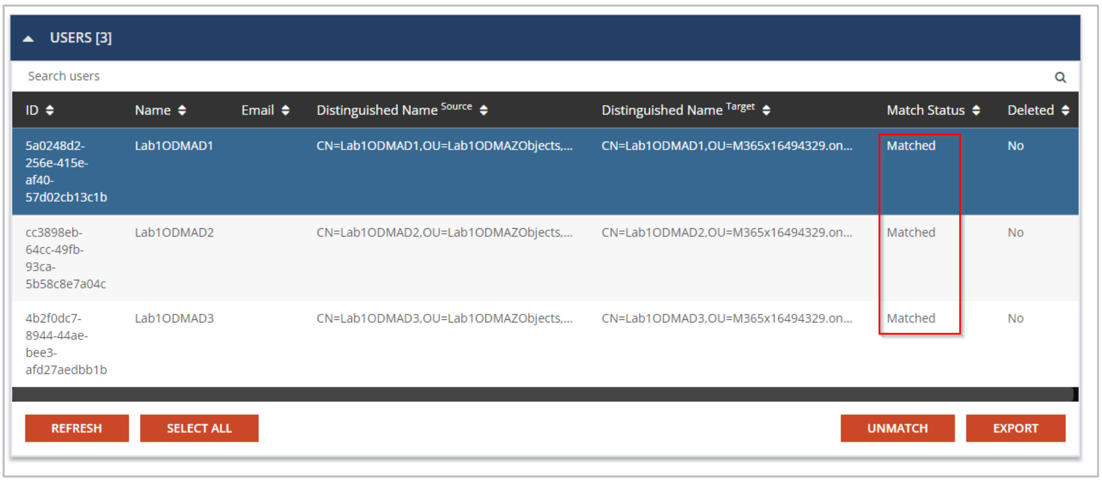


8. Select the Local On-Premises AD environment and click on *Details*.



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		

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



USERS [3]

Search users

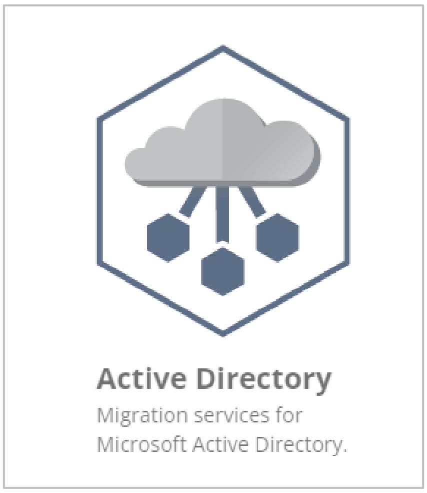
ID	Name	Email	Distinguished Name Source	Distinguished Name Target	Match Status	Deleted
5a0248d2-256e-415e-af40-57d02cb13c1b	Lab1ODMAD1		CN=Lab1ODMAD1,OU=Lab1ODMAZObjects,...	CN=Lab1ODMAD1,OU=M365x16494329.on...	Matched	No
cc3898eb-64cc-49fb-93ca-5b58c8e7a04c	Lab1ODMAD2		CN=Lab1ODMAD2,OU=Lab1ODMAZObjects,...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

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

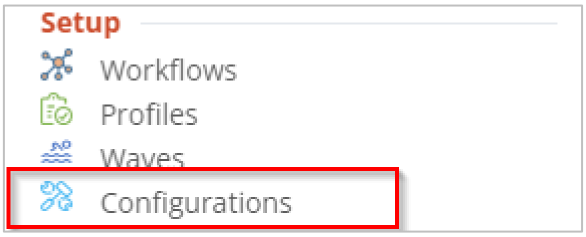
1. Log in to *On Demand.*
2. Navigate to *Migration,* select the project, and click on *Active Directory.*
3. Click on the *Active Directory* icon.



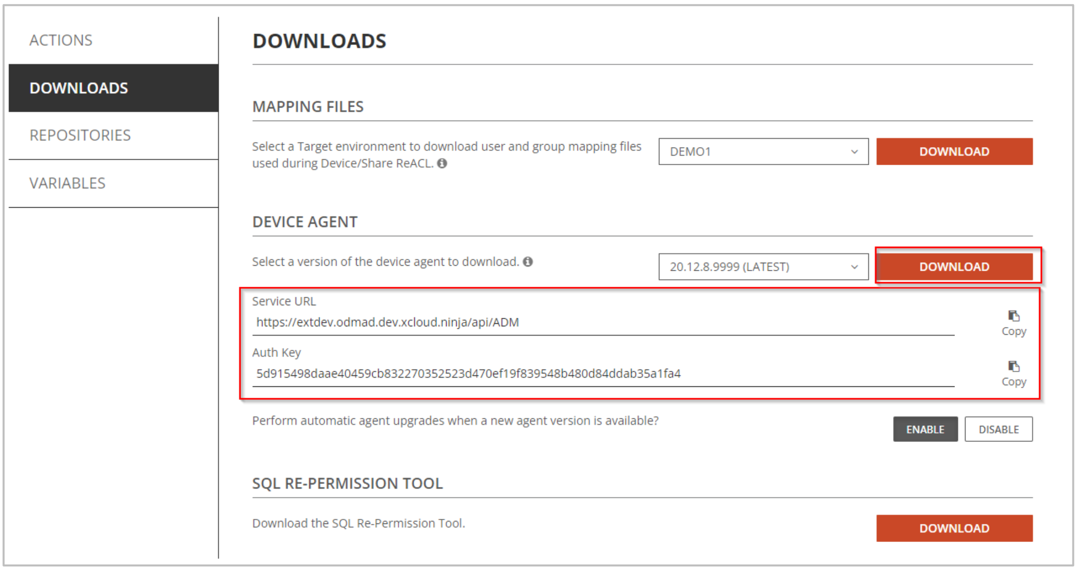
Active Directory

Migration services for Microsoft Active Directory.

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.



DOWNLOADS

MAPPING FILES

Select a Target environment to download user and group mapping files used during Device/Share ReACL.

DEMO1

DEVICE AGENT

Select a version of the device agent to download.

20.12.8.9999 (LATEST)

Service URL

https://extdev.odmad.dev.xcloud.ninja/api/ADM

Auth Key

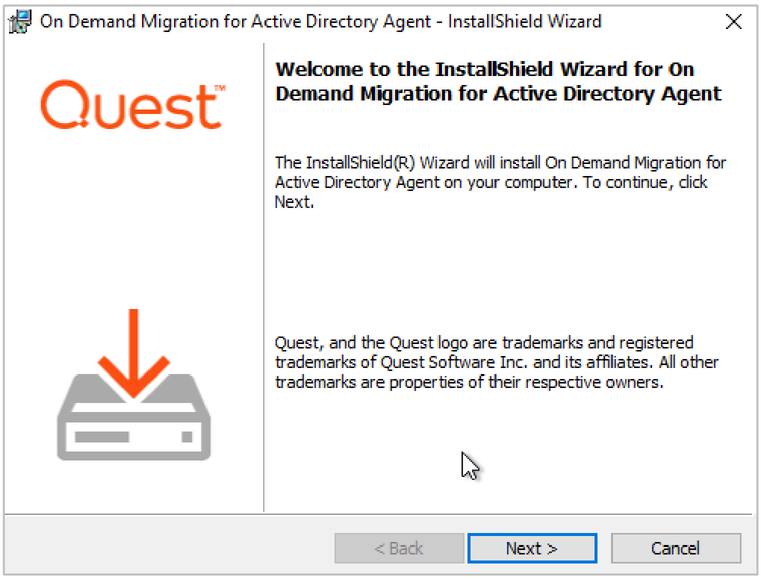
5d915498daae40459cb832270352523d470ef19f839548b480d84ddab35a1fa4

Perform automatic agent upgrades when a new agent version is available?

SQL RE-PERMISSION TOOL

Download the SQL Re-Permission Tool.

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.

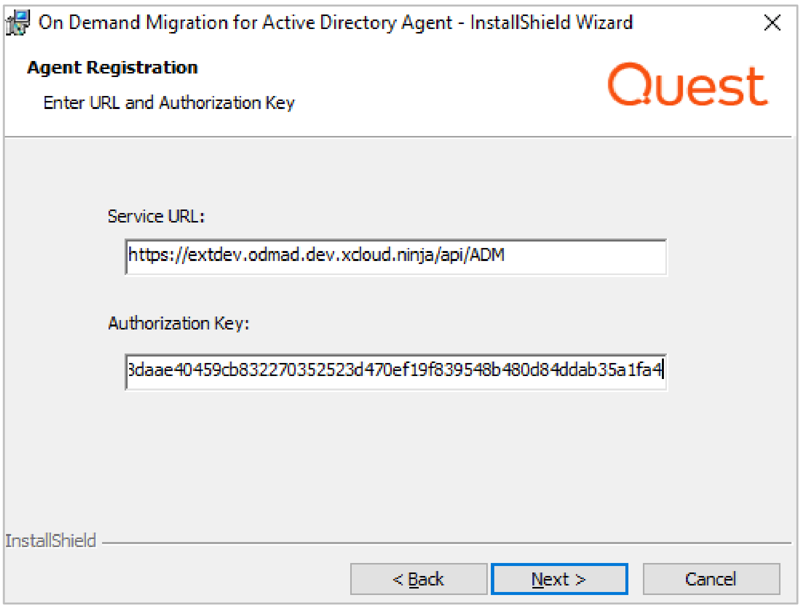


On Demand Migration for Active Directory Agent - InstallShield Wizard

Welcome to the InstallShield Wizard for On Demand Migration for Active Directory Agent

The InstallShield(R) Wizard will install On Demand Migration for Active Directory Agent on your computer. To continue, click Next.

Quest, and the Quest logo are trademarks and registered trademarks of Quest Software Inc. and its affiliates. All other trademarks are properties of their respective owners.



On Demand Migration for Active Directory Agent - InstallShield Wizard

Agent Registration

Enter URL and Authorization Key

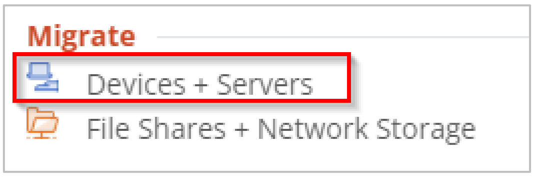
Service URL:

https://extdev.odmad.dev.xcloud.ninja/api/ADM

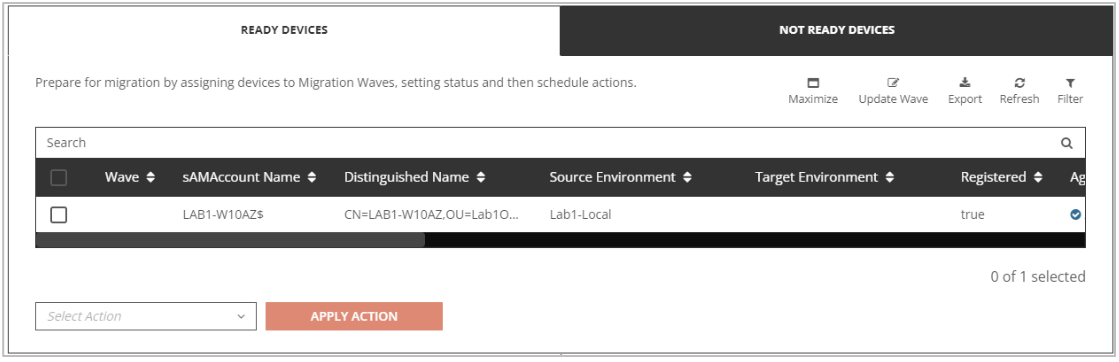
Authorization Key:

3daae40459cb832270352523d470ef19f839548b480d84ddab35a1fa4

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.



READY DEVICES | NOT READY DEVICES

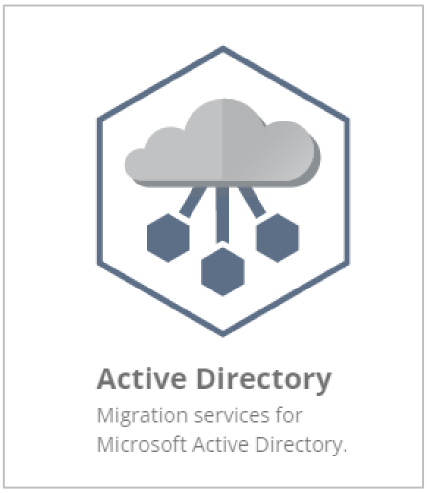
Prepare for migration by assigning devices to Migration Waves, setting status and then schedule actions.

□	Wave	sAMAccount Name	Distinguished Name	Source Environment	Target Environment	Registered	Ag
□		LAB1-W10AZ$	CN=LAB1-W10AZ,OU=Lab1O...	Lab1-Local		true	✓

0 of 1 selected

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

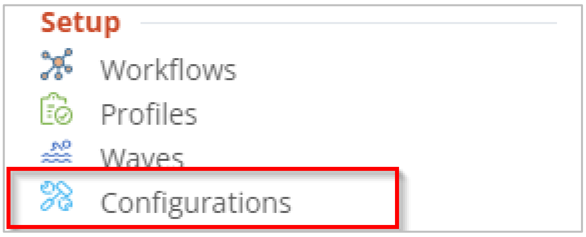
1. Log in to *On Demand.*
2. Navigate to *Migration,* select the project, and click on *Active Directory.*
3. Click on the *Active Directory* icon.



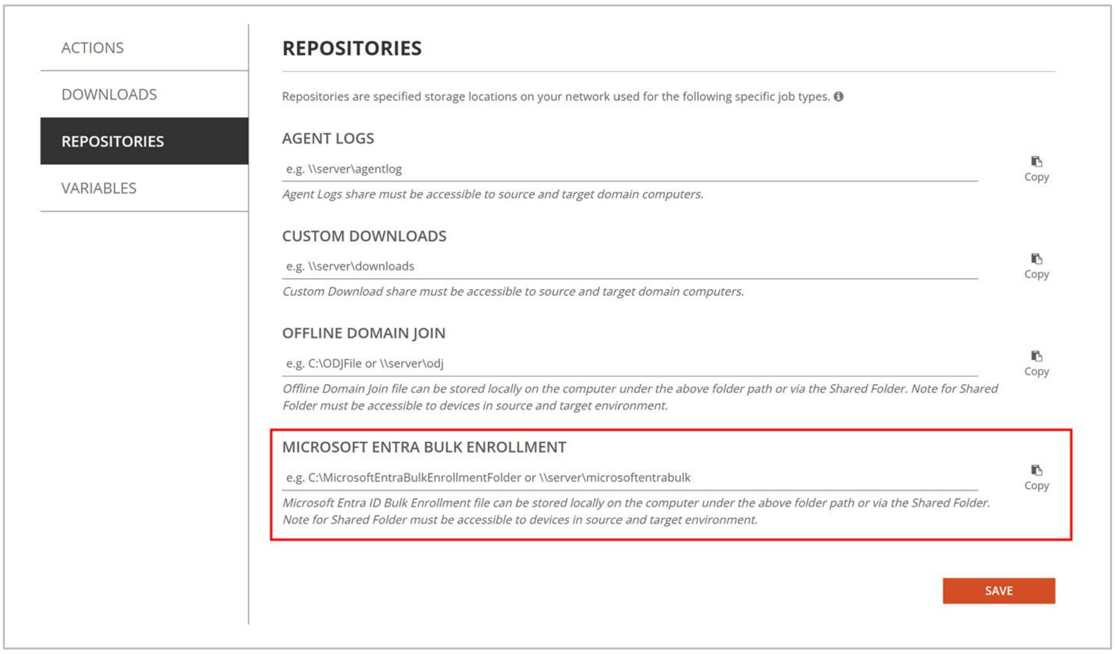
Active Directory

Migration services for Microsoft Active Directory.

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.*



REPOSITORIES

Repositories are specified storage locations on your network used for the following specific job types.

AGENT LOGS

e.g. \\server\agentlog

Agent Logs share must be accessible to source and target domain computers.

CUSTOM DOWNLOADS

e.g. \\server\downloads

Custom Download share must be accessible to source and target domain computers.

OFFLINE DOMAIN JOIN

e.g. C:\ODJFile or \\server\odj

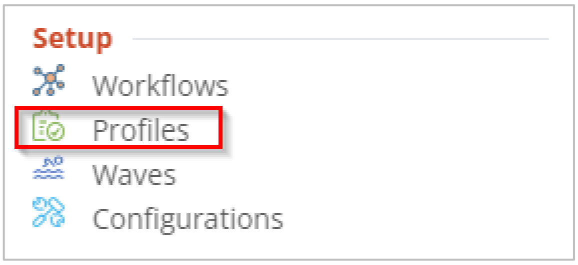
Offline Domain Join file can be stored locally on the computer under the above folder path or via the Shared Folder. Note for Shared Folder must be accessible to devices in source and target environment.

MICROSOFT ENTRA BULK ENROLLMENT

e.g. C:\MicrosoftEntraBulkEnrollmentFolder or \\server\microsoftentrabulk

Microsoft Entra ID Bulk Enrollment file can be stored locally on the computer under the above folder path or via the Shared Folder. Note for Shared Folder must be accessible to devices in source and target environment.

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.*

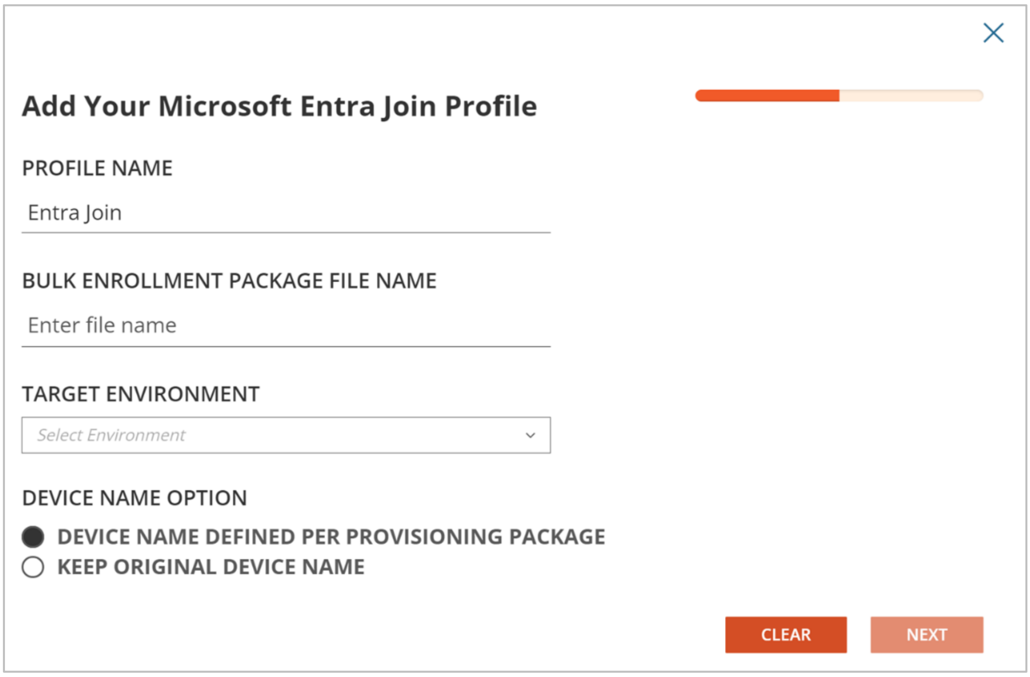
   a. Name of the Profile

   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

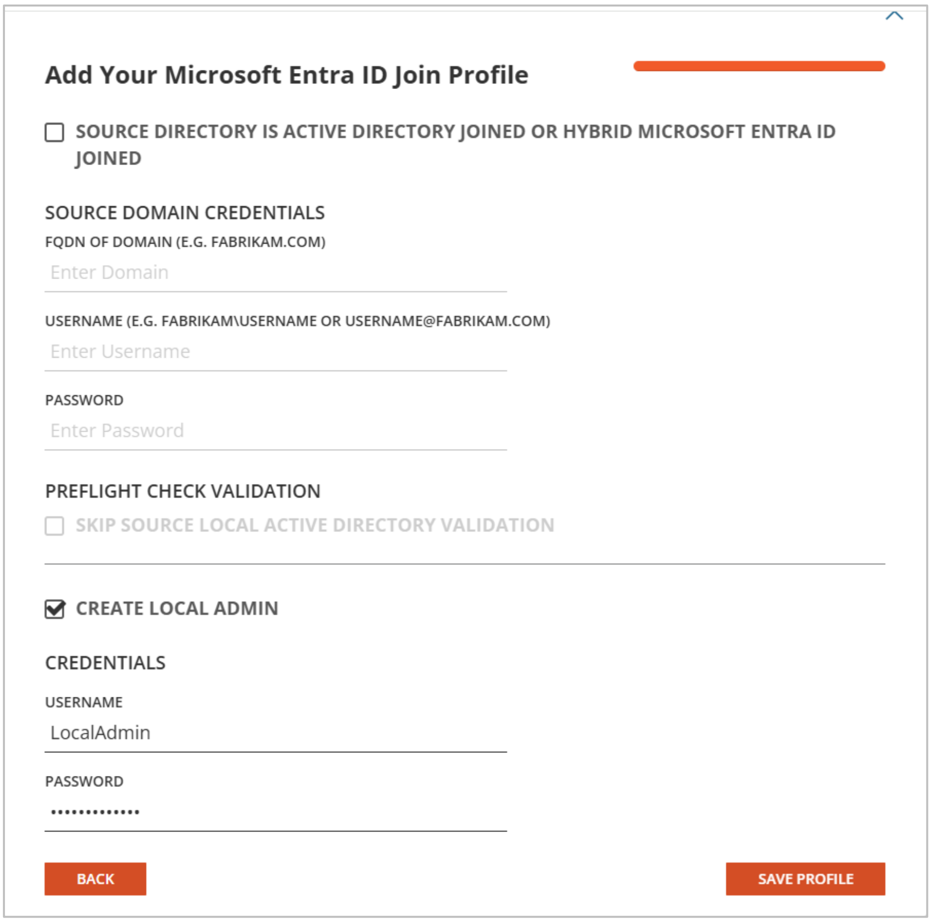
○ KEEP ORIGINAL DEVICE NAME

   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

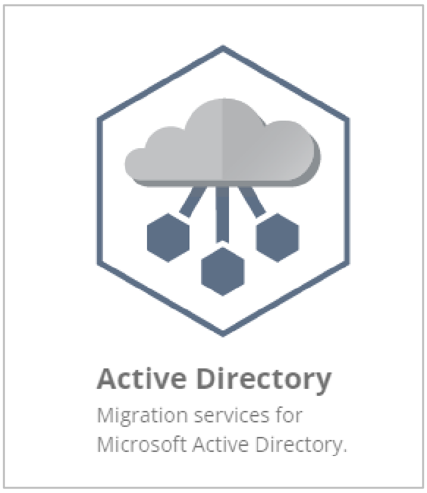
•••••••••••••

h. Click Save Profile

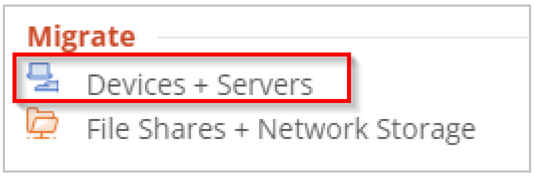
Perform Device Migration

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.

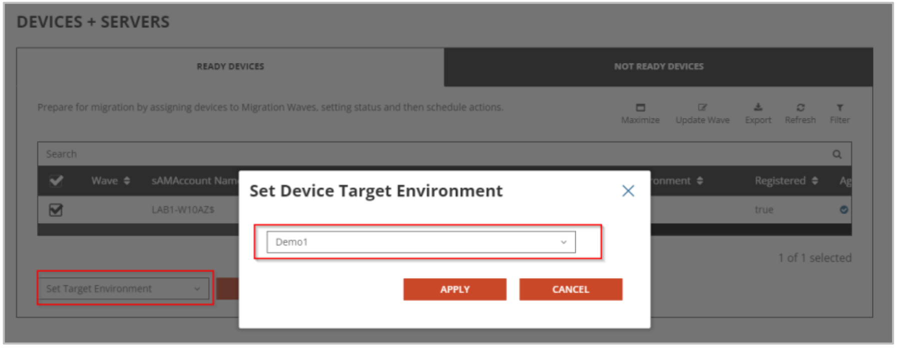


4. Via the hamburger menu, click on *Devices + Servers.*



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.*



Prepare for migration by assigning devices to Migration Waves, setting status and then schedule actions.

✓	Wave	sAMAccount Name	…onment	Registered	Ag…
☑		LAB1-W10AZ$		true	

1 of 1 selected

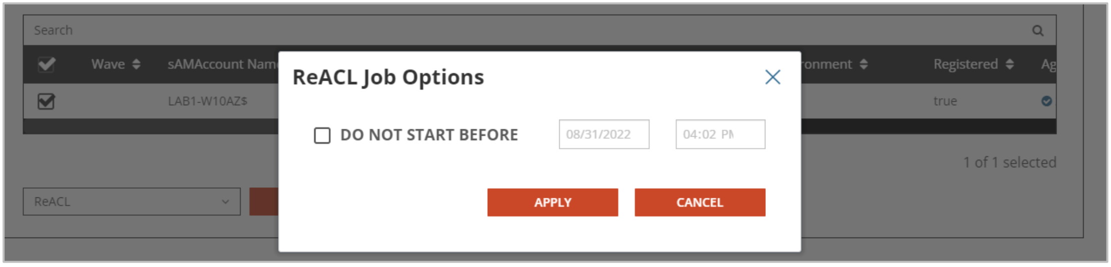
Set Target Environment

Set Device Target Environment

Demo1

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*.



✓	Wave	sAMAccount Nam…	…onment	Registered	Ag…
☑		LAB1-W10AZ$		true	

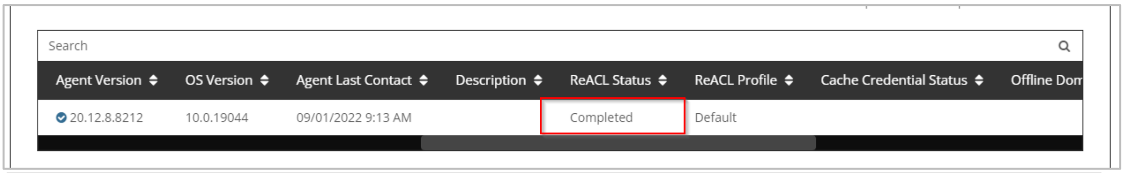
1 of 1 selected

ReACL

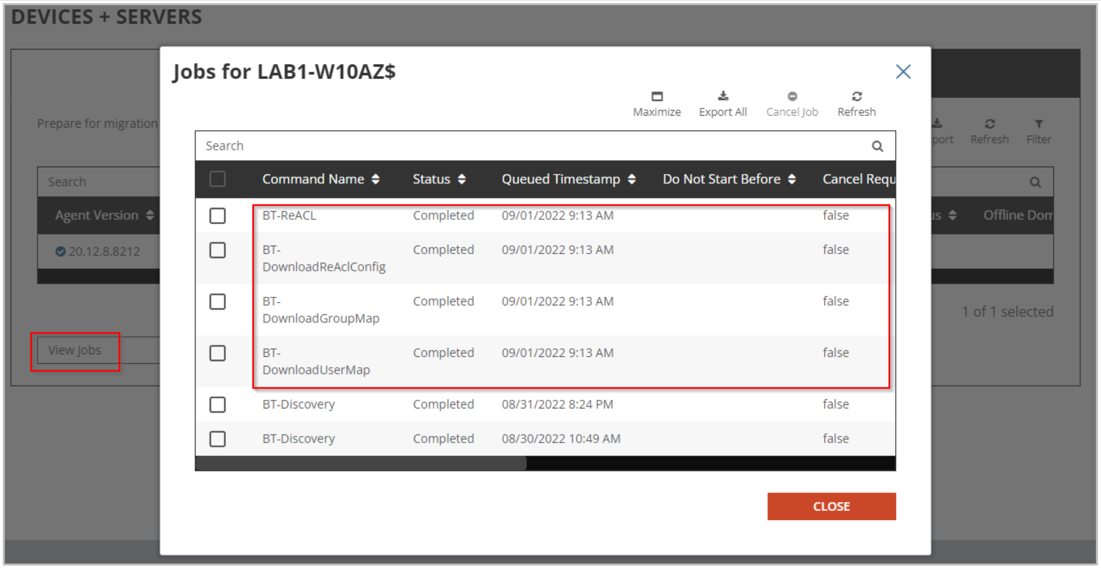
ReACL Job Options

□ DO NOT START BEFORE 08/31/2022 04:02 PM

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.



Agent Version	OS Version	Agent Last Contact	Description	ReACL Status	ReACL Profile	Cache Credential Status	Offline Dom…
20.12.8.8212	10.0.19044	09/01/2022 9:13 AM		Completed	Default		



Prepare for migration

Agent Version

20.12.8.8212

View Jobs

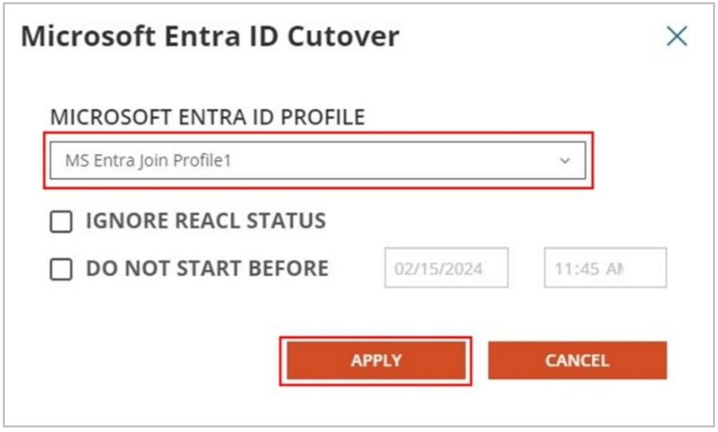
1 of 1 selected

Jobs for LAB1-W10AZ$

□	Command Name	Status	Queued Timestamp	Do Not Start Before	Cancel Requ…
□	BT-ReACL	Completed	09/01/2022 9:13 AM		false
□	BT-DownloadReAclConfig	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

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*.



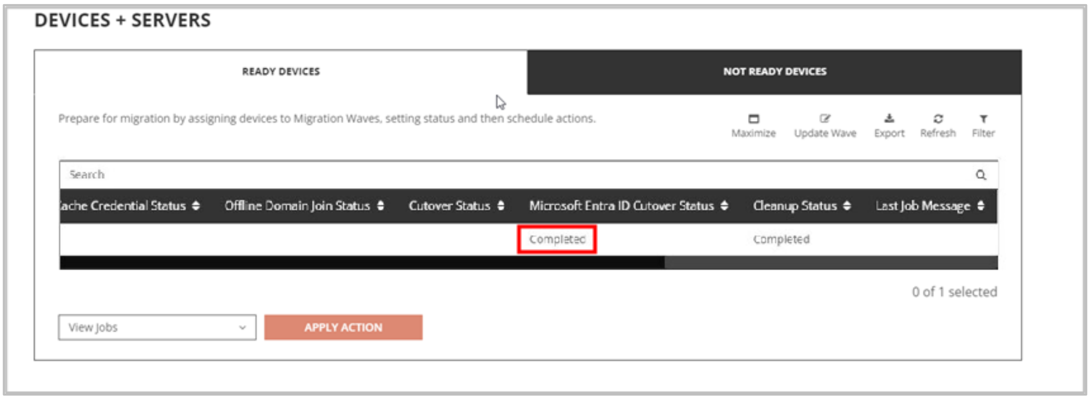
Microsoft Entra ID Cutover

MICROSOFT ENTRA ID PROFILE: MS Entra Join Profile1

□ IGNORE REACL STATUS

□ DO NOT START BEFORE 02/15/2024 11:45 AM

9. 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.



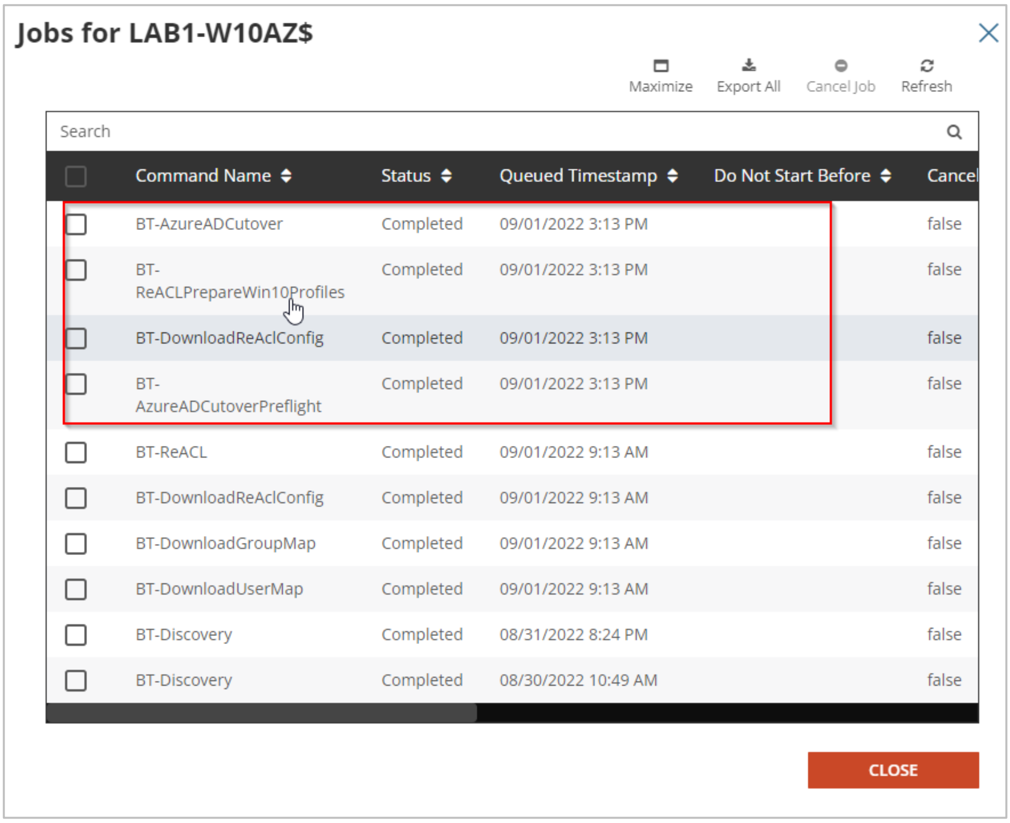
DEVICES + SERVERS

Prepare for migration by assigning devices to Migration Waves, setting status and then schedule actions.

ache Credential Status	Offline Domain Join Status	Cutover Status	Microsoft Entra ID Cutover Status	Cleanup Status	Last Job Message
			Completed	Completed	

0 of 1 selected

View Jobs



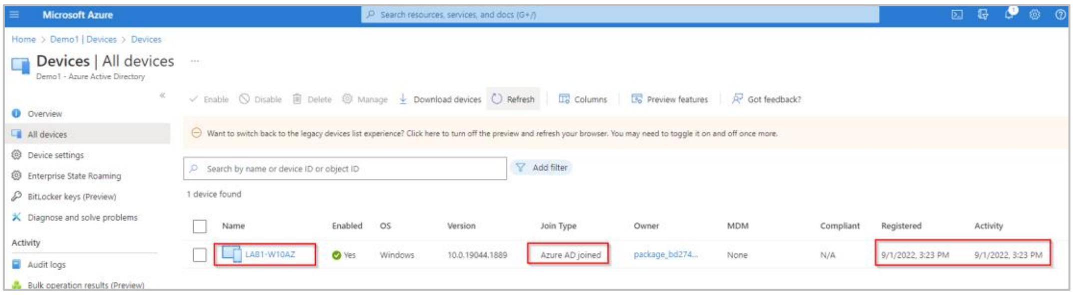
Jobs for LAB1-W10AZ$

□	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-DownloadReAclConfig	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-DownloadReAclConfig	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.

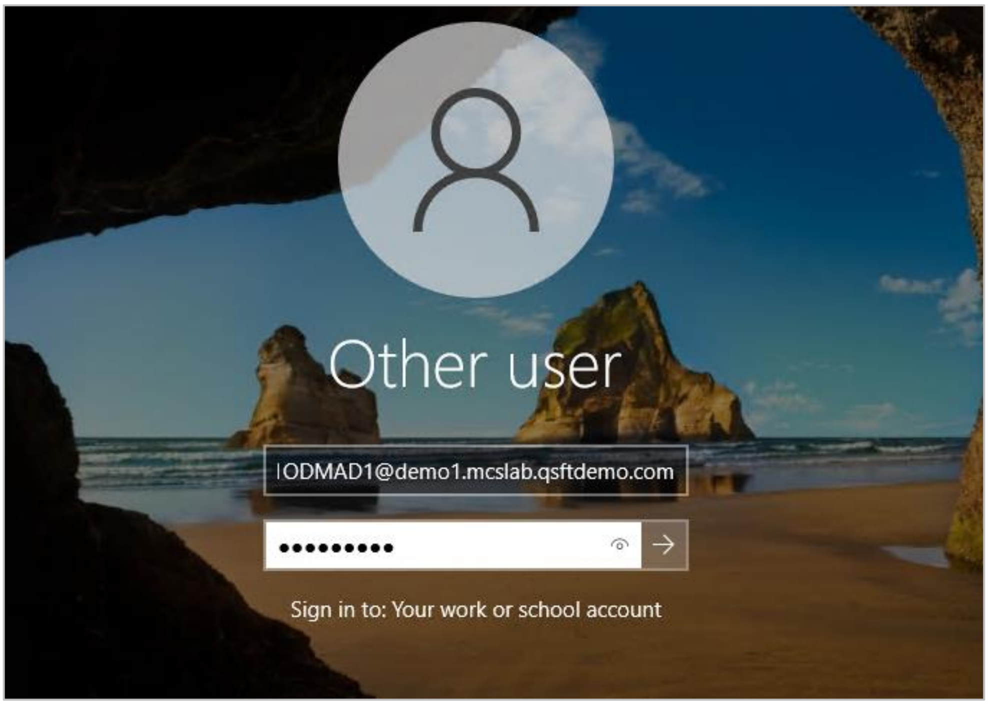


Want to switch back to the legacy devices list experience? Click here to turn off the preview and refresh your browser. You may need to toggle it on and off once more.

1 device found

□	Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant	Registered	Activity
□	LAB1-W10AZ	✓ Yes	Windows	10.0.19044.1889	Azure AD joined	package_bd274...	None	N/A	9/1/2022, 3:23 PM	9/1/2022, 3:23 PM

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



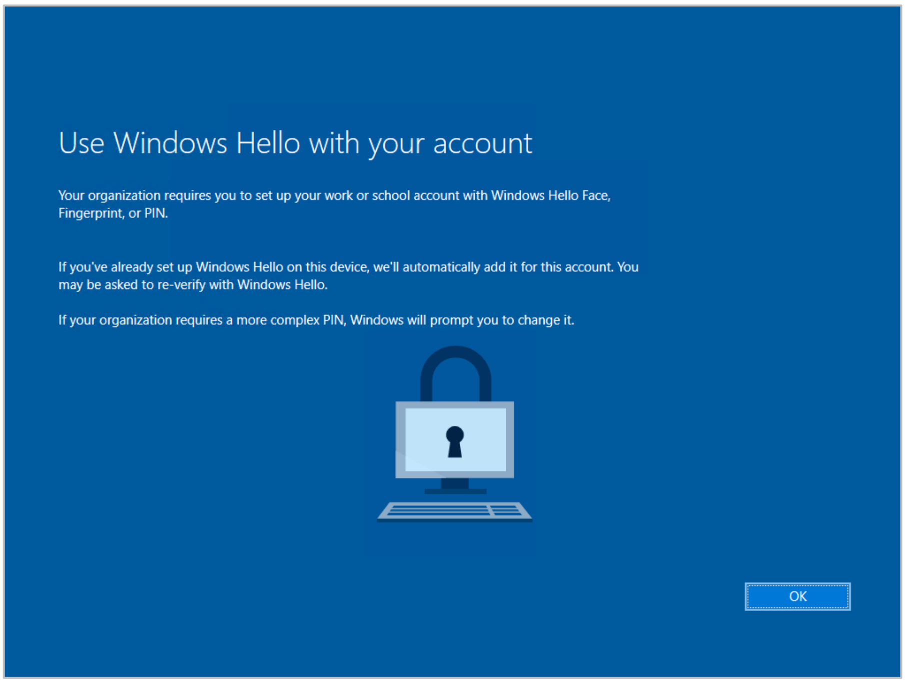
Other user

IODMAD1@demo1.mcslab.qsftdemo.com

●●●●●●●●●●

Sign in to: Your work or school account

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



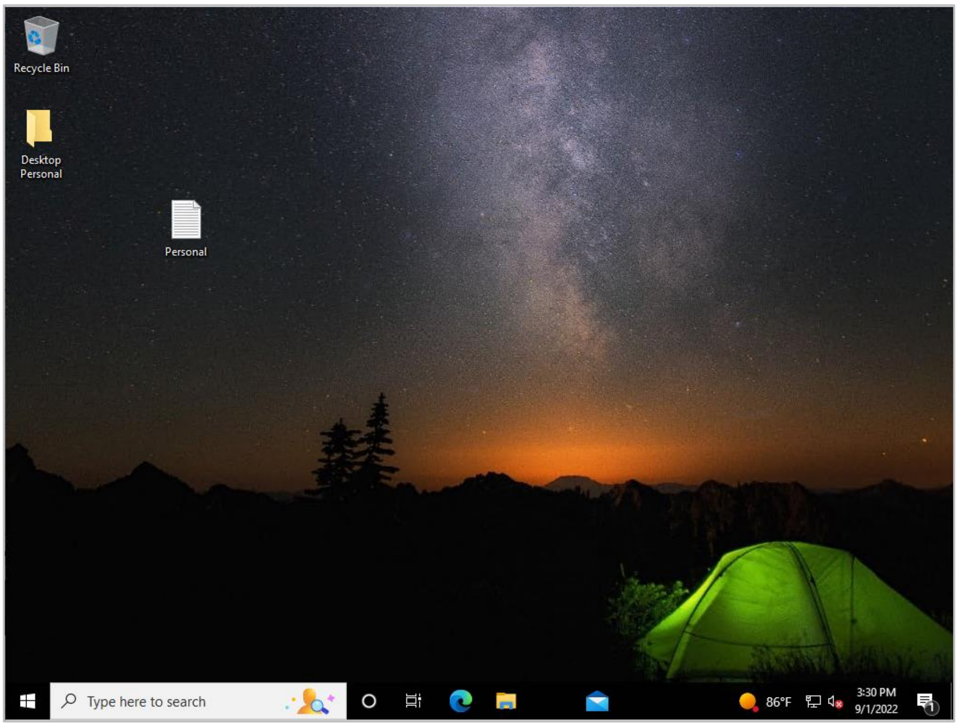
Use Windows Hello with your account

Your organization requires you to set up your work or school account with Windows Hello Face, Fingerprint, or PIN.

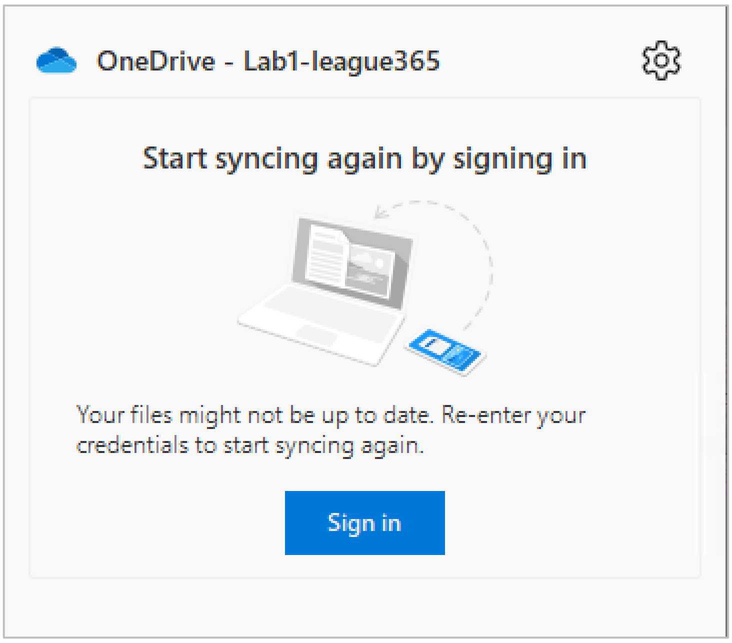
If you've already set up Windows Hello on this device, we'll automatically add it for this account. You may be asked to re-verify with Windows Hello.

If your organization requires a more complex PIN, Windows will prompt you to change it.

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*.



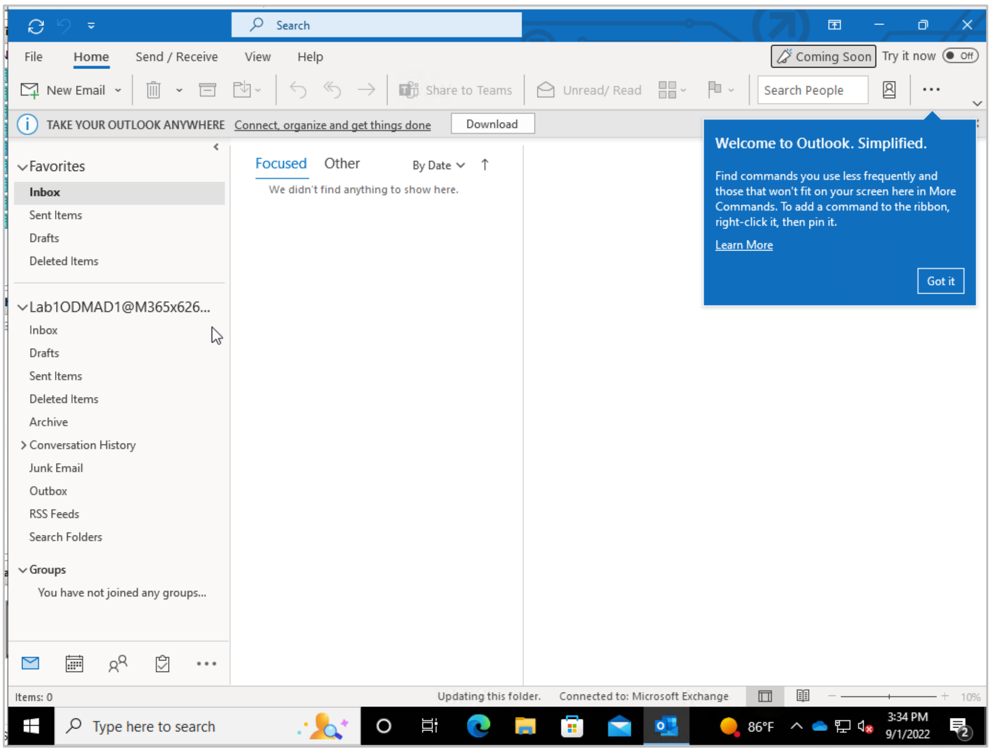
OneDrive - Lab1-league365

Start syncing again by signing in

Your files might not be up to date. Re-enter your credentials to start syncing again.

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.

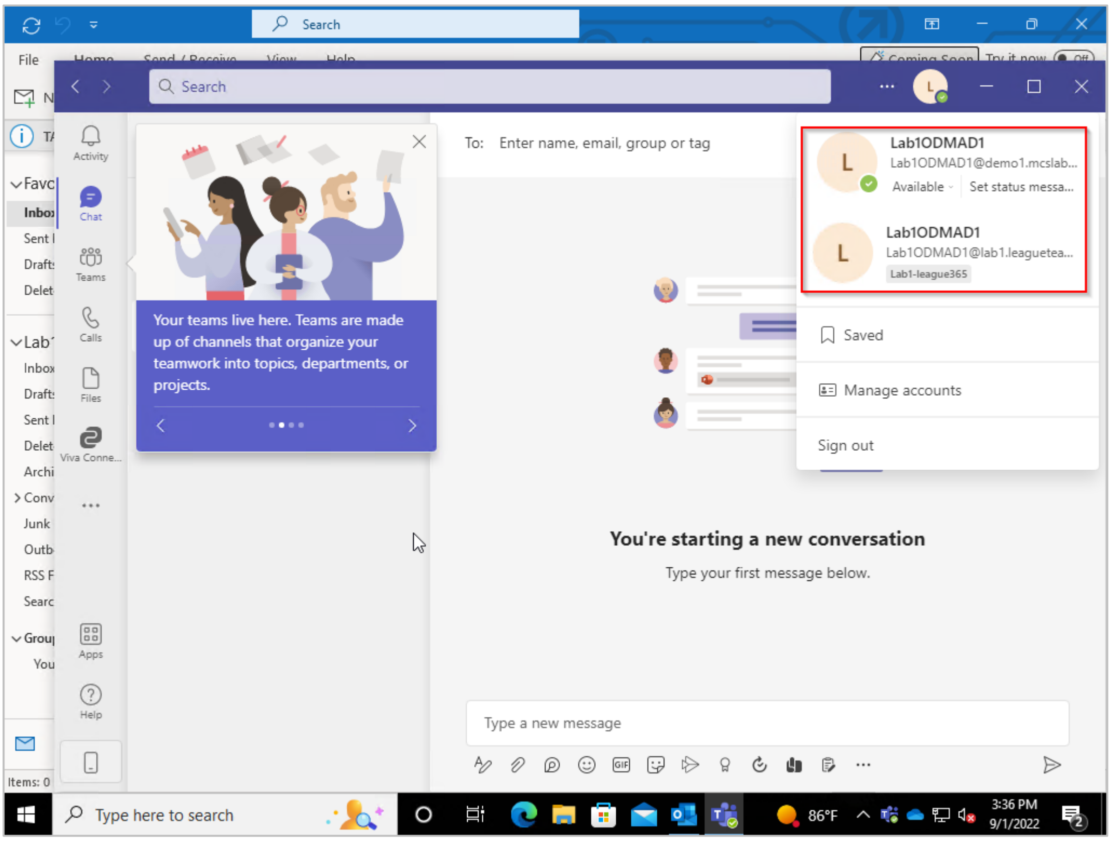


We didn't find anything to show here.

Welcome to Outlook. Simplified.

Find commands you use less frequently and those that won't fit on your screen here in More Commands. To add a command to the ribbon, right-click it, then pin it.

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.



Your teams live here. Teams are made up of channels that organize your teamwork into topics, departments, or projects.

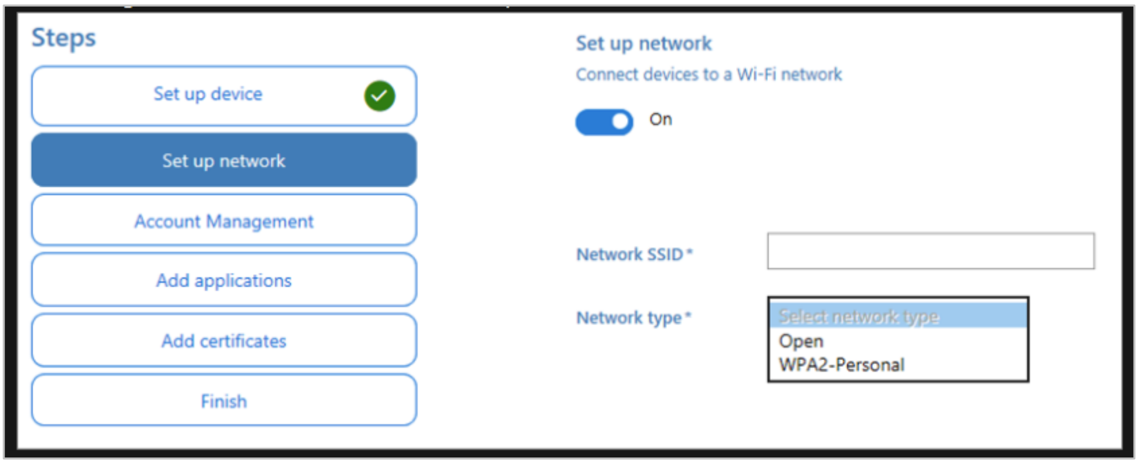
You're starting a new conversation

Type your first message below.

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.



Set up network

Connect devices to a Wi-Fi network

On

Network SSID *

Network type *

Select network type
Open
WPA2-Personal

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
- enablecredsspsupport:i:0
- username:s:Lab1ODMAD1@demo1.mcslab.qsftdemo.com
- domain:s:AzureAD

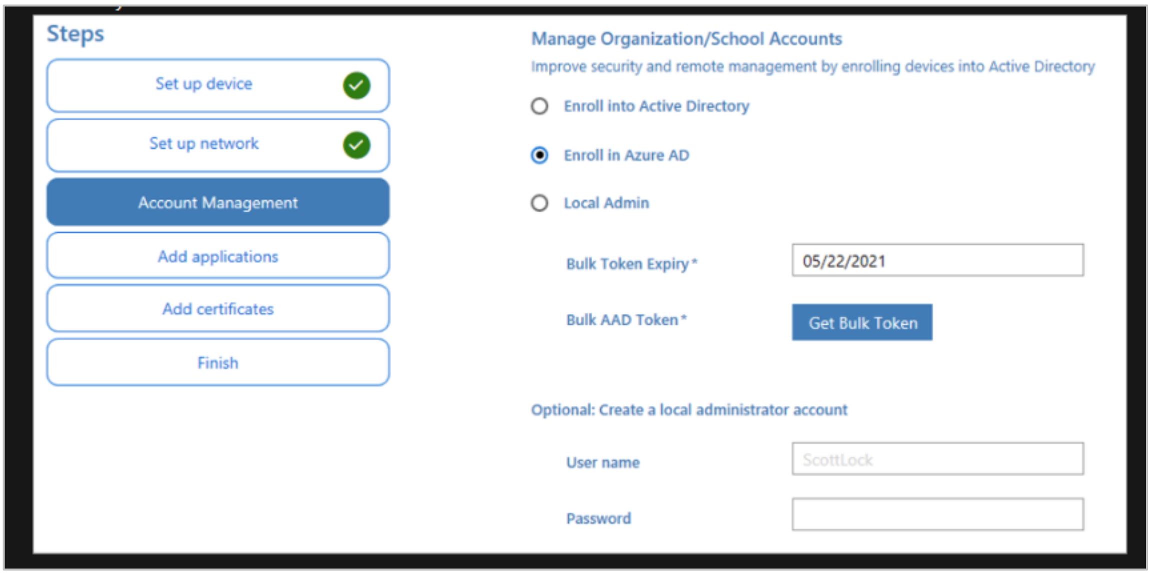
Additional information and instruction can be found at this Microsoft Soft Link Remote Desktop Connection for credentials - Windows Server | Microsoft Docs

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.



Steps

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

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* 05/22/2021

Bulk AAD Token* Get Bulk Token

Optional: Create a local administrator account

User name ScottLock

Password

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.

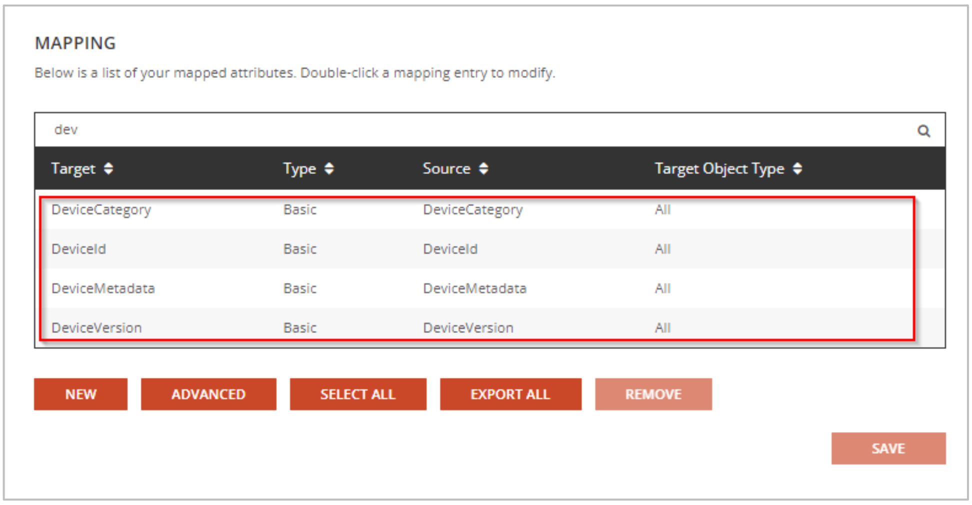
After my user devices are Microsoft Entra ID Joined to the target tenant, how can users switch their Microsoft Apps such as OneDrive, Teams, and

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.

dev

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

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"
}
```

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.