MIGRATION PLAYBOOK · IDENTITY

How to move from on-premises Active Directory to Microsoft Entra ID

Most organisations get to Entra ID in stages: sync identities, move sign-in to the cloud, move devices to Entra join, then shift management of users to the cloud. This guide covers each decision with the commands you will use.

Updated 4 Nov 2026 7 phases 31 detailed steps 12 official sources

START HERE

How do you move from on-premises Active Directory to Microsoft Entra ID?

SHORT ANSWER

This moves your users, sign-in, devices and apps from on-premises Active Directory (AD, the Windows Server directory) to Microsoft Entra ID (the cloud directory behind Microsoft 365). It is a change of where people are managed, not a data copy.

- **Recommended route:** Phased move: Cloud Sync with password hash sync, then Entra join and source of authority per user
- **Order:** Change one layer at a time, from the one everything else depends on: the directory copy first, then sign-in, then devices and apps, and only then who manages each user.
- **7 phases:** Get ready, Set up sync, Move sign-in to the cloud, Move devices, Move apps off AD, Hand users to the cloud and Turn off sync and retire AD.
- **You're done when:** Every user signs in through the Entra sign-in page, and no domain is still federated.

The recommended route copies users to the cloud with Microsoft Entra Cloud Sync (a small agent installed on your servers), moves sign-in to password hash sync (Entra ID checks a hash of each AD password, so users keep one password), Entra joins PCs (joins them to Entra ID instead of AD) as they are

reset or replaced, and then transfers source of authority for each user (Microsoft's name for handing that user's management from AD to Entra ID). It happens in stages, not in one weekend: your device refresh cycle and the apps that still need AD set the pace.

RECOMMENDED ROUTE

Phased move: Cloud Sync with password hash sync, then Entra join and source of authority per user

Microsoft recommends Cloud Sync for most organisations, password hash sync is the simplest sign-in, and users move one at a time with a rollback.

▼ Other options and when to use them

- **Stay hybrid on Microsoft Entra Cloud Sync**
  : AD will stay for a year or more. Stop after the sign-in phase.
- **Stay hybrid on Microsoft Entra Connect Sync**
  : You have groups over 50,000 members, more than 150,000 objects in a domain, complex sync rules, or hybrid joined devices that still need device sync.
- **Turn off directory sync for the whole tenant**
  : You are small, nothing authenticates to AD any more, and every user can go cloud-only at once.

TOOLS FOR THIS PLAN

Are you ready?
22-question readiness check

Plan your dates
Dated countdown you can add to your calendar

New to the jargon?
Plain-English migration glossary

ORDER TO MIGRATE IN, AND WHY

Change one layer at a time, from the one everything else depends on: the directory copy first, then sign-in, then devices and apps, and only then who manages each user. Every step keeps AD working as the fallback until the last one, which is the only step that is hard to undo.

1 **Clean up AD: stale accounts, duplicate and badly formatted attributes**
Everything in sync scope lands in Entra ID, and objects with bad values fail to sync. It is far easier to fix them before the first sync.

2 **Sync users and groups to Entra ID, with password hash sync turned on**
Cloud sign-in, Entra joined PCs and the final hand-over all need the users in Entra ID first. Password hash sync is also the fallback sign-in if AD FS fails.

3 **Move sign-in to the cloud: pilot group, then one domain at a time**

Microsoft requires users to stop signing in through AD FS before their management can move, and a pilot shows sign-in problems before a whole domain changes.

4 **Entra join PCs at their normal reset or replacement**

There is no supported in-place conversion, so this step follows your hardware refresh. Hybrid joined PCs keep working meanwhile.

5 **Move or replace apps that use LDAP or Kerberos with a password**

Users of these apps cannot move to cloud management, so their apps decide when they can move.

6 **Finish any Exchange Server to Exchange Online move**

Microsoft lists no on-premises Exchange workloads as a prerequisite for transferring source of authority.

7 **Transfer source of authority per user: pilot first, then groups of users**

Each transfer can be rolled back for that one user, so problems stay small.

8 **Turn off directory sync, then retire AD FS, sync servers and domain controllers**

Turning off sync is tenant-wide and cannot be reversed for 72 hours, and a demoted forest only comes back from backup. So it goes last.

SETTINGS CHECKLIST: DECIDE THESE BEFORE YOU COPY

Built-in and third-party tools treat these differently. Tick each one off once you have decided.

Download this checklist (Excel)

☐ **Sync engine: Cloud Sync or Connect Sync**

Which Microsoft sync tool copies users from AD to Entra ID during the move.

▼ How each tool handles it

Built-in method	Microsoft calls Cloud Sync the recommended path for most organisations. Cloud Sync does not support groups over 50,000 members, more than 150,000 objects per domain, or device sync for hybrid join. Connect Sync supports these but needs a dedicated server and a sync cycle at least every 7 days.

Tip: If you still hybrid join new PCs, stay on Connect Sync until they are all Entra joined, then switch.

Microsoft Learn: Microsoft Entra Cloud Sync migration decision guide

- [ ] **Sync scope**
  Which OUs (AD folders), users, groups and contacts sync, and which stale accounts to disable or delete first.

  ▼ **How each tool handles it**

Built-in method	Both Cloud Sync and Connect Sync copy everything in the OUs you scope, including disabled and test accounts. Neither cleans up AD for you.

  Tip: Scope to the OUs that hold real people and groups, and move service and test accounts out of them.

  Microsoft Learn: Microsoft Entra Cloud Sync migration decision guide

- [ ] **Duplicate and badly formatted attributes**
  Who fixes duplicate or malformed mail, proxyAddresses and userPrincipalName values, and by when.

  ▼ **How each tool handles it**

Built-in method	Microsoft requires these values to be unique. Connect Sync and Cloud Sync do not fix them: the affected objects report errors and stay out of sync until you fix them in AD.
IdFix	Free Microsoft tool that lists duplicate and malformed attributes before sync, so you can fix them in bulk.

  Tip: Fix values in AD, not in the cloud, and rerun the scan before every widening of scope.

  Microsoft Learn: Synchronize domain users to Microsoft 365

- [ ] **Sign-in method**
  Password hash sync, pass-through authentication (Entra ID checks each password against AD through an agent) or keeping AD FS.

  ▼ **How each tool handles it**

Built-in method	Microsoft recommends turning on password hash sync whatever method you pick, because it is the fallback if AD or AD FS fails. Failover to it is manual.

  Tip: Turn password hash sync on now, even if AD FS stays for a while, and write the failover steps into your rollback plan.

  Microsoft Learn: Authentication for Microsoft Entra hybrid identity solutions

- [ ] **Pilot groups for staged rollout**
  Which users test cloud sign-in first, and in which groups.

▼ How each tool handles it

Built-in method Staged rollout accepts up to 10 groups per feature, no nested or dynamic groups, and 200 users or fewer in a new group when you first add it.

Tip: Create plain cloud security groups for each wave, with directly added members.

Microsoft Learn: Migrate to cloud authentication using Staged Rollout

- [ ] **Legacy sign-in clients**

Which scanners, printers and old apps that sign in with POP3 or SMTP must change before AD FS goes.

▼ How each tool handles it

Built-in method Staged rollout does not cover legacy authentication: those clients keep signing in through federation until the domain converts.

Tip: Filter the Entra sign-in logs by client app for legacy clients, and move each one to modern authentication first.

Microsoft Learn: Migrate to cloud authentication using Staged Rollout

- [ ] **Domain conversion window**

When each federated domain switches to cloud sign-in, and in what order.

▼ How each tool handles it

Built-in method Converting a domain from federated to managed affects every user on it at once. Microsoft says it can take up to 60 minutes, and new browser sign-ins may not prompt during that time.

Tip: Convert the smallest or a test domain first, out of business hours, and keep AD FS until every domain is done.

Microsoft Learn: Migrate from federation to cloud authentication

- [ ] **Device join type**

Which PCs stay hybrid joined (joined to both AD and Entra ID) for now, and when each is reset to Entra join.

▼ How each tool handles it

Built-in method Microsoft has no supported way to turn a hybrid joined PC into an Entra joined one without a Windows reset. Hybrid joined PCs need regular network contact with a domain controller.

Quest On Demand Migration	Converts domain joined or hybrid joined Windows 10 and 11 PCs to Entra joined and keeps user profiles. Not Microsoft supported, so pilot each model.
ForensiT User Profile Wizard	Moves the existing domain profile to the user's Entra ID account. The join itself uses a provisioning package.

Tip: Put the reset date for each PC in your device list, and keep VPN in place for remote hybrid joined PCs until then.

Microsoft Learn: Join your cloud-native endpoints to Microsoft Entra

- [ ] **Group Policy settings**

Which Group Policy settings Entra joined PCs still need, and how Intune will apply them instead.

▼ How each tool handles it

Built-in method	Entra joined PCs are not in AD, so Group Policy does not reach them. Settings must be rebuilt as Intune policies.

Tip: Import your GPO reports into Intune Group Policy analytics to see which settings have a cloud equivalent, and rebuild only those you still need.

Microsoft Learn: Join your cloud-native endpoints to Microsoft Entra

- [ ] **File shares and printers**

Whether on-premises shares and printers stay, and how Entra joined PCs reach them.

▼ How each tool handles it

Built-in method	Microsoft says Entra joined PCs can open on-premises resources with single sign-on, as long as the PC can reach a domain controller.

Tip: Test a share by path and a network printer on an Entra joined pilot PC, on site and over VPN.

Microsoft Learn: Join your cloud-native endpoints to Microsoft Entra

- [ ] **Apps that need AD**

For each app that uses LDAP, Kerberos or AD FS: move it to Entra ID, upgrade it, replace it, or keep its users on AD.

▼ How each tool handles it

Built-in method	Microsoft says users of apps that need password-based LDAP bind or Kerberos with a password cannot move to cloud management.

Tip: Give each app an owner and a date in your application inventory, because the last app sets the date AD can go.

Microsoft Learn: Configure user Source of Authority

- [ ] **Source of authority transfer**

Which users move to cloud management first, and the prerequisites each must meet.

▼ How each tool handles it

Built-in method	Transfer is per user through Microsoft Graph and can be rolled back per user. It needs Connect Sync 2.5.76.0 or Cloud Sync agent 1.1.1370.0 or later, no on-premises Exchange workloads and no AD FS sign-in for those users. Microsoft lists Entra ID Free as the licence.

Tip: Start with a few pilot users and check the audit log entry and that each one is editable in the Entra admin center.

Microsoft Learn: Configure user Source of Authority

- [ ] **Turning off directory sync**

Whether you turn sync off for the whole tenant at the end, and who approves it.

▼ How each tool handles it

Built-in method	Turning off directory sync is tenant-wide, clears on-premises properties, and cannot be turned back on for 72 hours.

Tip: Do it only after every user has moved and the sync client is uninstalled, never as a troubleshooting step.

Microsoft Learn: Turn off directory synchronization for Microsoft 365

- [ ] **Service accounts and last domain controller**

What still logs on to AD, and what evidence you need before demoting the last domain controller.

▼ How each tool handles it

Built-in method	Once the last domain controller is demoted, only a system state backup can bring the forest back.

Tip: Review logon events (4624) across a full business cycle, including month-end and year-end jobs, before you demote.

THE PLAN, PHASE BY PHASE

1 Get ready

Before you change anything

Count users, groups, contacts and computers per domain, and note the 20 largest groups.

List every app with its owner and sign-in method (LDAP, Kerberos, AD FS or other).

List PCs by Windows version, and every Group

Policy object (GPO, a set of AD-managed PC settings).

If you run AD FS (on-premises federation servers), back up the Microsoft 365 relying party trust.

Disable or delete stale accounts and groups in AD so they do not sync.

Watch out: Duplicate or badly formatted mail, proxyAddresses or userPrincipalName values stop those objects syncing.

WAYS AROUND IT

- Fix the values in AD, not in the cloud, and rerun the scan until it is clean.

TOOLS THAT CAN DO IT

IdFix
Free Microsoft tool that lists duplicate and malformed attributes before sync, so you can fix them in bulk.

Show the detailed steps (4) →

2 Set up sync

Check your counts against the Cloud Sync limits below, and choose Cloud Sync unless one is hit.

Install the Cloud Sync agent on two domain-joined servers,

so one takes over if the other fails.

Scope sync to the OUs (AD folders) that hold real users, groups and contacts.

If you keep Connect Sync, pause its scheduler while you change settings, then turn it back on.

Watch out: Cloud Sync does not support groups over 50,000 members, more than 150,000 objects per domain, or device sync for hybrid join.

WAYS AROUND IT

- Stay on Connect Sync until the blocker is gone, for example until devices are Entra joined.

Watch out: Connect Sync only: Microsoft says a sync cycle must complete at least once every 7 days, so a long pause is not safe.

WAYS AROUND IT

- Pause the scheduler only for a change window, and check it with Get-ADSyncScheduler.

Show the detailed steps (5) →

3 Move sign-in to the cloud

Turn on password hash sync (Entra ID checks a hash of each AD password), even if AD FS stays for now.

Save your current

federation settings for each domain with your rollback plan.

Pilot cloud sign-in with staged rollout (cloud sign-in for chosen groups only) for a cloud security group of 200 users or fewer.

Convert the smallest federated domain (signing in through

AD FS) to managed (cloud sign-in) first, out of business hours.

Check pilot users can sign in at myapps.microsoft.com on and off the office network.

> **Watch out:** Staged rollout does not accept nested or dynamic groups, and allows up to 10 groups per feature.
>
> **WAYS AROUND IT**
>
> - Create plain cloud security groups for each pilot wave.

> **Watch out:** Legacy sign-in such as POP3 and SMTP ignores staged rollout, so scanners and old apps can break when AD FS goes.
>
> **WAYS AROUND IT**
>
> - Find legacy clients in the Entra sign-in logs and move them to modern authentication before converting domains.

> **Watch out:** Converting a domain from federated to managed affects every user on it at once, and Microsoft says it can take up to 60 minutes.

WAYS AROUND IT

- Convert one domain at a time, test domain first, and keep AD FS until all are done.

Show the detailed steps (4) →

4 Move devices

At each PC's normal reset or replacement

Register new PCs with Windows Autopilot and use a profile that Entra joins them.

Give every hybrid joined PC (joined to both AD and Entra ID) a reset or replacement date.

Keep VPN

in place for remote hybrid joined PCs until they are reset.

Test a file share and a network printer on an Entra joined pilot PC.

> **Watch out:** Microsoft has no supported way to turn a hybrid joined PC into an Entra joined one without a Windows reset.
>
> **WAYS AROUND IT**
>
> - Reset or replace PCs on their normal refresh cycle, using Autopilot.
>
> **TOOLS THAT CAN DO IT**
>
> **Quest On Demand Migration**
> Converts domain joined or hybrid joined Windows 10 and 11 PCs to Entra joined and keeps user profiles. Not Microsoft supported, so pilot each model.
>
> **ForensiT User Profile Wizard**
> Moves the existing domain profile to the user's Entra ID account. The join itself uses a provisioning package.

> **Watch out:** Microsoft says hybrid joined PCs become unusable without regular line of sight (network contact) to a domain controller.

WAYS AROUND IT

- Keep VPN or office connectivity for those PCs until each is Entra joined.

Show the detailed steps (4) →

5 Move apps off AD

Add each AD FS app to Entra ID as an enterprise app, then remove its AD FS relying party.

Use Windows Hello for Business with cloud Kerberos trust for apps that still need Kerberos.

Give each app that uses LDAP passwords a replacement or upgrade date.

> **Watch out:** Users of apps that need password-based LDAP bind or Kerberos with a password cannot move to cloud management.
>
> **WAYS AROUND IT**
>
> - Leave those users on AD until their apps are replaced or modernised.

Show the detailed steps (3) →

6 Hand users to the cloud

Finish any Exchange mailbox move and retire on-premises Exchange workloads first.

Upgrade Connect Sync to 2.5.76.0 or the

Cloud Sync agent to 1.1.1370.0 or later.

Transfer source of authority (which directory manages the user) for a few pilot users through Microsoft Graph.

Check the audit log entry and that each user is editable in the Entra admin center.

Move the remaining users in groups, once their apps and devices are clear.

> **Watch out:** The transfer needs no on-premises Exchange workloads and no AD FS sign-in for those users.
>
> **WAYS AROUND IT**
>
> - Complete the Exchange to Exchange Online move and the domain conversion before this phase.

> **Watch out:** Source of authority transfer (handing a user's management from AD to Entra ID) is a newer Microsoft feature.
>
> **WAYS AROUND IT**
>
> - Check its release status on Microsoft Learn before production use, and keep the per-user rollback steps handy.

Show the detailed steps (6) →

7 Turn off sync and retire AD

When nothing depends on AD

Review domain controller logons (event 4624) across a full business cycle,

including month-end jobs.

Uninstall Connect Sync or the Cloud Sync agents, then turn off directory sync for the tenant.

Take a system state backup of a domain controller and keep it per your records policy.

Remove AD FS and

WAP servers, then the sync servers, then demote the domain controllers.

> **Watch out:** Turning off directory sync applies to the whole tenant. You must wait 72 hours to turn it back on, and on-premises properties are cleared.
>
> **WAYS AROUND IT**
>
> - Do it last, after per-user transfers, and never as a troubleshooting step.

> **Watch out:** Once the last domain controller is demoted, only the system state backup can bring the forest back.
>
> **WAYS AROUND IT**
>
> - Keep the backup, and record who approved each step that cannot be undone.

Show the detailed steps (2) →

You are finished when

- Every user signs in through the Entra sign-in page, and no domain is still federated.
- Every PC shows AzureAdJoined YES and DomainJoined NO in dsregcmd /status.
- Every user shows isCloudManaged true (managed in Entra ID, not AD), or directory sync is off for the tenant.
- Domain controller logs show no logons from users, services or computers before the last one is demoted.

Tools named in this plan are independent third-party products, not endorsed by the platform vendor and not paid placements. Check the tool's own documentation and run a pilot first.

CLICK BY CLICK

What does each step involve?

Open a part when you reach it in the plan. Each step says where to go, what to do and what you should see.

About this migration

What it covers, limits at a glance

Moving identity off Active Directory is rarely a single cutover. Users, sign-in, devices and applications each move on their own timeline. A typical path is: sync users with Entra Connect Sync or Cloud Sync, use cloud authentication (password hash sync), Entra join new devices through Intune and Autopilot, move apps that need LDAP or Kerberos, and finally make Entra ID the source of authority for users.

If you are also moving mail, finish the mailbox move first: Microsoft says user SOA transfer requires that you have no on-premises Exchange workloads. See Exchange to Exchange Online.

SYNC OPTIONS
Microsoft Entra Connect Sync or Microsoft Entra Cloud Sync. Microsoft calls Cloud Sync the recommended path forward for most organisations

SIGN-IN
Password hash sync, pass-through authentication or federation. Microsoft says enable password hash sync whichever you choose

DEVICES
Microsoft recommends Entra join for new and reset Windows devices. Hybrid join cannot be converted without a reset

CLOUD-ONLY USERS
Transfer user source of authority (SOA) per object, or turn off directory sync for the whole tenant

LICENCE FOR SOA
Microsoft Entra Free, per Microsoft Learn

1 What you need before step one

Need	Details	Where to get it
Hybrid Identity Administrator in Microsoft Entra ID	To install sync agents, turn on staged rollout and check Entra Connect status.	Microsoft Entra admin center, https://entra.microsoft.com
Hybrid Administrator, plus Application Administrator or Cloud Application Administrator	Hybrid Administrator calls the source of authority (SOA) APIs. One of the application roles grants consent to the Graph permission.	Microsoft Entra admin center, Roles and administrators
Enterprise Admin or Domain Admin in Active Directory	For Connect Sync setup, the Cloud Sync agent service account and the seamless SSO computer account.	Your AD forest
Admin PC with the Active Directory and Group Policy PowerShell modules	Install the Remote Server Administration Tools (RSAT) for Active Directory on a domain-joined Windows PC.	Windows Settings, Optional features (RSAT)
Microsoft Graph PowerShell	For domain conversion, SOA transfer and turning off sync.	Install Microsoft Graph PowerShell and connect
A sync server or agent server	An existing Connect Sync server, or a domain-joined Windows Server for Connect Sync or Cloud Sync agents.	Install Microsoft Entra Connect Sync, or the Cloud Sync steps in Step 2
Intune and Entra licences for device and policy work	Entra join with Intune and Autopilot needs Intune licensing. Check Microsoft's current licensing pages.	Microsoft 365 admin center, Billing

2 Assess what depends on AD

4 steps –

1

Inventory identities

Where: Windows PowerShell on a domain-joined admin PC with the Active Directory module, then your Identity and licence mapping sheet

Count users, groups, contacts, service accounts and computers per domain and forest. Run the commands once per domain, adding `-Server contoso.com` to each command for other domains. Note large groups: Cloud Sync supports groups up to 50,000 members, Connect Sync supports larger ones. Record the counts and the largest groups in the mapping sheet.

```
Get-ADForest | Select-Object -ExpandProperty Domains
(Get-ADUser -Filter *).Count
(Get-ADGroup -Filter *).Count
(Get-ADComputer -Filter *).Count
(Get-ADObject -Filter 'objectClass -eq "contact"').Count
Get-ADGroup -Filter * -Properties member | Select-Object Name, @{n='Members';e={$_.member.Count}}
| Sort-Object Members -Descending | Select-Object -First 20
```

✓ **You should see:** The first command lists every domain in the forest, the next four each return a number, and the last lists the 20 largest groups with their member counts.

2

Inventory AD-dependent apps

Where: Your Application inventory and dependency map, filled in with each app owner

Add one row per app with columns for app name, owner, server, sign-in method (LDAP bind, Kerberos, NTLM, AD FS or other) and number of users. Microsoft says users can't move to cloud SOA if they still use apps needing password-based LDAP bind or Kerberos with a password, so mark those rows clearly.

✓ **You should see:** Every app in use has an owner and a sign-in method recorded, and the LDAP and Kerberos apps are flagged.

3

Inventory devices and policy

Where: Windows PowerShell on the same admin PC, with the Active Directory and Group Policy modules

List domain-joined PCs and servers by operating system, and list every Group Policy object. Add your imaging tools to the sheet. Hybrid join is the right fit only if you still need Group Policy, existing imaging or Win32 apps that rely on AD machine authentication.

```
Get-ADComputer -Filter * -Properties OperatingSystem | Group-Object OperatingSystem | Select-Object Count, Name
Get-GPO -All | Select-Object DisplayName, GpoStatus, ModificationTime
```

✓ **You should see:** A count of computers per operating system, then a list of GPOs with their status and last change date.

4

Inventory federation

Where: Windows PowerShell run as administrator on the primary AD FS server

If you run AD FS, list relying parties and back up the Microsoft 365 relying party trust and its claims rules, as Microsoft recommends before changing sign-in. If you use a third-party IdP, export its list of connected apps from its own admin console. These need a plan before you change sign-in.

```
Get-AdfsRelyingPartyTrust | Select-Object Name, Enabled, Identifier
(Get-AdfsRelyingPartyTrust -Name "Microsoft Office 365 Identity Platform") | Export-CliXML "C:\temp\O365-RelyingPartyTrust.xml"
```

✓ **You should see:** A list of relying party trusts, and an O365-RelyingPartyTrust.xml file in C:\temp.

3 Choose Connect Sync or Cloud Sync

5 steps

Microsoft says new identity and synchronisation features are being developed primarily on Cloud Sync, making it the recommended path for most

organisations. Stay on Connect Sync if you have a confirmed blocker.

Need	Connect Sync	Cloud Sync
Users, groups, contacts, password hash sync, password writeback	Yes	Yes
Exchange hybrid attributes	Yes	Yes
Groups over 50,000 members	Yes	No
More than 150,000 objects per domain	Yes	No
Complex custom sync rules	Yes	Expression builder only
Configure pass-through auth or AD FS from the tool	Yes	Managed separately
Disconnected forests (mergers)	No	Yes
Multiple active agents with automatic failover	No	Yes
Provision cloud groups to AD	No	Yes
Configuration managed in Entra admin center	No	Yes

1

Check the Connect Sync scheduler

Where: Windows PowerShell run as administrator on the existing Microsoft Entra Connect Sync server

Check the scheduler settings, then start a delta sync to confirm sync works. The default cycle is every 30 minutes. If you have no sync server yet and Connect Sync is the right choice, install Microsoft Entra Connect Sync first.

```
Get-ADSyncScheduler
Start-ADSyncSyncCycle -PolicyType Delta
```

✓ **You should see:** Get-ADSyncScheduler shows SyncCycleEnabled : True and the current sync interval. Start-ADSyncSyncCycle returns Result Success.

2

Pause sync for changes

Where: Windows PowerShell run as administrator on the Connect Sync server

Disable the scheduler while you change configuration, and turn it back on afterwards. Microsoft says a sync cycle must run at least once every 7 days.

```
Set-ADSyncScheduler -SyncCycleEnabled $false
# make changes
Set-ADSyncScheduler -SyncCycleEnabled $true
```

✓ **You should see:** Get-ADSyncScheduler shows SyncCycleEnabled : False while paused and True again when you finish.

3

Download the Cloud Sync agent

Where: Microsoft Entra admin center (https://entra.microsoft.com) > Entra Connect > Cloud Sync > Agents, signed in on the agent server

Cloud Sync uses a lightweight provisioning agent with outbound-only connections. Sign in as at least a Hybrid Identity Administrator. Select **Download on-premises agent**, then **Accept terms & download**.

✓ **You should see:** AADConnectProvisioningAgentSetup.exe is in the Downloads folder on the server.

4

Install and register the agent

Where: The agent server, File Explorer > Downloads, then the provisioning agent configuration wizard

Run `AADConnectProvisioningAgentSetup.exe`. Tick **I agree to the license terms and conditions** and select **Install**. On **Welcome** select **Next**. On **Connect Microsoft Entra ID** sign in as a Hybrid Identity Administrator. On **Configure Service Account** choose **Create gMSA** (enter domain administrator credentials) or **Use custom gMSA**. On **Connect Active Directory** add your domain with **Add directory** if it is not listed, then select **Next**, **Next** and **Confirm**. The agent does not sync anything until you create a Cloud Sync configuration.

✓ **You should see:** A notification says the agent configuration was successfully verified. In the admin center, Entra Connect > Cloud Sync > Agents lists the agent with status active.

5

Add a second agent and check for blockers

Where: A second domain-joined server, then Microsoft Entra admin center > Entra Connect > Cloud Sync

Repeat the install on another server: deploy more than one agent for failover. Microsoft's guided migration tool currently lists device synchronisation as a migration blocker, so check it if you use hybrid join before moving off Connect Sync.

✓ **You should see:** Two agents show as active on the Agents page.

4 Choose the sign-in method

4 steps

Method	Where passwords are checked	Infrastructure	Notes
Password hash sync (PHS)	Microsoft Entra ID	Sync only	Microsoft says least effort to deploy and maintain
Pass-through authentication (PTA)	On-premises AD via agents	Microsoft recommends three agents; unconstrained access to DCs; not in a perimeter network	Enforces on-premises account states and sign-in hours immediately
Federation (AD FS)	AD FS	Two or more AD FS servers, two or more WAP servers, load balancing, TLS certificate	Microsoft says more complex to operate and troubleshoot

1

Enable password hash sync regardless

Where: Microsoft Entra Connect wizard on the sync server: Configure > Customize synchronization options > Optional features

Microsoft recommends enabling PHS with whichever method you choose. Entra ID Protection needs PHS for the leaked credentials report, and PHS is the fallback if PTA or AD FS fail. Failover is manual, through Entra Connect. Tick **Password hash synchronization** on **Optional features**, finish the wizard with **Configure**, and let a full password hash sync run.

✓ **You should see:** In the Microsoft Entra admin center, Entra ID > Entra Connect > Connect sync shows Password Hash Sync as Enabled.

2

Test with staged rollout

Where: Microsoft Entra admin center (https://entra.microsoft.com) > Entra ID > Entra Connect > Connect sync > Staged rollout of cloud authentication

If you federate today, Microsoft recommends testing cloud authentication with staged rollout for a pilot group. Use a cloud security group (nested and dynamic groups are not supported) with 200 members or fewer when you first add it. Select **Enable staged rollout for managed user sign-in**, slide **Password Hash Sync** to **On** (optionally **Seamless single sign-on** too) and add the pilot group. You can add up to 10 groups per feature. Reconfigure SaaS apps federated with AD FS to authenticate with Entra ID (see Step 5).

✓ **You should see:** A pilot user opening https://myapps.microsoft.com in a private browser window sees the Entra tenant-branded sign-in page instead of being redirected to AD FS.

3

Record the current federation settings

Where: PowerShell 7 on your admin PC, signed in with Microsoft Graph PowerShell

Record the current federation settings for each domain before you convert it. Microsoft says to review PreferredAuthenticationProtocol, federatedIdpMfaBehavior, SupportsMfa and PromptLoginBehavior for customisations. Save the output with your rollback plan.

```
Connect-MgGraph -Scopes "Domain.ReadWrite.All","Directory.AccessAsUser.All"
Get-MgDomainFederationConfiguration -DomainId contoso.com | Format-List
```

✓ **You should see:** The federation settings for contoso.com print as a list. Save them to a file.

4

Convert federated domains to managed

Where: The same PowerShell 7 session, connected to Microsoft Graph

Convert each domain. Microsoft says conversion may take up to 60 minutes and you do not have to convert all domains at once, so start with a test domain or the one with fewest users. Schedule it out of business hours. If Entra Connect originally configured your AD FS farm, Microsoft also documents doing this in the wizard under **Configure** > **Change user sign-in** > **Password hash synchronization**.

```
Update-MgDomain -DomainId contoso.com -AuthenticationType "Managed"
Get-MgDomain -DomainId contoso.com
```

✓ **You should see:** Get-MgDomain shows AuthenticationType Managed. In the Entra admin center, Entra ID > Entra Connect shows Federation as Disabled.

5 Decide on device join

4 steps

Join type	What it is	Use when
Microsoft Entra joined	Joined only to Entra ID, managed by Intune	Default for new, refurbished and reset Windows devices
Microsoft Entra hybrid joined	Joined to on-premises AD and registered in Entra ID	You still need Group Policy, existing imaging, or Win32 apps that rely on AD machine authentication

1

New devices: Entra join

Where: Microsoft Intune admin center (https://intune.microsoft.com) for Windows Autopilot, or on a single pilot PC: Settings > Accounts > Access work or school > Connect

Microsoft says Entra join should be the default for new and reset endpoints, and hybrid join for new endpoints is typically not recommended. At scale, register devices with Windows Autopilot (export the Autopilot hardware hash) and assign a deployment profile that uses Microsoft Entra join. For a single pilot PC, select **Connect**, then **Join this device to Microsoft Entra ID** and sign in as the user.

```
dsregcmd /status
```

✓ **You should see:** On the device, dsregcmd /status shows AzureAdJoined : YES and DomainJoined : NO.

2

Existing devices: plan resets

Where: Your device inventory sheet, then on each device at its refresh date

Microsoft states there is no supported path to convert a hybrid joined device to Entra joined without a Windows reset. Add a target reset or replacement date to each hybrid joined device in your inventory, and reset or replace devices on their normal refresh cycle.

✓ **You should see:** Every hybrid joined device has a planned date. After reset, dsregcmd /status shows AzureAdJoined : YES and DomainJoined : NO.

3

Keep line of sight for hybrid devices

Where: Your VPN or network design for remote staff, checked on a hybrid device with Command Prompt

Hybrid joined devices need periodic network line of sight to domain controllers. Without it they become unusable. Keep VPN or other connectivity in place until each device has been reset to Entra join.

```
dsregcmd /status
```

✓ **You should see:** A hybrid device shows AzureAdJoined : YES and DomainJoined : YES, and users can sign in away from the office over VPN.

4

Test on-premises resources

Where: An Entra joined pilot PC signed in as a pilot user, in File Explorer and Settings > Bluetooth & devices > Printers & scanners

Microsoft says Entra joined devices can access on-premises resources with single sign-on. Open a file share by path (for example `\\fs01\Shares\Finance`) and add a network printer. Test with a pilot group before scaling.

✓ **You should see:** The share opens without a password prompt and the printer installs.

6 Move applications off AD

3 steps

1

SaaS and federated apps

Where: Microsoft Entra admin center > Entra ID > Enterprise apps > New application, then AD FS Management on the AD FS server

Search the gallery for the app, add it, open **Single sign-on** and choose SAML or OpenID Connect as the app supports, then assign a pilot group. Once users sign in through Entra ID, remove the AD FS relying party. Microsoft suggests confirming with Microsoft Entra Connect Health that no new AD FS requests arrive before removing the Microsoft 365 trust.

```
Remove-AdfsRelyingPartyTrust -TargetName "App name"
```

✓ **You should see:** Pilot users reach the app from https://myapps.microsoft.com and the relying party no longer appears in AD FS Management.

2

Kerberos apps

Where: Your Windows Hello for Business deployment in Intune, following Microsoft's cloud Kerberos trust guidance on Microsoft Learn

For apps that still need Kerberos, Microsoft points to passwordless sign-in with Windows Hello for Business and Cloud Kerberos Trust. With Cloud Sync provisioning to AD, Entra ID can remain the source of authority while an AD account is maintained.

✓ **You should see:** A pilot user signs in with Windows Hello for Business and opens the Kerberos app without a password prompt.

3

LDAP apps

Where: Your Application inventory and dependency map, and each app's own LDAP or directory settings screen

For each app flagged for LDAP, record the LDAP server and bind account from its settings. Replace or modernise apps that use password-based LDAP bind before transferring those users' source of authority.

✓ **You should see:** Every LDAP app has a replacement or modernisation date, and its users are excluded from SOA transfer until then.

7 Make Entra ID the source of authority

6 steps

Microsoft documents user source of authority (SOA) transfer: an administrator moves management of a synced user from AD DS to Entra ID, after which sync no longer updates the object. Check its current release status on Microsoft Learn before production use.

1

Meet the prerequisites

Where: The sync server: Control Panel > Programs and Features (Connect Sync), or the Properties > Details tab of C:\Program Files\Microsoft Azure AD Connect Provisioning Agent\AADConnectProvisioningAgent.exe (Cloud Sync)

Microsoft lists: Connect Sync 2.5.76.0 or later, or Cloud Sync provisioning agent 1.1.1370.0 or later; Hybrid Administrator role; Entra Free licence; no on-premises Exchange workloads; no AD FS federated authentication for the users; and no apps needing password-based LDAP bind or Kerberos with a password. Read the version number and upgrade if it is lower.

✓ **You should see:** The installed version is at or above the minimum and the user is clear of every listed dependency.

2

Consent to the Graph permission

Where: PowerShell 7 with Microsoft Graph PowerShell, signed in as Application Administrator or Cloud Application Administrator

Connect with the documented permission and accept the consent prompt. Microsoft also documents granting it in Graph Explorer under **Consent to permissions**.

```
Connect-MgGraph -Scopes "User-OnPremisesSyncBehavior.ReadWrite.All"
Get-MgContext | Select-Object -ExpandProperty Scopes
```

✓ **You should see:** The scope list includes User-OnPremisesSyncBehavior.ReadWrite.All.

3

Check a user's state

Where: The same PowerShell session, then Microsoft Entra admin center > Entra ID > Users

Read the user's current setting. In the admin center, open the user: synced users have read-only fields and show the source as Windows Server AD DS.

```
Invoke-MgGraphRequest -Method GET -Uri
"https://graph.microsoft.com/v1.0/users/user@contoso.com/onPremisesSyncBehavior?
`$select=isCloudManaged"
```

✓ **You should see:** The response shows isCloudManaged False.

4

Transfer SOA

Where: The same PowerShell session, then the Audit logs page in the Microsoft Entra admin center (search for audit logs)

Set `isCloudManaged` to true and read it back. Confirm the "Change Source of Authority from AD to cloud" entry in the audit log, then confirm the user can be edited in the cloud.

```
Invoke-MgGraphRequest -Method PATCH -Uri
"https://graph.microsoft.com/v1.0/users/user@contoso.com/onPremisesSyncBehavior" -Body
'{"isCloudManaged": true}' -ContentType "application/json"
Invoke-MgGraphRequest -Method GET -Uri
"https://graph.microsoft.com/v1.0/users/user@contoso.com/onPremisesSyncBehavior?
`$select=isCloudManaged"
```

✓ **You should see:** The GET returns isCloudManaged True, the audit log shows the activity, and the user's fields are editable in the admin center.

5

Keep on-premises attributes if needed

Where: Microsoft Graph, for the transferred user objects

Transferred users keep attributes such as onPremisesSamAccountName and onPremisesSecurityIdentifier. Microsoft says you maintain them through Graph if users still need on-premises access. Do not delete them if users still need on-premises resource access.

✓ **You should see:** Transferred users still reach on-premises file shares and apps that use these attributes.

6

Rollback

Where: Microsoft Graph PowerShell, then Windows PowerShell on the Connect Sync server

Microsoft documents a rollback: remove the user from SOA-transferred groups and access packages, set `isCloudManaged` to false, and run a sync cycle. Microsoft's steps also turn off the `blockCloudObjectTakeoverThroughHardMatchEnabled` feature flag first and turn it back on afterwards; follow the Configure user Source of Authority page for that call. The rollback is not complete until the next sync finishes.

```
Invoke-MgGraphRequest -Method PATCH -Uri
"https://graph.microsoft.com/v1.0/users/user@contoso.com/onPremisesSyncBehavior" -Body
'{"isCloudManaged": false}' -ContentType "application/json"
# on the Connect Sync server
Start-ADSyncSyncCycle -PolicyType Delta
```

✓ **You should see:** The audit log shows "Undo changes to Source of Authority from AD DS to cloud" and, after the sync, the user is read-only in the cloud again.

8 Turn off directory sync (whole tenant) 2 steps −

When nothing depends on AD any more, you can turn off directory synchronisation for the tenant. This converts synced users and groups to cloud-only.

1

Uninstall the sync client first

Where: The sync server or agent servers: Control Panel > Programs and Features

Microsoft advises uninstalling Connect Sync or Cloud Sync first if the goal is permanent, otherwise the portal may show optional features such as PHS as still enabled. Select the Microsoft Entra Connect entry (or the provisioning agent) and choose **Uninstall**.

✓ **You should see:** The sync software no longer appears in Programs and Features, and Cloud Sync agents no longer show as active in the Entra admin center.

2

Turn off sync with Microsoft Graph PowerShell

Where: PowerShell 7 on your admin PC, signed in as a Hybrid Identity Administrator

Run the commands below. Read the 72-hour warning first.

```
Install-Module Microsoft.Graph -Force
Connect-MgGraph -Scopes "Organization.ReadWrite.All,Directory.ReadWrite.All"
$organizationId = (Get-MgOrganization).Id
$params = @{ onPremisesSyncEnabled = $false }
Update-MgOrganization -OrganizationId $organizationId -BodyParameter $params
Get-MgOrganization | Select OnPremisesSyncEnabled
```

✓ **You should see:** The last command no longer shows OnPremisesSyncEnabled as True, and synced users become editable in the cloud as the change completes.

⚠ **You must wait 72 hours to undo it.** Microsoft says you must wait 72 hours before turning directory sync back on, and the change clears on-premises

properties including OnPremisesSamAccountName and OnPremisesUserPrincipalName. Do not use it as a troubleshooting step.

9 Decommission AD

3 steps

1 Confirm nothing authenticates to AD

Where: Each domain controller: Event Viewer > Windows Logs > Security, or Windows PowerShell run as administrator

Review domain controller security logs for remaining logons from users, services and devices. Filter for logon event 4624 and note any account or computer that is not the DC itself.

```
Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4624} -MaxEvents 200 | Select-Object TimeCreated, Message
```

✓ **You should see:** Over an agreed observation period, no user, service or workstation logons appear apart from the ones you have planned to remove.

2 Retire servers in order

Where: Server Manager > Manage > Remove Roles and Features on AD FS and WAP servers, Programs and Features on the sync server, then PowerShell on each domain controller

Remove AD FS and WAP servers, sync servers, then demote domain controllers once no device or app needs them. Demote the last domain controller only after the backup in the next step.

```
Uninstall-ADDSDomainController
```

✓ **You should see:** Each server restarts without the role, and the demoted DC no longer appears in Active Directory Sites and Services.

3

Keep backups

Where: Windows PowerShell run as administrator on a domain controller, writing to a separate backup volume

Take and retain a system state backup of a domain controller in line with your records policy.

```
wbadmin start systemstatebackup -backupTarget:E:
```

✓ **You should see:** wbadmin reports that the backup operation successfully completed. Store the backup per your records policy.

WORTH KNOWING

What can go wrong, and how do you avoid it?

The detail behind the plan: options compared, and what experienced engineers check first. Tap any item.

Compare all the ways to do this — 4 options

Stay hybrid on Microsoft Entra Cloud Sync

LOW EFFORT

Best for: Organisations keeping AD for now with no Connect Sync blocker, including disconnected forests after a merger

+ The path Microsoft recommends for most organisations, where new sync features are developed first
+ Lightweight agents with outbound-only connections, and several active agents for automatic failover
+ Configuration lives in the Microsoft Entra admin center, not on a sync server
– Does not support groups over 50,000 members or more than 150,000 objects per domain
– Custom sync rules are limited to the expression builder
– Microsoft lists device synchronisation as a migration blocker, so check it if you use hybrid join

Read more →

Stay hybrid on Microsoft Entra Connect Sync

MEDIUM EFFORT

Best for: Organisations with a confirmed Cloud Sync blocker: very large groups or directories, or complex custom sync rules

+ Supports large groups, large domains and complex custom rules
+ Can configure pass-through authentication or AD FS from the same tool
– A sync server to patch, monitor and keep running (a sync cycle must run at least once every 7 days)
– Not where Microsoft is developing new sync features

Read more →

Phased move to cloud-only (Entra join, then source of authority per user)

HIGH EFFORT

Best for: Organisations retiring AD over time while some users, apps or devices still depend on it

+ Users move one at a time, with a documented rollback for each
+ New and reset Windows devices go straight to Entra join through Intune and Autopilot
+ Transferred users keep on-premises attributes for remaining resource access
– Needs no on-premises Exchange workloads, no AD FS for those users, and no apps using password-based LDAP bind or Kerberos with a password
– Hybrid joined PCs cannot be converted: each needs a reset to become Entra joined
– Check the current release status of source of authority transfer before production use

Read more →

Turn off directory sync for the whole tenant

LOW EFFORT

Best for: Small organisations where nothing authenticates to AD any more and every user can go cloud-only at once

+ Converts every synced user and group to cloud-only in one change
+ Lets you uninstall the sync client and start retiring domain controllers
– All or nothing: you must wait 72 hours before you can turn sync back on
– Clears on-premises properties such as OnPremisesSamAccountName and OnPremisesUserPrincipalName

Read more →

OUR ADVICE

If AD will stay for a year or more, run Cloud Sync with password hash sync unless the comparison table shows a blocker, in which case stay on Connect Sync. To leave AD, take the phased route: finish Exchange, Entra join devices as they are replaced or reset, move LDAP and Kerberos apps, then transfer source of authority per user. Turn off sync for the whole tenant only at the end, or if you are small enough that nothing depends on AD today.

Turn on password hash sync before you need it

REDUCES RISK

If you use AD FS or pass-through authentication and the on-premises side fails, users cannot sign in to anything in Microsoft 365. Microsoft recommends PHS with every sign-in method because it is the fallback, and failover to it is manual.

WHAT TO DO

Enable **Password hash synchronization** on the Entra Connect **Optional features** page now, even if you keep federation for a while, and write the failover steps into your rollback plan.

Microsoft Learn: Authentication for Microsoft Entra hybrid identity solutions

Clean up AD before you sync more of it

REDUCES RISK

Everything in scope ends up in Entra ID: disabled accounts, test users, old service accounts and stale groups. Once there, they clutter licensing, access reviews and Conditional Access scoping.

WHAT TO DO

Use OU filtering in the Entra Connect wizard (**Domain and OU filtering**) or Cloud Sync scoping so only real users, groups and contacts sync. Disable or delete stale objects in AD first.

Check the Cloud Sync limits before you switch

SAVES TIME

Cloud Sync does not support groups over 50,000 members or more than 150,000 objects per domain, and the guided migration tool lists device synchronisation as a blocker. Finding this mid-migration forces a rollback to Connect Sync.

WHAT TO DO

Use the group size output from Step 1 and the object counts per domain. If any limit is hit, or you still hybrid join devices, stay on Connect Sync for now.

Microsoft Learn: Microsoft Entra Cloud Sync migration decision guide

Pilot sign-in changes with staged rollout, not a domain flip

USER IMPACT

Converting a domain from federated to managed affects every user on it at once and Microsoft says it can take up to 60 minutes. Staged rollout lets a group test cloud sign-in first.

WHAT TO DO

Use cloud security groups (not nested or dynamic), add 200 users or fewer per new group, and remember the 10-group limit per feature. Convert the smallest domain first, out of hours.

Microsoft Learn: Migrate to cloud authentication using Staged Rollout

Legacy protocols do not follow staged rollout

REDUCES RISK

Microsoft says legacy authentication such as POP3 and SMTP is not supported by staged rollout and falls back to federation. Scanners and line-of-business apps that send mail can break when you finally turn off AD FS.

WHAT TO DO

Check the Entra sign-in logs for legacy authentication clients before converting domains, and move those devices and apps to modern authentication first.

Microsoft Learn: Migrate to cloud authentication using Staged Rollout

Budget for device resets, not device conversions

COST LEVER

Microsoft states there is no supported way to convert a hybrid joined device to Entra joined without a Windows reset. A plan that assumes in-place conversion will stall.

WHAT TO DO

Move devices to Entra join at their normal refresh or reset, using Autopilot. Keep hybrid join and line of sight to domain controllers for the rest until then.

TOOLS THAT CAN GET AROUND THIS

Microsoft has no in-place conversion, but these third-party tools re-join a domain joined or hybrid joined Windows PC to Microsoft Entra ID and keep the user's existing profile, so the device does not need a reset. It is not a Microsoft-supported path, so pilot it on each hardware model first.

Quest On Demand Migration

Converts domain joined or hybrid joined Windows 10 and 11 devices to Entra joined and updates the user profiles during the join.

ForensiT User Profile Wizard

Migrates an existing domain profile to the user's Azure AD (Entra ID) account. The Entra join itself is done with a provisioning package.

Third-party tools, not endorsed by the platform vendor. Confirm in the tool's documentation and run a pilot first.

Microsoft Learn: Join your cloud-native endpoints to Microsoft Entra

Finish Exchange before transferring source of authority

REDUCES RISK

Microsoft lists no on-premises Exchange workloads as a prerequisite for user SOA transfer. Mailbox attributes managed by an Exchange server will not be editable the way you expect after the switch.

WHAT TO DO

Complete the mailbox move and plan the last Exchange server first. See the Exchange to Exchange Online guide.

Microsoft Learn: Configure user Source of Authority

Move SOA per user before turning sync off for the tenant

REDUCES RISK

Turning off directory sync is tenant wide, clears on-premises properties and cannot be reversed for 72 hours. Per-user SOA transfer has a documented rollback.

WHAT TO DO

Transfer SOA for pilot users first and leave the tenant-wide switch until every user and app has moved and the sync client is uninstalled.

Microsoft Learn: Turn off directory synchronization for Microsoft 365

Service accounts and app dependencies outlive users

REDUCES RISK

The last things holding AD up are usually service accounts, LDAP binds from old apps and printers or scanners using Kerberos. Users can be cloud-only while these still need a domain controller.

WHAT TO DO

Keep the application inventory current and review DC security logs over a full business cycle (including month-end and year-end jobs) before demoting the last DC.

Find attribute errors before the sync engine does

SAVES TIME

Microsoft requires mail, proxyAddresses and userPrincipalName to be unique before you sync. Entra Connect and Cloud Sync do not fix duplicates or bad values: they report errors for the affected objects, which stay out of sync until you fix them in AD.

WHAT TO DO

Scan the in-scope OUs for duplicate and malformed attributes before the first sync and before you widen scope. Fix them in AD, not in the cloud, and rerun the scan

until it is clean.

TOOLS THAT CAN GET AROUND THIS

Microsoft's free IdFix tool queries on-premises AD before sync and lists objects with duplicate or badly formatted values in the attributes that sync, so you can fix them in bulk instead of chasing sync errors one by one.

IdFix

Microsoft says running IdFix makes sure your on-premises Active Directory is ready for directory synchronisation.

Third-party tools, not endorsed by the platform vendor. Confirm in the tool's documentation and run a pilot first.

Microsoft Learn: Synchronize domain users to Microsoft 365

FINISH SAFELY

How do you check it worked, or roll back?

Full validation checklist

9 checks

Run these before you declare the migration complete. Record the results in the data validation report.

Check	How to check	What good looks like
Synced object counts match AD	On the admin PC, rerun the Step 1 counts (`(Get-ADUser -Filter *).Count` , groups and contacts) for the OUs in sync scope. In PowerShell 7 with Microsoft Graph, count synced users with `Get-MgUser -All -Property OnPremisesSyncEnabled | Where-Object OnPremisesSyncEnabled` and compare.	Every in-scope user, group and contact exists in Entra ID; any difference is explained by OU filtering or scoping you chose.

Check	How to check	What good looks like
Sync is healthy and running on schedule	On the Connect Sync server run `Get-ADSyncScheduler` and `Start-ADSyncSyncCycle -PolicyType Delta`. For Cloud Sync, open Microsoft Entra admin center > Entra Connect > Cloud Sync and check the agents and provisioning logs.	SyncCycleEnabled is True, the delta cycle completes without export errors, and every Cloud Sync agent shows as active.
Domains use the sign-in method you intended	In PowerShell 7 connected to Microsoft Graph, run `Get-MgDomain -DomainId contoso.com` for each domain you converted.	AuthenticationType shows Managed for every converted domain and Federated only for domains you have not yet moved.
Users sign in with cloud authentication, inside and outside the office	Sign in as pilot users in a private browser at https://myapps.microsoft.com, on and off the corporate network. In the Microsoft Entra admin center, filter the sign-in logs by those users and check the result and authentication details.	Sign-ins succeed through the Entra sign-in page with MFA as your policies require, and none are redirected to AD FS.
Devices hold a Primary Refresh Token	On a sample of Entra joined and hybrid joined PCs, open Command Prompt and run `dsregcmd /status`.	AzureAdJoined is YES (and DomainJoined is YES for hybrid devices) and AzureAdPrt is YES.
Outlook, Teams and OneDrive keep working after the sign-in change	On a pilot PC and a pilot phone, open Outlook, Teams and OneDrive after the domain conversion and after a restart. Check that OneDrive shows no sign-in prompt in its notification area icon and that mobile apps stay signed in.	Clients stay signed in or prompt once for the Entra sign-in page; mail, chat and file sync continue without errors.

Check	How to check	What good looks like
On-premises file shares, printers and apps still work	On an Entra joined pilot PC, open a file share by path (for example \\fs01\Shares\Finance), add a network printer, and sign in to each app in the Application inventory and dependency map that uses Kerberos or LDAP.	Shares and printers open with single sign-on, and every app owner signs off their app in the pilot test plan.
Source of authority transfers are recorded and editable	For transferred users, run the `onPremisesSyncBehavior?$select=isCloudManaged` GET request from the source of authority section, then search the Entra audit logs for "Change Source of Authority from AD to cloud".	isCloudManaged is true, an audit entry exists for each user, and the user can be edited in the Entra admin center.
Nothing still authenticates to the domain controllers (before demotion)	On each domain controller, run `Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4624}` or filter Event Viewer > Windows Logs > Security for event 4624, across a full business cycle including month-end jobs.	No logons appear from users, service accounts or computers other than the domain controllers themselves.

Rollback plan

If it goes wrong —

ROLL BACK IF

- Pilot or production users cannot sign in after a domain converts to managed, and the cause is not fixed within the change window
- Hybrid joined devices lose their Primary Refresh Token or cannot reach domain controllers
- An application in the dependency map fails for transferred source of authority users and has no quick fix
- Sync export errors or unexpected deletes appear in Entra ID after a sync configuration change

POINT OF NO RETURN

Converting a domain and transferring source of authority per user can both be reversed. Turning off directory sync for the whole tenant is the real point of no return: Microsoft says you must wait 72 hours before you can turn it back on, and it clears on-premises properties such as OnPremisesSamAccountName and OnPremisesUserPrincipalName. Demoting the last domain controller removes the forest; only the system state backup can bring it back.

1

Stop further changes

Where: Windows PowerShell run as administrator on the Connect Sync server

Pause the scheduler so no more changes export while you assess. Leave it paused only as long as needed: Microsoft says a sync cycle must run at least once every 7 days.

```
Set-ADSyncScheduler -SyncCycleEnabled $false
```

✓ **You should see:** `Get-ADSyncScheduler` shows SyncCycleEnabled False.

2

Move pilot users back to federation

Where: Microsoft Entra admin center (https://entra.microsoft.com) > Entra ID > Entra Connect > Connect sync > Staged rollout of managed user sign-in

Remove the affected users or groups from the staged rollout features, or slide the feature to Off. Users then sign in through the federated provider again.

✓ **You should see:** Affected users are redirected to the AD FS or third-party sign-in page.

3

Federate a converted domain again

Where: PowerShell 7 on your admin PC, connected with Connect-MgGraph using Domain.ReadWrite.All

Recreate the federation with `New-MgDomainFederationConfiguration` using the settings you saved with `Get-MgDomainFederationConfiguration` in the auth step. This only works while the AD FS farm still exists. Allow up to 60 minutes for the change.

✓ **You should see:** `Get-MgDomain -DomainId contoso.com` shows AuthenticationType Federated and users sign in through AD FS.

4

Return a user to AD as source of authority

Where: PowerShell 7 with Microsoft Graph, then Windows PowerShell on the Connect Sync server

Follow the documented rollback on Microsoft Learn: Configure user Source of Authority. Remove the user from SOA-transferred groups and access packages, set `isCloudManaged` to false with the PATCH request, then run `Start-ADSyncSyncCycle -PolicyType Delta`. Handle the blockCloudObjectTakeoverThroughHardMatchEnabled flag as that page describes.

✓ **You should see:** After the next sync, the user shows Windows Server AD DS as the source and cloud fields are read-only again.

5

Restart sync and confirm

Where: Windows PowerShell run as administrator on the Connect Sync server

Turn the scheduler back on with `Set-ADSyncScheduler -SyncCycleEnabled $true` and run a delta cycle.

✓ **You should see:** The cycle completes with no export errors and object counts match the validation baseline.

6

If sync was turned off for the tenant

Where: PowerShell 7 on your admin PC, signed in as a Hybrid Identity Administrator

Wait the 72 hours Microsoft requires, reinstall Connect Sync or Cloud Sync, then set `onPremisesSyncEnabled` back to true with `Update-MgOrganization` and run a full sync. Check the Synchronization Service Manager for duplicate or unmatched objects before users rely on it.

✓ **You should see:** `Get-MgOrganization | Select OnPremisesSyncEnabled` shows True and synced users show AD as the source.

7

Accept what cannot be undone

Where: Your Rollback plan and Decommission checklist

Record that a demoted last domain controller or a deleted forest can only come back from the system state backup taken with `wbadmin`, and that a PC reset to Entra join has to be joined to the domain again to return to hybrid join.

✓ **You should see:** The change record lists each irreversible step and who approved it.

Agree the triggers and who decides before the go / no-go meeting. Use the rollback plan template.

Common problems and fixes

6 errors

`Hybrid joined laptop cannot sign in away from the office`

Cause: Hybrid joined devices need periodic line of sight to a domain controller.

Fix: Provide VPN or line of sight, or move the device to Entra join after a reset.

`Users cannot sign in after an AD FS outage`

Cause: Federation depends on on-premises AD FS and failover to PHS is manual.

Fix: Enable PHS now so you can switch the sign-in method in Entra Connect during an outage.

`SOA transfer fails or user still read-only in the cloud`

Cause: Sync client below the minimum version, missing Graph permission, or the user has on-premises Exchange or AD FS dependencies.

Fix: Upgrade Connect Sync to 2.5.76.0 or later (or the Cloud Sync agent to 1.1.1370.0 or later), consent to User-OnPremisesSyncBehavior.ReadWrite.All, and clear the prerequisites.

`Cannot re-enable directory sync after turning it off`

Cause: Microsoft requires a 72-hour wait after turning sync off.

Fix: Wait 72 hours, then re-enable. Plan the turn-off as a one-way change.

`Cloud Sync migration tool reports a blocker`

Cause: Device synchronisation for hybrid join is listed as a migration blocker in the guided tool.

Fix: Keep Connect Sync for device sync until devices are Entra joined, or review the tool's requirements.

`Objects not syncing after configuration changes`

Cause: The Connect Sync scheduler was left disabled.

Fix: Run Set-ADSyncScheduler -SyncCycleEnabled $true and start a delta sync.

Search the full error library →

FAQ

Frequently asked questions

Should I use Entra Connect Sync or Cloud Sync?

Microsoft calls Cloud Sync the recommended path forward for most organisations. Stay on Connect Sync if you need features it lacks, such as very large groups or complex sync rules.

Which sign-in method should I use?

Password hash sync is the simplest. Microsoft recommends enabling it whichever method you use, because it backs up PTA and federation and powers leaked credential detection.

Can I convert hybrid joined PCs to Entra joined?

Not in place. Microsoft says a Windows reset is required.

How do I make synced users cloud-only?

Either transfer user source of authority per user through Microsoft Graph, or turn off directory sync for the whole tenant.

Do I need Entra ID P1 or P2?

Microsoft lists Entra Free for user SOA. Features such as Entra ID Protection need P2. Check Microsoft's current licensing pages.

Do Entra joined devices still reach file shares?

Microsoft says Entra joined devices can access on-premises resources with single sign-on. Pilot it before rolling out.

SOURCES

Official sources

12 official pages this guide is based on

Vendors change limits and features, so confirm details on the source before you rely on them. Last checked 4 Nov 2026.

- Microsoft Learn: Microsoft Entra Cloud Sync migration decision guide
- Microsoft Learn: What is Microsoft Entra Cloud Sync?
- Microsoft Learn: Install the Microsoft Entra provisioning agent (Cloud Sync)
- Microsoft Learn: Migrate to cloud authentication using Staged Rollout
- Microsoft Learn: Microsoft Entra Connect Sync scheduler
- Microsoft Learn: Authentication for Microsoft Entra hybrid identity solutions
- Microsoft Learn: Migrate from federation to cloud authentication
- Microsoft Learn: User Source of Authority overview
- Microsoft Learn: Configure user Source of Authority
- Microsoft Learn: Turn off directory synchronization for Microsoft 365
- Microsoft Learn: Join your cloud-native endpoints to Microsoft Entra
- Microsoft Learn: What is a Microsoft Entra hybrid joined device?