MIGRATION PLAYBOOK · IDENTITY AND SECURITY

How to migrate from AD FS to Microsoft Entra ID

Discover every relying party, give users password hash sync or pass-through sign-in, pilot with staged rollout, move apps with the AD FS application migration wizard, convert your domains to managed, then remove AD FS and WAP the way Microsoft documents.

Updated 4 Nov 2026 6 phases 31 detailed steps 12 official sources

START HERE

How do you migrate from AD FS to Microsoft Entra ID?

SHORT ANSWER

This retires AD FS (Active Directory Federation Services, the on-premises servers that sign users in to Microsoft 365 and other apps) and moves that sign-in to Microsoft Entra ID, the cloud directory behind Microsoft 365. Nothing is copied: you change where passwords and MFA (multi-factor authentication) are checked.

- **Recommended route:** Staged rollout, then domain conversion and app waves
- **Order:** Give every user a working cloud sign-in before anything is switched off, and keep AD FS running as the fallback until the very end.
- **6 phases:** Find what uses AD FS, Prepare cloud sign-in, Pilot cloud sign-in, Move the apps, Switch the domains and Remove AD FS.
- **You're done when:** Every domain shows Managed in Get-MgDomain, and staged rollout features are Off.

The recommended route turns on password hash sync (Entra ID checks a hash of each AD password), tests cloud sign-in with a pilot group using staged rollout (cloud sign-in for chosen groups while AD FS still serves everyone else), converts each domain from federated (signing in through AD FS) to managed

(signing in through Entra ID), moves each app that signs in through AD FS (Microsoft calls these relying party trusts), then removes the AD FS servers. Expect a few weeks of running both, plus at least one quiet week before you remove AD FS.

RECOMMENDED ROUTE

Staged rollout, then domain conversion and app waves

Pilot groups test cloud sign-in while AD FS stays as the fallback, and the migration wizard handles the basics for SAML apps.

▼ Other options and when to use them

- **Direct switch with Entra Connect Change user sign-in**
  : Entra Connect set up your AD FS farm, it serves only Microsoft 365, and everyone can change in one window.
- **Move Microsoft 365 now, keep AD FS for some apps**
  : A few legacy or header-based apps cannot move yet. Keep a small AD FS farm for them until they do.

TOOLS FOR THIS PLAN

Are you ready?
22-question readiness check

Plan your dates
Dated countdown you can add to your calendar

Check your DNS
MX, SPF, DKIM and DMARC lookup

New to the jargon?
Plain-English migration glossary

ORDER TO MIGRATE IN, AND WHY

Give every user a working cloud sign-in before anything is switched off, and keep AD FS running as the fallback until the very end. Microsoft says users and apps can move in either order, but recommends users first, because Microsoft 365 is usually the busiest app on AD FS.

1 **Inventory and back up: relying party trusts, federation settings, the AD FS farm**

You cannot plan apps you have not found, and your rollback is to federate the domain again with the settings you saved.

2 **Turn on password hash sync and build Conditional Access in Report-only mode**

Users need a cloud sign-in method and the same protections before AD FS stops checking them. Report-only shows the effect without blocking anyone.

3 **Register users for Entra MFA**

After conversion only Entra MFA applies, so an MFA adapter on AD FS (such as Duo) stops prompting.

4 **Pilot cloud sign-in with staged rollout groups**

The domain stays federated, so everyone outside the pilot is untouched and the pilot can be undone by removing them from the group.

5 **Convert domains to managed, one at a time, smallest first**

Each conversion moves every user on that domain at once and can take up to 60 minutes, so a small domain shows problems with fewer people affected.

6 **Move the apps in waves, SAML apps with the wizard first**

These can run alongside or after the domains. The wizard handles the basics for SAML apps, which leaves the hand-built apps for later waves.

7 **Give apps published through Web Application Proxy a new publishing path**

Removing Web Application Proxy (WAP) takes them offline, and nothing moves them for you.

8 **Watch for a week, then uninstall AD FS and WAP**

Microsoft asks for at least one week with no AD FS sign-ins. After uninstall, going back means building a new farm.

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)

☐ **Cloud sign-in method**

Password hash sync, pass-through authentication (an on-premises agent checks each password), or certificate-based sign-in for smart card users.

▼ How each tool handles it

Built-in method	Microsoft recommends password hash sync. Its decommission guide says pass-through authentication should only be used where regulation forbids syncing password information. Password hash sync also gives you a fallback if pass-through agents or AD fail.

Tip: Turn password hash sync on and let a full sync cycle finish before the pilot, even if you choose pass-through authentication.

Microsoft Learn: AD FS decommission guide

- [ ] **Where MFA happens**

Whether Entra MFA replaces any MFA adapter on AD FS (such as Duo), or that provider plugs into Entra ID instead.

▼ **How each tool handles it**

Built-in method	While a domain is federated, the federatedIdpMfaBehavior setting controls whether Entra ID accepts MFA done by AD FS. After conversion, only Entra MFA applies.
Microsoft Entra external MFA	Lets an external MFA provider meet Entra ID MFA requirements. Each user of it needs a Microsoft Entra ID P1 or P2 licence.
Duo for Microsoft Entra ID external MFA	Duo counts as an Entra ID MFA method and can satisfy Conditional Access. Running the old Duo custom control too can prompt some users twice.

Tip: Save the current value with Get-MgDomainFederationConfiguration before you change anything.

Microsoft Learn: Migrate from federation to cloud authentication

- [ ] **AD FS access rules**

Which AD FS access control policies (for example, block outside the office, require MFA) become Conditional Access policies.

▼ **How each tool handles it**

Built-in method	Access rules on AD FS do not carry over. Conditional Access needs a Microsoft Entra ID P1 licence for each user. Microsoft 365 Business Premium and Microsoft 365 E3 include P1; Microsoft 365 E5 includes P2, which also covers it.

Tip: Build each policy in Report-only mode during the pilot, and add one that blocks legacy sign-in.

Microsoft Learn: Microsoft Entra licensing

- [ ] **Pilot groups and users staged rollout cannot test**

Who is in each pilot wave, and how you handle users the pilot cannot cover.

▼ **How each tool handles it**

Built-in method Staged rollout needs plain assigned groups (no nested or dynamic groups), with up to 200 users in a new group when first added. It cannot test legacy sign-in (POP3, SMTP), smart cards, Windows Hello for Business certificate trust or non-persistent VDI (virtual desktops reset at sign-out).

Tip: Give each new pilot user a Temporary Access Pass (a one-time sign-in code) so they skip their last AD FS sign-in.

Microsoft Learn: Migrate to cloud authentication using Staged Rollout

- [ ] **App inventory**

Which relying party trusts are still used, and who owns each one.

▼ How each tool handles it

Built-in method The AD FS application migration dashboard in Entra ID only shows apps with sign-ins in the last 30 days, and hides Microsoft relying parties. It needs Connect Health agents on the AD FS servers.

Tip: Export every trust with PowerShell, reconcile it against the dashboard, and ask owners about quarterly and year-end apps.

Microsoft Learn: AD FS application migration to move AD FS apps to Microsoft Entra ID

- [ ] **SAML apps**

Which SAML apps move with the migration wizard, and who tests each one.

▼ How each tool handles it

Built-in method The wizard creates the enterprise app for SAML apps only. It does not move the signing certificate or Conditional Access, and not every claim rule translates as is.

Tip: Use Migration status details to see which claims need review, and test with each app owner before production.

Microsoft Learn: AD FS application migration to move AD FS apps to Microsoft Entra ID

- [ ] **OIDC, OAuth and WS-Fed apps**

Who rebuilds each non-SAML app in Entra ID, and when.

▼ How each tool handles it

Built-in method The wizard does not handle these. Each is set up by hand as an app registration or enterprise app, and the app itself must be updated with the new settings.

Tip: Book time with each app vendor or developer early, because they usually make the change on their side.

Microsoft Learn: AD FS application migration to move AD FS apps to Microsoft Entra ID

- [ ] **Apps published through Web Application Proxy**

How each internal web app published through WAP will be reached from outside after WAP goes.

▼ **How each tool handles it**

Built-in method	Microsoft's decommission guide tells you to remove published apps before uninstalling WAP, but does not move them anywhere.
Microsoft Entra application proxy	Publishes on-premises web apps, including Kerberos and form-based ones, through outbound-only connectors.
Strata Maverics Identity Orchestration	Sends each user to AD FS or Entra ID depending on whether they have moved, so an app follows your user waves.

Tip: List every published app in the Remote Access Management Console and test its new path from outside the network.

Microsoft Learn: AD FS decommission guide

- [ ] **Sign-in page and username format**

What the new sign-in page looks like, and how you tell users.

▼ **How each tool handles it**

Built-in method	AD FS sign-in page customisations (onload.js) cannot be copied to Entra ID. Users must sign in with their full UPN or email address. Company branding needs a Microsoft 365 or paid Entra ID licence.

Tip: Set up company branding before the pilot and send users a screenshot of the new page.

Microsoft Learn: Migrate from federation to cloud authentication

- [ ] **Password expiry**

Whether cloud passwords of synced users must expire on the same schedule as AD passwords.

▼ **How each tool handles it**

Built-in method	By default, password hash sync sets synced users' cloud passwords to never expire, and staged rollout users get no

expiry either.

Tip: Review CloudPasswordPolicyForPasswordSyncedUsersEnabled with your security owner before cutover.

Microsoft Learn: Implement password hash synchronization

- [ ] **How domains are converted**

Whether to convert with Entra Connect or with PowerShell, and in which window.

▼ How each tool handles it

Built-in method	The Entra Connect Change user sign-in option converts all federated domains at once, and only if Entra Connect set up the farm. Update-MgDomain in PowerShell converts one domain at a time. Each conversion can take up to 60 minutes.

Tip: Convert outside business hours, test or smallest domain first. Modern Outlook, Teams and OneDrive keep working on their existing tokens.

Microsoft Learn: Migrate from federation to cloud authentication

- [ ] **Hybrid joined PCs and seamless SSO**

How domain PCs keep signing in automatically after AD FS goes.

▼ How each tool handles it

Built-in method	Hybrid joined Windows 10 and later PCs sign in with a Primary Refresh Token from Entra ID. Seamless SSO (for older PCs) uses a Kerberos key that Microsoft says to roll over at least every 30 days.

Tip: Run dsregcmd /status on sample PCs after conversion and check AzureAdPrt shows YES.

Microsoft Learn: Migrate from federation to cloud authentication

- [ ] **When to remove AD FS**

How long you watch for AD FS traffic, and what backup you keep.

▼ How each tool handles it

Built-in method	Microsoft asks for at least one week of testing after moving authentication, checking AD FS event logs or Connect Health for any sign-ins.

Tip: Take a final Rapid Restore Tool backup before you uninstall, and keep it until your rollback period ends.

Microsoft Learn: AD FS decommission guide

THE PLAN, PHASE BY PHASE

1 Find what uses AD FS

Before you change sign-in

- Export every relying party trust (an app that signs in through AD FS) to a CSV file.
- Give each trust an owner, protocol and business importance in your app inventory.
- Turn on verbose AD FS

auditing on each AD FS server.

Install the Connect Health agent on every AD FS and WAP (Web Application Proxy) server.

Save each federated domain's federation settings, and take a Rapid Restore Tool backup of the farm.

> ⚠ **Watch out:** The migration dashboard only shows apps used in the last 30 days, and hides Microsoft relying parties.
>
> **WAYS AROUND IT**

- Reconcile the dashboard against your PowerShell export, and ask each owner when the app is next used.

Show the detailed steps (5) →

2 Prepare cloud sign-in

Turn on password hash sync (Entra ID checks a hash of each AD password) in Entra Connect.

Use pass-through authentication (an on-premises agent checks each password) only if regulation forbids syncing password

data, with at least three agents.

Rebuild each AD FS access rule as a Conditional Access policy (an Entra sign-in rule) in Report-only mode, plus one blocking legacy sign-in.

Set up company branding and ask pilot users to

register for Entra MFA.

Watch out: If AD FS uses a third-party MFA adapter such as Duo, only Entra MFA applies after conversion.

WAYS AROUND IT

- Have users register for Entra MFA during the pilot.

TOOLS THAT CAN DO IT

Microsoft Entra external MFA
Lets an external MFA provider meet Entra ID MFA requirements. Each user of it needs a Microsoft Entra ID P1 or P2 licence.

Duo for Microsoft Entra ID external MFA
Duo counts as an Entra ID MFA method and can satisfy Conditional Access. Running the old Duo custom control too can prompt some users twice.

Watch out: AD FS sign-in page customisations do not carry over, and users must sign in with their full UPN or email.

WAYS AROUND IT

- Set up Entra company branding and tell users what the new page looks like.

Watch out: Password hash sync sets the cloud passwords of synced users to never expire by default, whatever your AD policy says.

WAYS AROUND IT

- Review CloudPasswordPolicyForPasswordSyncedUsersEnabled with your security owner before cutover.

Show the detailed steps (4) →

3 Pilot cloud sign-in

Create cloud-only security groups with directly added

members for each pilot wave.

Turn on staged rollout (cloud sign-in for chosen groups only) for password hash sync and the pilot group.

Give each new pilot user a Temporary Access Pass so they skip their last AD FS

sign-
in.

Test
sign-
in
at
myapps.microsoft.com
on
and
off
the
office
network.

Check
the
AD
FS
event
logs
for
pilot
users
still
reaching
AD
FS.

Watch out: Staged rollout does not accept nested or dynamic groups, and a new group can hold 200 users when first added.

WAYS AROUND IT

- Use several plain assigned groups for larger waves.

Watch out: Staged rollout cannot test legacy sign-in (POP3, SMTP), smart cards, Windows Hello certificate trust or non-persistent VDI.

WAYS AROUND IT

- Move legacy clients to modern authentication, plan certificate-based sign-in for smart card users, and keep non-persistent VDI federated for now.

Show the detailed steps (3) →

4 Move the apps

Open the AD FS application migration dashboard and start with apps marked Ready to migrate.

Use Begin migration for each SAML app, then add missing claims and Conditional Access.

Give the app the Entra signing certificate or metadata, test

instance first, then production.

Set up OIDC, OAuth and WS-Fed apps by hand as app registrations or enterprise apps.

Disable each migrated trust, and remove it once the app owner signs off.

> **Watch out:** The wizard moves SAML apps only, and does not move the signing certificate, Conditional Access or every claim rule.
>
> **WAYS AROUND IT**
>
> - Budget hand work per app, using the Migration status details to see which claims need review.

Watch out: Internal apps published through WAP are not moved anywhere when you remove WAP.

WAYS AROUND IT

- List every published app in the Remote Access Management Console and test a new publishing path for each.

TOOLS THAT CAN DO IT

Microsoft Entra application proxy
Publishes on-premises web apps, including Kerberos and form-based ones, through outbound-only connectors.

Strata Maverics Identity Orchestration
Sends each user to AD FS or Entra ID depending on whether they have moved, so an app follows your user waves.

Show the detailed steps (5) →

5 Switch the domains

Out of business hours

Check whether Entra Connect set up your AD FS farm. Only then can its Change user sign-in option convert the domains.

If you use pass-through authentication, confirm every agent shows Active first.

Convert one domain at a time from federated to managed, starting with a test or the smallest domain.

Turn staged rollout off once every domain is managed.

Check a sample of hybrid joined PCs still get a Primary Refresh Token with dsregcmd /status.

> **Watch out:** Each conversion can take up to 60 minutes, and new browser sign-ins may not prompt during that time.
>
> **WAYS AROUND IT**
>
> - Convert outside business hours. Modern Outlook, Teams and OneDrive keep working on their existing tokens.

> **Watch out:** The Entra Connect Change user sign-in option converts all federated domains at once.
>
> **WAYS AROUND IT**
>
> - Use Update-MgDomain in PowerShell to convert one domain at a time instead.

Turn this phase into dated tasks with the cutover planner

Show the detailed steps (5) →

6 Remove AD FS

At least one week after the switch

Check Connect Health and the AD FS

event logs show no sign-ins for a full week.

Remove the Microsoft 365 trust and take a final Rapid Restore Tool backup.

Remove the AD FS load balancer entries and DNS records.

Uninstall WAP, then AD FS (secondary servers

before the primary).

Delete the certificates and service account, wipe the servers and empty the certificate container in AD.

> **Watch out:** Once AD FS is uninstalled and its certificates deleted, going back means building a new farm.
>
> **WAYS AROUND IT**
>
> - Start this phase only after the agreed rollback period, and keep the Rapid Restore backup.

> **Watch out:** Seamless SSO (automatic sign-in on domain PCs) uses a Kerberos key that does not roll over by itself.
>
> **WAYS AROUND IT**
>
> - Roll it over at least every 30 days, or rely on the Primary Refresh Token on Windows 10 and later.

Check your DNS records before and after the change

Show the detailed steps (6) →

You are finished when

- Every domain shows Managed in Get-MgDomain, and staged rollout features are Off.

- Users see the Entra sign-in page with MFA on and off the network, and no sign-in reaches AD FS.
- Every relying party trust is migrated, disabled or kept with a named owner and date.
- Connect Health shows no AD FS sign-ins for a full week before you uninstall.

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 —

AD FS usually does two jobs: it signs users in to Microsoft 365 through a federated domain, and it acts as the identity provider for other apps through relying party trusts. Moving to Microsoft Entra ID means moving both. Microsoft says you can do them in either order but recommends moving user authentication first.

This guide covers discovery with Connect Health and the AD FS application migration dashboard (which replaced the old AD FS application activity report), choosing password hash sync or pass-through authentication, piloting with staged rollout, moving apps, converting domains, and the decommission steps in Microsoft's AD FS decommission guide. If you also want to retire Active Directory itself, continue with the Active Directory to Entra ID guide.

SIGN-IN METHODS
Password hash sync (Microsoft recommended), pass-through authentication or certificate-based authentication

PILOT
Staged rollout for groups while domains stay federated

APP DISCOVERY
AD FS application migration in Entra ID (Usage & insights), fed by Connect Health

WIZARD SCOPE
SAML apps only; OIDC, OAuth and WS-Fed are configured by hand

DOMAIN SWITCH
Entra Connect Change user sign-in, or Update-MgDomain -AuthenticationType Managed

DECOMMISSION
Watch at least one week, then follow Microsoft's AD FS decommission guide

1 What you need before step one

Need	Details	Where to get it
Hybrid Identity Administrator	For staged rollout and domain conversion. Microsoft's Option A uses a Global Administrator in Entra Connect.	Microsoft Entra admin center (https://entra.microsoft.com)
Cloud Application Administrator or Application Administrator	To use the AD FS application migration wizard and configure enterprise apps. Global Reader or Report Reader can view the dashboard.	Microsoft Entra admin center (https://entra.microsoft.com)
AD FS administrator	Local administrator on the AD FS and WAP servers, for PowerShell, auditing and the Connect Health agent.	Your Active Directory
Domain Administrator	To enable seamless SSO, which creates the AZUREADSSO computer account.	Your Active Directory
Microsoft Entra ID P1 or P2	Needed for Connect Health and the AD FS application migration wizard.	Microsoft or your partner; check current pricing with them
Microsoft Entra Connect Sync, latest version	Microsoft says upgrading first cuts conversion time from potentially hours to minutes.	Install or upgrade Entra Connect Sync
Connect Health agent for AD FS	On every AD FS and WAP server, to feed usage data to Entra ID.	https://www.microsoft.com/en-us/download/details.aspx?id=108777

Need	Details	Where to get it
PTA authentication agent (PTA only)	Version 1.5.1742.0 or later, on Windows Server 2016 or later.	https://aka.ms/getauthagent
Microsoft Graph PowerShell	For federation settings and domain conversion.	Install Microsoft Graph PowerShell

2 Discover relying parties and back up AD FS

5 steps

1

Export every relying party trust

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

List all relying party trusts, including disabled ones, with their identifiers. Add an owner, protocol and business criticality for each in your app inventory.

```
Get-AdfsRelyingPartyTrust | Select-Object Name,Enabled,@{n="Identifier";e={$_.Identifier -join ";"}},WSFedEndpoint,ProtocolProfile | Export-Csv C:\migration\adfs-rps.csv -NoTypeInformation
```

✓ **You should see:** C:\migration\adfs-rps.csv has one row per trust, including Microsoft Office 365 Identity Platform.

2

Turn on AD FS auditing

Where: Windows PowerShell run as administrator on the primary AD FS server (repeat on each AD FS server)

Connect Health usage data needs AD FS audit logs, which are not fully enabled by default. Check the AD FS service account has **Generate security audits** in Local Security Policy (**Security Settings** > **Local Policies** > **User Rights Assignment**), then run the commands below. In AD FS Management, under **Edit Federation Service Properties** > **Events**, check **Success audits** and **Failure audits** are ticked. Make sure no Group Policy disables AD FS auditing.

```
auditpol.exe /set /subcategory:"Application Generated" /failure:enable /success:enable
Set-AdfsProperties -AuditLevel Verbose
Get-AdfsProperties | Select-Object AuditLevel
```

✓ **You should see:** AuditLevel shows Verbose, and Event Viewer shows events with source AD FS Auditing in the Security log.

3

Install the Connect Health agent for AD FS

Where: Each AD FS and Web Application Proxy server, in a browser and then the installer

Download the agent from `https://www.microsoft.com/en-us/download/details.aspx?id=108777`, run it, select **Install** and sign in with an account allowed to register agents when prompted. Install it on the WAP servers too.

```
Test-MicrosoftEntraConnectHealthConnectivity -Role ADFS
```

✓ **You should see:** The connectivity test passes and the farm appears under AD FS services in Microsoft Entra Connect Health (https://aka.ms/aadconnecthealth).

4

Save the federation settings for rollback

Where: PowerShell 7 on your admin PC, connected with Connect-MgGraph

Record the federation configuration of each federated domain. Look for customised **PreferredAuthenticationProtocol**, **federatedIdpMfaBehavior**, **SupportsMfa** and **PromptLoginBehavior**.

```
Connect-MgGraph -Scopes "Domain.Read.All"
Get-MgDomain | Select-Object Id,AuthenticationType
Get-MgDomainFederationConfiguration -DomainId contoso.com | Format-List * | Out-File
C:\migration\contoso-federation.txt
```

✓ **You should see:** A text file per federated domain with its federation settings.

5

Back up the AD FS farm and Microsoft 365 trust

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

Take a backup with the AD FS Rapid Restore Tool (download and usage on Microsoft's Rapid Restore Tool page), and export the Microsoft 365 relying party trust with its claim rules.

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

✓ **You should see:** A Rapid Restore backup file and C:\temp\O365-RelyingPartyTrust.xml are stored off the server.

3 Choose and prepare the cloud sign-in method

4 steps

Method	How it works	Microsoft's guidance
Password hash sync (PHS)	Entra Connect syncs a hash of the password hash to Entra ID	Recommended. Works if on-premises AD is unavailable

Method	How it works	Microsoft's guidance
Pass-through authentication (PTA)	Agents on-premises check passwords against AD in real time	Use only where regulation forbids syncing password information. At least 3 agents in production
Certificate-based authentication (CBA)	Users sign in with X.509 certificates from your PKI	Phishing-resistant; a replacement for AD FS smart card sign-in
Seamless SSO	Kerberos SSO for domain-joined PCs on the corporate network	For Windows 7 and 8.1; Windows 10 and later use the Primary Refresh Token

1

Enable password hash sync

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

Sign in, step through to **Optional features**, tick **Password hash synchronization**, and complete the wizard with **Configure**. This does not change how federated users sign in yet.

✓ **You should see:** In the Entra admin center under Entra ID > Entra Connect > Connect Sync, Password Hash Sync shows Enabled, and a full password sync cycle completes.

2

Install PTA agents (PTA only)

Where: Two or more domain-joined Windows Server 2016 or later servers that are not the Entra Connect server, in a browser

Download the agent from `https://aka.ms/getauthagent` and install it, signing in when prompted. Microsoft recommends at least three agents in production and allows up to 40 per tenant. Agents need outbound 443 and 80, and access to login.windows.net and login.microsoftonline.com for registration. Treat these servers as Tier 0.

✓ **You should see:** Entra ID > Entra Connect > Connect Sync > Pass-through authentication lists every agent with status Active.

3

Enable seamless SSO if you have older Windows clients

Where: Windows PowerShell run as administrator on the Entra Connect server, in %ProgramFiles%\Microsoft Azure Active Directory Connect

Import the modules, sign in as Hybrid Identity Administrator when the window opens, then enable the forest with domain administrator credentials. Deploy the seamless SSO URLs to the intranet zone by Group Policy as Microsoft's quickstart describes.

```
Import-Module "$env:ProgramFiles\Microsoft Azure AD Sync\Bin\ADSync\ADSync.psd1"
Import-Module .\AzureADSSO.psd1
New-AzureADSSOAuthenticationContext
$creds = Get-Credential
Enable-AzureADSSOForest -OnPremCredentials $creds
Get-AzureADSSOStatus | ConvertFrom-Json
```

✓ **You should see:** Get-AzureADSSOStatus lists your forest under Domains, and an AZUREADSSOACC computer account exists in AD.

4

Check UPN sync for managed users

Where: PowerShell 7 on your admin PC, connected with Connect-MgGraph

Microsoft says the `synchronizeUpnForManagedUsersEnabled` setting must be true after moving to cloud authentication, or UPN changes for licensed users will not sync. Check it now.

```
Connect-MgGraph -Scopes "OnPremDirectorySynchronization.Read.All"
(Get-MgDirectoryOnPremiseSynchronization).Features | Format-List
SynchronizeUpnForManagedUsersEnabled
```

✓ **You should see:** SynchronizeUpnForManagedUsersEnabled : True

4 Replace AD FS access rules and prepare users

3 steps

1

Map AD FS access control policies to Conditional Access

Where: AD FS Management on the AD FS server (Relying Party Trusts > each trust > Edit Access Control Policy), then Microsoft Entra admin center (https://entra.microsoft.com) > Entra ID > Conditional Access > Policies

For each trust, note who is permitted, from which networks, and whether MFA is required. Build matching Conditional Access policies scoped to a pilot group and set to **Report-only**. Add a policy to block legacy authentication, as Microsoft recommends.

✓ **You should see:** Report-only results in the sign-in logs match what AD FS enforces today.

2

Create the pilot groups

Where: Microsoft Entra admin center (https://entra.microsoft.com) > Entra ID > Groups > New group

Create cloud-only security groups with assigned membership for each wave. Staged rollout does not support nested or dynamic groups, and limits a new group to 200 users when you first add it.

✓ **You should see:** Pilot groups exist with direct user members only.

3

Set up branding and MFA registration

Where: Microsoft Entra admin center (https://entra.microsoft.com) > Entra ID > Custom branding, and Entra ID > Authentication methods > Policies

Configure company branding so users recognise the new sign-in page. Enable the methods you want (Microsoft Authenticator, passkeys, Temporary Access Pass) and ask pilot users to register at `https://aka.ms/mysecurityinfo`.

✓ **You should see:** Pilot users show as MFA capable in Authentication methods > User registration details.

5 Pilot with staged rollout

3 steps −

1

Turn on staged rollout for the pilot group

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

Slide **Password Hash Sync** (or **Pass-through authentication**) to **On**, and **Seamless single sign-on** if you use it. Do not combine PHS and PTA. Add the pilot group to each feature. Users in a new group switch straight away; edits to an existing group can take up to 24 hours.

✓ **You should see:** The staged rollout page shows the features On with your pilot group, and the audit log records the change.

2

Issue a Temporary Access Pass to new pilot users

Where: Microsoft Entra admin center (https://entra.microsoft.com) > Entra ID > Users > select the user > Authentication methods > Add authentication method > Temporary Access Pass

A user newly added to staged rollout needs one more AD FS sign-in before managed authentication applies. Microsoft's workaround is a TAP straight after adding them, so they sign in to Entra ID and register their methods without going to AD FS.

✓ **You should see:** The user signs in with the TAP and registers Microsoft Authenticator or a passkey.

3

Validate sign-in outside and inside the network

Where: A private browser window at https://myapps.microsoft.com, then Microsoft Entra admin center (https://entra.microsoft.com) > Entra ID > Monitoring & health > Sign-in logs

Off the corporate network, enter a pilot user's UPN: they should see the Entra sign-in page, not AD FS. On the network with seamless SSO, they should see "Trying to sign you in" and sign in silently. Filter the sign-in logs by the user and check the result. Check the AD FS event logs for any pilot users still reaching AD FS.

✓ **You should see:** Pilot sign-ins succeed in Entra ID and no longer appear in the AD FS logs.

6 Move apps with the AD FS application migration wizard

5 steps

1

Open the AD FS application migration dashboard

Where: Microsoft Entra admin center (https://entra.microsoft.com) > Entra ID > Enterprise apps > Usage & insights > AD FS application migration

The dashboard lists relying parties with sign-ins in the last 1, 7 or 30 days. Use **All apps** to see usage, and select the **Migration status** link for each app to see which configuration and claim rule tests passed. Status is **Ready to migrate**, **Needs review** or **Additional steps required**.

✓ **You should see:** Each active relying party appears with a migration status. Reconcile the list with your PowerShell export from Step 1.

2

Migrate a SAML app with Begin migration

Where: AD FS application migration > Ready to migrate tab > Begin migration

On **Basics** keep or change the app name and optionally pick a gallery template. Review the read-only **User & groups** (taken from the trust's access control policy; groups must be synced), **SAML configurations** (identifier and reply URL) and **Claims** tabs, read **Next steps**, then select **Create** on **Review + create**.

✓ **You should see:** A notification reads Application migration successful, and the app appears on the Ready to configure tab. It stays inactive until the app sends sign-ins to Entra ID.

3

Finish the app configuration and point the app at Entra ID

Where: Ready to configure tab > Configure application in Microsoft Entra, then the app's own admin settings

On the **SAML-based Sign-on** page, add any claims the wizard could not move and download the **Federation Metadata XML** or certificate: the wizard does not migrate the AD FS signing certificate. Add Conditional Access for the app. Follow Microsoft's stages: point a test instance of the app at Entra ID first, then production, by replacing the AD FS metadata or URLs in the app.

✓ **You should see:** Test users reach the app from https://myapps.microsoft.com and their sign-ins appear under the enterprise app's Sign-in logs.

4

Configure OIDC, OAuth, WS-Fed and legacy apps by hand

Where: Microsoft Entra admin center (https://entra.microsoft.com) > Entra ID > App registrations > New registration, or Enterprise apps > New application

Register OAuth 2.0, OpenID Connect and WS-Federation line-of-business apps as app registrations, and custom SAML or WS-Fed apps as non-gallery enterprise apps. Publish apps that use Kerberos or header-based authentication through Microsoft Entra application proxy or a Secure Hybrid Access partner.

✓ **You should see:** Each non-SAML app has an Entra registration and signs in a test user.

5

Disable, then remove, each migrated trust

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

When an app is live on Entra ID, disable its trust first so you can re-enable it quickly if something was missed. Remove it after the app owner signs off.

```
Disable-AdfsRelyingPartyTrust -TargetName "Contoso Payroll"
# after sign-off
Remove-AdfsRelyingPartyTrust -TargetName "Contoso Payroll"
```

✓ **You should see:** The trust no longer appears in AD FS Management, and the app keeps working through Entra ID.

Rollback for a migrated app. The wizard does not clean up after itself. To roll back before the app uses Entra ID, delete the new enterprise application and its app registration.

7 Convert domains from federated to managed

5 steps

1

Check how federation was configured

Where: Microsoft Entra Connect on the sync server (Start > Microsoft Entra Connect > Configure) > Additional tasks > View federation configuration (under Manage Federation)

If the AD FS farm is listed, Entra Connect set it up and you can use Option A below. If not, use Option B with PowerShell.

✓ **You should see:** You know whether to use Option A or Option B.

2

Option A: change user sign-in in Entra Connect

Where: Microsoft Entra Connect on the sync server (Start > Microsoft Entra Connect > Configure) > Change user sign-in

Sign in with a Global Administrator. On **User sign-in** choose **Password hash synchronization** and tick **Do not convert user accounts**, or choose **Pass-through authentication**; tick **Enable single sign-on** if you need seamless SSO. Enter domain administrator credentials on **Enable single sign-on**, keep **Start the synchronization process when configuration completes** ticked and select **Configure**. This converts all federated domains at once.

✓ **You should see:** In the Entra admin center, Entra Connect shows Federation Disabled and your chosen sign-in method Enabled.

3

Option B: convert each domain with Microsoft Graph PowerShell

Where: PowerShell 7 on your admin PC, connected with Connect-MgGraph, out of business hours

For PTA, first confirm every agent shows **Active**, or you risk an outage. Convert one domain at a time, starting with a test domain or the smallest. Allow up to 60 minutes for the change to take effect. If you used PTA, update the sign-in method in Entra Connect afterwards so it recognises PTA as enabled.

```
Connect-MgGraph -Scopes "Domain.ReadWrite.All","Directory.AccessAsUser.All"
Update-MgDomain -DomainId contoso.com -AuthenticationType "Managed"
Get-MgDomain -DomainId contoso.com | Select-Object Id,AuthenticationType
```

✓ **You should see:** AuthenticationType shows Managed, and a user outside the pilot signs in on the Entra sign-in page without reaching AD FS.

4

Turn off staged rollout

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

Microsoft says staged rollout is not a permanent state. Once all domains are managed, slide each feature back to **Off**.

✓ **You should see:** All staged rollout features show Off and sign-ins keep working.

5

Check hybrid joined devices

Where: Command Prompt on a sample of hybrid joined Windows PCs

Run `dsregcmd /status` and check the device still gets a Primary Refresh Token. Microsoft notes Windows 10 earlier than 1903, and users with non-routable UPNs, fell back to AD FS WS-Trust during staged rollout and need attention now. If your hybrid join SCP pointed at AD FS, re-run **Configure device options** in Entra Connect for a managed domain.

```
dsregcmd /status
```

✓ **You should see:** AzureAdJoined : YES and AzureAdPrt : YES on each sample device.

Rollback. To go back, federate the domain again with New-MgDomainFederationConfiguration using the settings saved in Step 1, plus any extra claim rules from the exported Microsoft 365 trust.

8 Decommission AD FS and WAP

6 steps

1

Confirm nothing still uses AD FS

Where: Microsoft Entra Connect Health (https://aka.ms/aadconnecthealth) > AD FS services > your farm, and Event Viewer on each AD FS server

Wait at least one week after moving authentication. Check Connect Health usage and the AD FS event logs for any successful or failed sign-ins. Any traffic means a trust or client still depends on AD FS. When there is none, remove the Microsoft 365 trust.

```
Remove-AdfsRelyingPartyTrust -TargetName "Microsoft Office 365 Identity Platform"
```

✓ **You should see:** No sign-in events for a full week, and no relying party trusts left with traffic.

2

Take a final backup and note the certificate container

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

Optionally take a final Rapid Restore Tool backup. Note the **CertificateSharingContainer** DN; you delete it at the end. If the AD FS configuration database is on SQL Server, delete that database before uninstalling.

```
Get-AdfsProperties | Select-Object CertificateSharingContainer
```

✓ **You should see:** The DN is recorded in your Decommission checklist.

3

Remove load balancer and DNS entries

Where: Your load balancer management console and DNS Manager (dnsmgmt.msc) or public DNS host

Remove AD FS entries from internal and external load balancers, and delete the DNS records for the farm name (for example `sts.contoso.com`).

✓ **You should see:** nslookup sts.contoso.com no longer resolves.

4

Uninstall WAP

Where: Each Web Application Proxy server: Remote Access Management Console, then Windows PowerShell as administrator

Remove any published web applications for AD FS, then uninstall the role.

```
Uninstall-WindowsFeature Web-Application-Proxy,CMAK,RSAT-RemoteAccess
```

✓ **You should see:** The command reports Success and the Remote Access role is gone.

5

Uninstall AD FS, secondary nodes first

Where: Windows PowerShell as administrator on each AD FS server, secondary servers before the primary

Uninstall AD FS and the Windows Internal Database, then delete the database files.

```
Uninstall-WindowsFeature ADFS-Federation,Windows-Internal-Database
del C:\Windows\WID\data\adfs*
```

✓ **You should see:** The feature is removed and no adfs* files remain in C:\Windows\WID\data.

6

Clean up certificates, servers and AD

Where: Certificates console (certlm.msc) on each server, then ADSI Edit (adsiedit.msc) on a domain controller

Delete the AD FS SSL certificates from each server, then re-image the servers with full disk formatting. Delete the AD FS service account. In ADSI Edit, remove the contents of the CertificateSharingContainer DN you recorded.

✓ **You should see:** The Decommission checklist shows servers wiped, the service account deleted and the container emptied.

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 3 options −

Staged rollout, then domain conversion and app waves

MEDIUM EFFORT

Best for: Most organisations with Microsoft 365 and several relying party trusts

+ Pilot groups test cloud sign-in while AD FS stays as fallback
+ App migration wizard handles SAML basics in one click
– Weeks of running both
– Staged rollout group limits and unsupported scenarios to plan around

Read more →

Direct switch with Entra Connect Change user sign-in

LOW EFFORT

Best for: Small organisations whose AD FS farm was set up by Entra Connect and serves only Microsoft 365

+ One wizard converts all federated domains
+ Fewest steps
– Every user changes at once
– Only available if Entra Connect configured AD FS originally

Read more →

Move Microsoft 365 now, keep AD FS for some apps

MEDIUM EFFORT

Best for: Organisations with legacy or header-based apps that cannot move yet

+ Removes the Microsoft 365 outage risk quickly
+ Legacy apps can later move behind Microsoft Entra application proxy
– AD FS and WAP stay patched and monitored meanwhile
– Two identity providers for apps

Read more →

OUR ADVICE

Use staged rollout unless AD FS serves only Microsoft 365 and you can change everyone in one window. If a few apps cannot leave AD FS, convert the domains anyway and keep a small AD FS farm for those apps until they move.

Turn on password hash sync even if you pick pass-through authentication

REDUCES RISK

Microsoft recommends password hash sync for cloud authentication, and the decommission guide says PTA should only be used where regulation forbids syncing password information. If PTA agents or AD fail, PHS gives you a sign-in method you can switch to.

WHAT TO DO

Enable **Password hash synchronization** on Entra Connect's **Optional features** page before the pilot (Step 2), and let a full cycle finish, whichever method you choose.

Microsoft Learn: AD FS decommission guide

Move user sign-in before apps

REDUCES RISK

Microsoft says user authentication and app migration can happen in any order but recommends user authentication first. It removes the Microsoft 365 dependency on AD FS, which is usually the busiest relying party.

WHAT TO DO

Plan the staged rollout pilot and domain conversion (Steps 4 and 6) as the first milestone, and run app waves in parallel or after.

Microsoft Learn: AD FS decommission guide

Do not rely on the migration dashboard alone for your app list

REDUCES RISK

The AD FS application migration dashboard only shows relying parties with user sign-ins in the last 30 days and hides Microsoft relying parties. Quarterly or annual apps (payroll year-end, audit portals) do not appear.

WHAT TO DO

Export every relying party trust with PowerShell (Step 1) and reconcile it against the dashboard. Ask each owner when the app is next used before you mark a trust as unused.

Microsoft Learn: AD FS application migration to move AD FS apps to Microsoft Entra ID

Expect hand work for claims, certificates and non-SAML apps

SAVES TIME

The wizard supports SAML apps only. It does not migrate the signing certificate, Conditional Access, or OIDC, OAuth and WS-Fed configurations, and not every AD FS claim rule translates as-is.

WHAT TO DO

Use the **Migration status** details for each app to see which claim rules need review. Budget time per app to upload the Entra signing certificate or metadata to the app, rebuild missing claims and recreate access rules as Conditional Access.

Microsoft Learn: AD FS application migration to move AD FS apps to Microsoft Entra ID

Find users and devices that staged rollout cannot test

USER IMPACT

Legacy authentication such as POP3 and SMTP is not supported in staged rollout. Windows Hello for Business hybrid certificate trust with AD FS as registration authority and smart card users are not supported. Non-persistent VDI must stay on a federated domain.

WHAT TO DO

Check sign-in logs for legacy protocols, list WHfB certificate trust and smart card users, and plan certificate-based authentication or a separate path for them. Keep non-persistent VDI users federated until you have a supported design.

Microsoft Learn: Migrate to cloud authentication using Staged Rollout

Plan the domain conversion window

USER IMPACT

Microsoft says converting a domain from federated to managed can take up to 60 minutes, and new browser sign-ins may not prompt for credentials during that time.

WHAT TO DO

Convert out of business hours, one domain at a time, starting with a test domain or the one with fewest users, as Microsoft suggests. Modern authentication clients keep working on their refresh tokens.

Microsoft Learn: Migrate from federation to cloud authentication

Decide where MFA happens before you cut over

REDUCES RISK

With a federated domain, MFA may come from AD FS (for example an MFA adapter) or Entra ID. The federatedIdpMfaBehavior setting controls whether Entra ID accepts MFA done by AD FS. After conversion, only Entra MFA applies.

WHAT TO DO

Record the current value with `Get-MgDomainFederationConfiguration` (Step 1). Get users registered for Entra MFA during the pilot and replace AD FS access control policies with Conditional Access before the domain converts.

TOOLS THAT CAN GET AROUND THIS

If AD FS uses a third-party MFA adapter such as Duo, Entra external MFA lets that provider satisfy Entra ID MFA requirements after conversion, so users keep the same second factor instead of re-registering on Entra MFA. It needs Entra ID P1 or P2 for each user.

Microsoft Entra external MFA

Lets users meet an Entra ID MFA requirement with an external provider while Entra ID keeps policy evaluation.

Duo for Microsoft Entra ID external MFA

Duo is recognised as an MFA method in Entra ID and can satisfy Conditional Access. Running the old Duo custom control alongside it can prompt some users twice.

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

Microsoft Learn: Migrate from federation to cloud authentication

AD FS sign-in page customisations do not carry over

USER IMPACT

Microsoft says onload.js customisations cannot be duplicated in Entra ID, and users must sign in with a full UPN or email. Organisation branding is not available on free Entra ID licences unless you have a Microsoft 365 licence.

WHAT TO DO

Set up company branding in Entra ID before the pilot, and tell users that the sign-in page and username format change.

Microsoft Learn: Migrate from federation to cloud authentication

Check password expiry behaviour for synced users

COMPLIANCE

By default, password hash sync sets synced users' cloud passwords to never expire, and staged rollout users get no expiry either. Users with an active session are not prompted to change an expired password.

WHAT TO DO

If users only use cloud services and must follow an expiry policy, review **CloudPasswordPolicyForPasswordSyncedUsersEnabled** in Microsoft's PHS article with your security owner before cutover.

Microsoft Learn: Implement password hash synchronization

Watch for at least a week before removing AD FS

REDUCES RISK

Microsoft's decommission guide says to test for at least one week after moving authentication and to check the AD FS event logs or Connect Health for any sign-in successes or failures, because they mean the servers are still in use.

WHAT TO DO

Keep Connect Health running through that week, review AD FS usage for every remaining trust, and take a final Rapid Restore Tool backup before you uninstall.

Microsoft Learn: AD FS decommission guide

Roll over the seamless SSO key

COMPLIANCE

Seamless SSO creates an AZUREADSSO computer account whose Kerberos key does not roll over by itself. Microsoft recommends rolling it over at least every 30 days.

WHAT TO DO

Add the rollover to your operations calendar, or use PRT-based SSO on Windows 10 and later, which Microsoft recommends for those devices.

Microsoft Learn: Migrate from federation to cloud authentication

Find a new home for apps published through Web Application Proxy

USER IMPACT

Web Application Proxy often publishes internal web apps that use Windows Integrated Authentication through Kerberos constrained delegation. Microsoft's decommission guide tells you to remove the published web applications before you uninstall WAP, but it does not move them anywhere, and the app migration wizard only handles SAML apps.

WHAT TO DO

Open the Remote Access Management Console on each WAP server and list every published application that is not an AD FS endpoint. Give each one a replacement publishing path and test it externally before you remove WAP.

TOOLS THAT CAN GET AROUND THIS

Microsoft Entra application proxy publishes the same internal apps through Entra ID, with Kerberos constrained delegation for Integrated Windows Authentication apps and outbound-only connectors instead of WAP. An identity orchestration product can also move users of an app from AD FS to Entra ID in groups.

Microsoft Entra application proxy

Publishes on-premises web apps, including Kerberos (IWA) and form-based apps, through outbound-only private network connectors.

Strata Maverics Identity Orchestration

Routes each sign-in to AD FS or Entra ID depending on whether the user has moved, so an app follows your user waves. Changes go in Maverics configuration, not application code.

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

Microsoft Learn: AD FS decommission guide

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
Every relying party trust is accounted for	Compare the `C:\migration\adfs-rps.csv` export from Step 1 with the AD FS application migration dashboard (Entra ID > Enterprise apps > Usage & insights) and your Application inventory and dependency map.	Each trust is marked migrated, disabled, or kept with a named owner and date; none are unexplained.
Domains are managed	In PowerShell 7 connected to Microsoft Graph, run `Get-MgDomain | Select-Object Id,AuthenticationType`.	Every domain you converted shows Managed; staged rollout features are back to Off.

Check	How to check	What good looks like
Users sign in on the Entra page with MFA, on and off the network	In a private browser at https://myapps.microsoft.com, sign in as test users off the corporate network, then on it with seamless SSO. In the Microsoft Entra admin center, filter the sign-in logs by those users.	Users see the branded Entra sign-in page (or sign in silently on the network), MFA and Conditional Access apply, and no sign-in reaches AD FS.
Password hash sync and UPN sync are working	In the Microsoft Entra admin center check the last sync time on the Entra Connect page. Run `(Get-MgDirectoryOnPremiseSynchronization).Features | Format-List SynchronizeUpnForManagedUsersEnabled` and test a UPN change on a test user.	Password sync is current, SynchronizeUpnForManagedUsersEnabled is True and the UPN change appears in Entra ID after the next cycle.
PTA agents are active (PTA only)	In the Microsoft Entra admin center open Entra Connect > Pass-through authentication and review the agent list.	At least the number of agents you planned show Active, on separate servers.
Migrated apps accept Entra ID tokens	For each migrated app, sign in from https://myapps.microsoft.com as a test user from each role group, and check the sign-in log entry for the enterprise application.	Sign-in succeeds with the expected claims and roles; the app owner signs off in the pilot test plan.
Outlook, Teams and OneDrive clients stay signed in	After domain conversion, restart a sample of PCs and phones and open Outlook, Teams and OneDrive.	Modern authentication clients keep working or prompt once for the Entra sign-in page.
Hybrid joined devices still get a Primary Refresh Token	On a sample of hybrid joined PCs, run `dsregcmd /status` in Command Prompt.	AzureAdPrt is YES on every sampled device.

Check	How to check	What good looks like
AD FS receives no traffic	Check Microsoft Entra Connect Health (https://aka.ms/aadconnecthealth) > AD FS services > your farm, and the AD FS event logs, for at least one week after the conversion.	No successful or failed sign-ins appear in Connect Health or the event logs.

Rollback plan

If it goes wrong

ROLL BACK IF

- Users cannot sign in after a domain converts and the cause is not fixed within the change window
- PTA agents go inactive and users fail to sign in
- A migrated app rejects SAML responses and the app owner cannot fix it on the day
- Hybrid joined devices stop receiving a Primary Refresh Token after conversion

POINT OF NO RETURN

Until you uninstall AD FS, every change here is reversible: apps can be pointed back at AD FS and domains can be federated again from your saved settings. Removing the Microsoft 365 relying party trust, uninstalling AD FS and WAP, deleting the farm DNS records and certificates, and cleaning the CertificateSharingContainer is the point of no return. After that, going back means building a new farm.

1

Pull pilot users out of staged rollout

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

Remove the affected group from each feature, or slide the feature to Off.

✓ **You should see:** Affected users are sent to the AD FS sign-in page again.

2

Re-enable a disabled relying party trust

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

Run `Enable-AdfsRelyingPartyTrust -TargetName "Contoso Payroll"`, then restore the AD FS metadata or URLs in the app's own admin settings.

✓ **You should see:** Users sign in to the app through AD FS and the AD FS event log shows the sign-ins.

3

Clean up a part-migrated app

Where: Microsoft Entra admin center (https://entra.microsoft.com) > Entra ID > Enterprise apps and App registrations

The migration wizard does not clean up after itself. If the app never switched to Entra ID, delete the enterprise application and its app registration.

✓ **You should see:** The app no longer appears in Enterprise apps or App registrations.

4

Federate the domain again

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

Run `New-MgDomainFederationConfiguration` with the values saved in `C:\migration\contoso-federation.txt`, then add any extra claim rules from the exported Microsoft 365 trust. If Entra Connect manages the farm, you can instead use Change user sign-in and select Federation with AD FS.

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

5

Restore the AD FS farm if it was damaged

Where: The primary AD FS server, using the AD FS Rapid Restore Tool

Restore the backup you took in Step 1 as described on the Microsoft Learn AD FS Rapid Restore Tool page, then re-import the Microsoft 365 trust from `O365-RelyingPartyTrust.xml` if needed.

✓ **You should see:** AD FS Management shows the farm, its trusts and certificates.

6

Record what cannot be undone

Where: Your Rollback plan and Decommission checklist

Note that removed trusts, an uninstalled farm, deleted certificates and the cleaned CertificateSharingContainer cannot be recovered without the Rapid Restore backup or a rebuild. Do not start the decommission section until the rollback period has ended.

✓ **You should see:** The decommission start date is after the agreed rollback period, signed off by the change owner.

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

Common problems and fixes

7 errors −

`Users cannot sign in after converting the domain to PTA`

Cause: PTA agents were not Active, or were blocked from reaching Entra ID.

Fix: Check agent status under Pass-through authentication, fix connectivity, or switch the sign-in method to password hash sync if it is already synced.

`UPN changes no longer sync for licensed users`

Cause: synchronizeUpnForManagedUsersEnabled is false.

Fix: Enable the feature as described in Microsoft's Entra Connect sync service features article.

`An app is missing from the AD FS application migration dashboard`

Cause: It had no sign-ins in the last 30 days, it is a Microsoft relying party, or Connect Health or AD FS auditing is not set up.

Fix: Install the agent on every AD FS and WAP server, turn on verbose auditing, and configure the app by hand if it is rarely used.

`App rejects the SAML response after migration (signature or certificate error)`

Cause: The wizard does not migrate the AD FS signing certificate.

Fix: Upload the Entra federation metadata or signing certificate to the app.

`Pilot users are still sent to AD FS`

Cause: The app sends a domain_hint, the client uses legacy authentication, or the user needs one more federated sign-in after being added.

Fix: Test domain_hint apps after conversion, move clients to modern authentication, and use a Temporary Access Pass for new pilot users.

`Hybrid joined device has no PRT after conversion`

Cause: Windows 10 earlier than 1903, or the user's UPN is not routable, so the device relied on AD FS WS-Trust.

Fix: Update Windows, fix the UPN suffix to a verified domain, and re-check with dsregcmd /status.

`Users with expired AD passwords are not asked to change them in the cloud`

Cause: PHS sets synced users to never expire in the cloud by default.

Fix: Review CloudPasswordPolicyForPasswordSyncedUsersEnabled with your security owner.

Search the full error library →

FAQ

Frequently asked questions

Should I move apps or users off AD FS first?

Microsoft says either order works but recommends migrating user authentication first.

Password hash sync or pass-through authentication?

Microsoft recommends password hash sync. Its decommission guide says PTA should only be used where regulation forbids syncing password information.

What happened to the AD FS application activity report?

It is now the AD FS application migration dashboard under Enterprise apps > Usage & insights in the Entra admin center, which also includes a one-click SAML migration wizard.

Does the AD FS migration wizard move OIDC or WS-Fed apps?

No. It supports SAML apps only. Configure OIDC, OAuth and WS-Fed apps as app registrations or enterprise apps by hand.

How long should I wait before decommissioning AD FS?

Microsoft says to test for at least one week after moving authentication and to confirm no sign-ins still reach AD FS.

Can I roll back the domain conversion?

Yes. Federate the domain again with New-MgDomainFederationConfiguration using the federation settings you documented before the change.

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: Migrate from federation to cloud authentication
- Microsoft Learn: Migrate to cloud authentication using Staged Rollout
- Microsoft Learn: AD FS application migration to move AD FS apps to Microsoft Entr...
- Microsoft Learn: Overview of AD FS application migration
- Microsoft Learn: Stages of migrating application authentication from AD FS
- Microsoft Learn: Configure SAML-based single sign-on (AD FS migration)
- Microsoft Learn: Monitor AD FS using Microsoft Entra Connect Health
- Microsoft Learn: Pass-through authentication quickstart
- Microsoft Learn: Implement password hash synchronization
- Microsoft Learn: AD FS decommission guide
- Microsoft Learn: AD FS Rapid Restore Tool
- Microsoft Learn: Configure Microsoft Entra hybrid join