RUNBOOK · EMAIL AND DOMAINS

# How to move a custom domain from one Microsoft 365 tenant to another

A domain can only be verified in one Microsoft 365 tenant at a time. This runbook shows how to release it from the source, verify it in the target and keep the window where mail has nowhere to go as short as possible.

Updated 4 Nov 2026  6 phases  26 detailed steps  7 official sources

START HERE

## How do you move a custom domain from one Microsoft 365 tenant to another?

SHORT ANSWER

This moves your email domain (such as contoso.com) from one Microsoft 365 tenant (your organisation's own Microsoft 365 setup) to another, usually as the last step of a Microsoft 365 tenant-to-tenant move. A domain can be in only one tenant at a time, so you take it off every user, group and address in the old tenant, remove it, then add and verify it in the new one.

- **Recommended route:** Planned cutover window: remove, then add
- **Order:** Get both tenants ready before the window, then remove, add and fix mail records, in that order.
- **6 phases:** Plan the window, Find everything using it, Release the domain, Verify in the new tenant, Fix DKIM and DMARC and Test and finish.
- **You're done when:** The domain is verified in the new tenant and gone from the old one.

Mail to the domain cannot be delivered between those two moments. Microsoft says removal takes from five minutes to about a day, depending on how many objects use the domain, so script it, rehearse it and pick a quiet window.

RECOMMENDED ROUTE

**Planned cutover window: remove, then add**

It is the method Microsoft documents and needs no extra service. Clearing every reference beforehand keeps the mail gap short.

▼ **Other options and when to use them**

- **Cutover with a mail queuing service in front, such as Cloudiway Mail Routing**
  : Senders must not see failures during the window.
- **Adopt a different domain in the new tenant**
  : A rebrand, or the old domain stays with the old organisation.
- **Move only a subdomain**
  : Only one business unit is moving and can use an address such as au.contoso.com.

**TOOLS FOR THIS PLAN**

**Are you ready?**
22-question readiness check

**Plan your dates**
Dated countdown you can add to your calendar

**Compare options**
Compare Microsoft 365 migration tools

**Check your DNS**
MX, SPF, DKIM and DMARC lookup

**New to the jargon?**
Plain-English migration glossary

**ORDER TO MIGRATE IN, AND WHY**

Get both tenants ready before the window, then remove, add and fix mail records, in that order. Each step needs the one before it: the new tenant cannot verify the domain until the old tenant has fully let it go.

1. **New tenant ready: users, mailboxes and groups on onmicrosoft.com addresses, with content copied**
   Only a final top-up copy is left on the night, which keeps the window short.
2. **TTLs lowered, and a spare admin on the onmicrosoft.com domain in the old tenant**
   Short TTLs make the DNS change take effect quickly, and you need an admin whose own sign-in is not on the domain you remove.
3. **Inventory of every object using the domain, and a rehearsed renaming script**
   Removal fails while anything still uses the domain, and finding stragglers during the window lengthens the mail gap.
4. **Users synced from on-premises Active Directory renamed there**

Cloud renames of synced users are blocked, and the next sync puts the old domain back.

5 **Old tenant: rename everything, then remove the domain**

The new tenant refuses or cannot verify the domain until it is gone.

6 **New tenant: verify, publish MX, Autodiscover and SPF, assign addresses**

Mail starts flowing as soon as MX points at the new tenant.

7 **DKIM and DMARC**

DKIM keys belong to the tenant, so the new tenant needs its own before its mail is signed.

8 **Tests, final mailbox top-up and old licences**

Mail that reached the old tenant before the switch is copied last, and old licences go only after retention needs are met.

**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)

- [ ] **TTL on mail records**

  How low to set the TTL (time to live: how long other servers cache a DNS record) and when.

  ▼ How each tool handles it

  | | |
  |---|---|
  | **Built-in method** | Your DNS host controls it, not Microsoft 365. Lower MX, Autodiscover, SPF and DKIM records to 300 seconds or your host's minimum at least one full old TTL period before the window. Lowering it on the night does not help servers that cached the old value. |

  **Tip:** Read the current TTL from your nameserver a week ahead, and diarise the change.

- [ ] **Every object that uses the domain**

  How you find and rename every sign-in name, address, alias, group, contact and app that uses the domain.

  ▼ How each tool handles it

  | | |
  |---|---|
  | **Built-in method** | Microsoft 365 will not remove a domain while anything still uses it, including secondary aliases and app ID URIs (the |

| | |
|---|---|
| | web addresses apps are registered under). Microsoft leaves you to clear them; it recommends PowerShell for hundreds of users. |
| **Quest On Demand Migration** | Domain Move removes the domain from old objects and adds it to matched new objects at cutover. You still change MX records when it prompts you. |

**Tip:** Write one script that reads your inventory CSV, test it on a spare domain, and run the inventory again the day before.

Microsoft Learn: Remove a domain

- [ ] **Users synced from Active Directory**

Whether synced users are renamed in on-premises Active Directory ahead of the window, or sync is turned off.

▼ **How each tool handles it**

| | |
|---|---|
| **Built-in method** | Cloud attributes of synced users are read-only. You cannot rename them in the old tenant, and Entra Connect puts the old domain back on the next sync if you try. |

**Tip:** Count synced users with Get-MgUser -Property OnPremisesSyncEnabled before you plan the window.

Microsoft Learn: Remove a domain

- [ ] **Force delete**

Whether force delete is allowed as a last resort, and with which settings.

▼ **How each tool handles it**

| | |
|---|---|
| **Built-in method** | Entra ID force delete renames whatever still uses the domain to the onmicrosoft.com domain and, by default, disables those user accounts. It refuses more than 1,000 references, federated domains and domains bought through Microsoft 365. |

**Tip:** Clear references yourself. If you must use force delete through Graph, set disableUserAccounts to false.

Microsoft Graph: domain forceDelete

- [ ] **Federated domains**

Whether the domain uses federation, and when you convert it.

▼ **How each tool handles it**

| | |
|---|---|
| **Built-in method** | A domain federated with AD FS (sign-in handled by your own servers) must be converted to managed sign-in in the old tenant first. Force delete does not work on federated domains. |

**Tip:** Convert the domain a week before the window, and test sign-in afterwards.

Microsoft Graph: domain forceDelete

- [ ] **Mail during the gap**

How long a gap is acceptable, and whether a service holds mail during it.

▼ **How each tool handles it**

| | |
|---|---|
| **Built-in method** | Microsoft 365 accepts mail for the domain nowhere while it is in neither tenant. Most sending servers retry temporary failures for a while, but a long removal or a slow DNS change turns delays into bounces. |
| **Cloudiway Mail Routing** | MX points to Cloudiway before you remove the domain, mail is queued, then MX returns to Microsoft 365. Meant for about 48 hours, and DMARC needs adjusting while it routes mail. |
| **Quest On Demand Migration** | Domain Move uses a relay service to keep inbound mail flowing while addresses move. |

**Tip:** Tell users and key customers the window in writing, and pick a time when inbound mail is low.

Microsoft Learn: Manage custom domain names in Microsoft Entra ID

- [ ] **Admin accounts**

Which admin accounts run the cutover in each tenant.

▼ **How each tool handles it**

| | |
|---|---|
| **Built-in method** | Microsoft warns not to change your own sign-in name if you are the only Global Administrator on the domain. An admin on the onmicrosoft.com domain keeps working when the domain goes. |

**Tip:** Create and test an onmicrosoft.com Global Administrator in both tenants before the window.

Microsoft Learn: Remove a domain

- [ ] **Verification record**

Who publishes the new TXT record and when.

▼ How each tool handles it

**Built-in method** The new tenant shows its own MS=ms TXT record. Replace the old tenant's record with it. Microsoft says verification can take up to 30 minutes after the record is added.

**Tip:** Choose "I'll add the DNS records myself" so you control the MX change.

Microsoft Learn: Add a domain to Microsoft 365

- [ ] **MX, Autodiscover and SPF values**

Which values you publish, copied from the new tenant.

▼ How each tool handles it

**Built-in method** Copy the values the new tenant's DNS records tab shows. The MX value for the new tenant can differ from the old one. Keep a single SPF record (the list of services allowed to send as your domain).

**Tip:** Keep the old values in your DNS record sheet for rollback.

Microsoft Learn: Add a domain to Microsoft 365

- [ ] **DKIM signing**

When you create keys in the new tenant and publish their records.

▼ How each tool handles it

**Built-in method** DKIM keys (signatures that prove mail is really from you) belong to the tenant. Mail from the new tenant is unsigned until its two selector CNAME records are published and signing is turned on.

**Tip:** Create the keys disabled, publish both CNAMEs, then turn signing on.

Microsoft Learn: Set up DKIM for your custom domain

- [ ] **DMARC policy**

Whether to relax DMARC for the weekend.

▼ How each tool handles it

**Built-in method** DMARC (your policy telling receivers how to treat mail that fails checks) is a DNS record and does not move with the tenant. At p=reject, mail that is unsigned and fails SPF can be rejected, including your own.

**Tip:** Update SPF first, and consider p=quarantine or p=none for the weekend, then restore it once DKIM signs.

Microsoft Learn: Set up DMARC

- [ ] **Subdomain instead of the whole domain**
  Whether the moving users could live on a subdomain such as au.contoso.com.

  ▼ **How each tool handles it**

  | | |
  |---|---|
  | **Built-in method** | Microsoft lets a subdomain be verified in a different tenant from its parent domain, so moving only a subdomain avoids removing the parent and the mail gap. |

  **Tip:** Check this before you plan a full domain move.

  Microsoft Learn: Manage custom domain names in Microsoft Entra ID

- [ ] **What the domain does not carry**
  Which links and partner settings need updating after the move.

  ▼ **How each tool handles it**

  | | |
  |---|---|
  | **Built-in method** | SharePoint and OneDrive addresses use the tenant's onmicrosoft.com name, not your domain, so they change. Guest accounts, sharing links and Teams federation in other organisations still point at the old tenant. |

  **Tip:** Ask partners to re-invite your users as guests, and list link changes in the user communication pack.

- [ ] **Licence overlap**
  When old tenant licences are removed.

  ▼ **How each tool handles it**

  | | |
  |---|---|
  | **Built-in method** | Both tenants need licences until the final top-up copy and any retention or legal hold period end. |

  **Tip:** Agree the removal date with your licensing partner and put it in the runsheet.

## THE PLAN, PHASE BY PHASE

### 1 Plan the window — One to two weeks before

Pick a quiet weekend or

evening and freeze new users, groups and aliases on the domain.

Lower the TTL (how long other servers cache a record) on MX, Autodiscover, SPF and DKIM at least one old TTL period before.

Create users, shared mailboxes and groups in

the new tenant, and pre-copy mailbox content.

Create a Global Administrator in the old tenant on the onmicrosoft.com domain and test it.

Decide how to handle mail during the gap, and tell users and key contacts.

> ⚠ **Watch out:** Microsoft 365 cannot accept mail for the domain while it is in neither tenant, and a long gap turns delays into bounces.

**WAYS AROUND IT**

- Keep the window short and quiet. Most sending servers retry temporary failures.

**TOOLS THAT CAN DO IT**

**Cloudiway Mail Routing**
MX points to Cloudiway before you remove the domain, mail is queued, then MX returns to Microsoft 365. Meant for about 48 hours, and DMARC needs adjusting.

**Watch out:** Both tenants need licences at once until the final top-up copy and any retention period end.

**WAYS AROUND IT**

- Agree the old licence removal date with your licensing partner and put it in the runsheet.

**Check your DNS records before and after the change**

**Show the detailed steps (5) →**

## 2 Find everything using it

**Before the window, and again the day before**

Export every recipient with an address on the domain, including secondary aliases.

List users whose sign-in name uses the domain, and

note which sync from Active Directory.

Change app registration ID URIs that use the domain to the onmicrosoft.com domain.

Script the renaming from your inventory and test it on a spare domain or subdomain.

> **Watch out:** Users synced from on-premises Active Directory cannot be renamed in the cloud, and sync puts the old domain back.
>
> **WAYS AROUND IT**
>
> - Change their sign-in names and addresses in Active Directory ahead of the window, or turn off sync as a planned step.

**Watch out:** Microsoft leaves you to clear every reference to the domain yourself.

**WAYS AROUND IT**

- Run the renaming as one rehearsed script that reads your inventory CSV.

**TOOLS THAT CAN DO IT**

**Quest On Demand Migration**
Domain Move swaps addresses from old to matched new objects and relays inbound mail while they move.

Show the detailed steps (3) →

## 3 Release the domain

Start of the window

Move every user's sign-in name to the onmicrosoft.com domain with PowerShell.

Change primary addresses and remove aliases on mailboxes, groups and distribution lists.

Remove or update

mail contacts and mail users on the domain.

Re-run the inventory and continue only when it returns nothing.

Remove the domain in the old tenant's admin center and confirm it has gone.

> **Watch out:** Entra ID force delete (a last-resort removal) renames whatever still uses the domain and, by default, disables those accounts. It refuses federated domains, domains bought through Microsoft 365 and more than 1,000 references.
>
> **WAYS AROUND IT**

- Clear every reference yourself and keep force delete as a last resort, with disableUserAccounts set to false.

**Show the detailed steps (5) →**

## 4 Verify in the new tenant

Add the domain in the new tenant and publish its MS=ms TXT record, replacing the old one.

Select Verify. It can take up to 30 minutes after the record is added.

Copy MX, Autodiscover

and SPF from the new tenant's DNS records tab, keeping one SPF record.

Set the domain as the sign-in name and primary address on users, shared mailboxes and groups.

> **Watch out:** The MX value for the new tenant can differ from the old one.
>
> **WAYS AROUND IT**
>
> - Always copy the value the new tenant shows, never the old record.

**Show the detailed steps (4) →**

## 5 Fix DKIM and DMARC

Create DKIM

keys in the new tenant, publish its two selector CNAMEs, then turn signing on.

Check your DMARC record is still published with the policy you expect.

> **Watch out:** DKIM keys belong to the tenant, so mail from the new tenant is unsigned until the new CNAMEs are live. With DMARC at reject, your own mail can be rejected.
>
> **WAYS AROUND IT**
>
> - Update SPF first, and consider setting DMARC to quarantine or none for the weekend, then restore it.

**Show the detailed steps (2) →**

## 6 Test and finish

End of the window

Send test mail

in and out and check the headers show spf=pass and dkim=pass.

Run the final mailbox top-up copy so mail that reached the old tenant is copied across.

Help users set up Outlook, phones and Teams again for the new tenant.

Remove old tenant licences only after retention and legal hold needs are met.

> **Watch out:** File links, guest accounts and Teams federation in other organisations still point at the old tenant.
>
> **WAYS AROUND IT**
>
> - Ask partners to re-invite your users as guests, and list link changes in the user communication pack.

> **Watch out:** Once the domain leaves the old tenant, going back repeats the mail gap, and bounced mail is not recovered.
>
> **WAYS AROUND IT**
>
> - Make the go / no-go call before you remove the domain, and keep your DNS record sheet for rollback.

**Show the detailed steps (4) →**

### You are finished when

- The domain is verified in the new tenant and gone from the old one.
- MX, Autodiscover and SPF point at the new tenant, and DKIM is signing.
- Every user, shared mailbox and group has its usual address, and users sign in with it.
- Mail flows both ways and no new mail reaches the old tenant.

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

Microsoft will not let the same domain be verified in two Entra tenants. To move `contoso.com` you have to remove it from every object in the source tenant, delete it from the source, then add and verify it in the target. Between those two moments the domain belongs to neither tenant and mail sent to it cannot be delivered to either.

This guide is the domain cutover part of a larger move. For mailboxes, OneDrive, SharePoint and Teams, follow the Microsoft 365 tenant-to-tenant guide and use this page on the night of the cutover.

RULE
**A domain can be verified in only one Microsoft Entra tenant**

REMOVAL TIME
**Minutes to about a day, depending on how many objects reference it**

FORCE DELETE
**Available for fewer than 1,000 references; Exchange objects must be cleared first**

MAIL GAP
**Unavoidable while the domain is in neither tenant; plan a short, quiet window**

FULL TENANT MOVE
**See the M365 tenant-to-tenant guide**

### 1 What you need before step one

| Need | Details | Where to get it |
|---|---|---|
| Global Administrator in both tenants | Sign in to the source with an account on the onmicrosoft.com domain, not the domain you are moving. | Microsoft 365 admin center, https://admin.microsoft.com |
| Exchange Online PowerShell | To find and change every address on the domain. | Install the module and connect |
| Microsoft Graph PowerShell | To find and rename user sign-in names and remove the domain. | Install Microsoft Graph PowerShell |
| DNS access | To change MX, Autodiscover, SPF, DKIM and the verification TXT record. | Your registrar or DNS host |
| Target mailboxes ready | Users, shared mailboxes and groups already created in the target and pre-staged with content. | Cross-tenant mailbox migration guide |
| A record sheet | Current DNS values and your inventory CSVs, for rollback. | DNS cutover record sheet template |

## 2 Plan the cutover window

5 steps

1

### Pick a quiet window and freeze changes

**Where: Your Cutover runsheet and change calendar**

Choose a weekend or evening when inbound mail is low. Freeze new users, groups and aliases in the source from the start of the window, and tell the helpdesk not to create objects on the domain.

✓ **You should see:** The runsheet has a start time, an end time and a named owner for each step, and the freeze is announced.

2

## Lower DNS TTLs in advance

**Where: Your DNS host's control panel > your domain > DNS records > Edit (per record)**

Lower the TTL on MX, Autodiscover, SPF and DKIM records to 300 seconds or your host's minimum at least one full TTL period before the window, so the new values take effect quickly. Follow lower DNS TTL before a migration.

```
nslookup -debug -type=mx contoso.com 8.8.8.8
```

✓ **You should see:** The ttl = value returned is at or below the new TTL.

3

## Prepare the target tenant first

**Where: Microsoft 365 admin center (admin.microsoft.com) of the TARGET tenant > Users > Active users, plus your migration tool**

Create users, shared mailboxes and groups in the target using the `.onmicrosoft.com` domain (see bulk create users). Pre-stage mailbox content with your migration tool so only a final sync is left.

✓ **You should see:** Every user in the inventory has a matching target account and the migration tool shows the initial sync complete.

4

### Make sure you have a second admin on another domain

**Where: Microsoft 365 admin center (admin.microsoft.com) of the SOURCE tenant > Users > Active users > Add a user**

At least one Global Administrator must sign in with an `.onmicrosoft.com` address, for example `admin@contoso.onmicrosoft.com`. Microsoft warns not to change your own username if you are the only Global Administrator on the domain. Create the account, assign the Global Administrator role under **Roles**, and test sign-in in a private browser window.

✓ **You should see:** You can sign in to the source admin center as an onmicrosoft.com Global Administrator.

5

### Decide how to handle mail during the gap

**Where: Your Cutover runsheet and User communication pack**

Options: accept that some senders get a temporary failure and retry, or put a third-party mail filtering or queuing service in front for the window so mail is held and delivered once the target is ready. Tell users and key customers in advance.

✓ **You should see:** The runsheet records the chosen approach, and the notice has gone to users and key contacts.

**Subdomains.** Microsoft allows a subdomain such as `au.contoso.com` to be verified in a different tenant from `contoso.com`. If you only need to move a subdomain, you may not need to remove the parent.

## 3 Find every object that uses the domain

3 steps

Removal fails while any user, group, contact, alias or app still references the domain. Find them all before the window.

1

## List Exchange recipients with the domain

**Where: PowerShell on your admin PC, connected with Connect-ExchangeOnline to the SOURCE tenant**

This includes secondary aliases, which are easy to miss in the admin center. It covers mailboxes, shared and resource mailboxes, contacts, distribution lists and Microsoft 365 groups.

```
Connect-ExchangeOnline -UserPrincipalName admin@contoso.onmicrosoft.com
Get-Recipient -ResultSize Unlimited | Where-Object { $_.EmailAddresses -like "*@contoso.com" } |
Select-Object Name,RecipientTypeDetails,PrimarySmtpAddress | Export-Csv C:\migration\contoso-
recipients.csv -NoTypeInformation
```

✓ **You should see:** C:\migration\contoso-recipients.csv lists every recipient with an address on the domain and its RecipientTypeDetails.

2

## List users whose sign-in name uses the domain

**Where: PowerShell on your admin PC, connected with Connect-MgGraph to the SOURCE tenant**

Use Microsoft Graph PowerShell. The last command asks Entra which objects still reference the domain.

```
Connect-MgGraph -Scopes "User.ReadWrite.All","Domain.ReadWrite.All"
Get-MgUser -All -Property UserPrincipalName,OnPremisesSyncEnabled | Where-Object {
$_.UserPrincipalName -like "*@contoso.com" } | Select-Object
UserPrincipalName,OnPremisesSyncEnabled
Get-MgDomainNameReference -DomainId contoso.com -All | Format-List Id,AdditionalProperties
```

✓ **You should see:** A list of users to rename, with OnPremisesSyncEnabled True marking users you must change in Active Directory.

3

### Check apps and synced objects

**Where: Microsoft Entra admin center (entra.microsoft.com) > Entra ID > App registrations > each app > Expose an API; and Active Directory Users and Computers for synced users**

App registrations with an app ID URI on the domain also block removal. Change those URIs to the onmicrosoft.com domain. If users are synced from on-premises Active Directory, change their UPN and proxy addresses there, not in the cloud, and let sync run.

✓ **You should see:** No application ID URI contains contoso.com, and synced users show the new UPN after the next sync cycle.

## 4 Move source objects off the domain

5 steps

1

### Change user sign-in names

**Where: PowerShell on your admin PC, connected with Connect-MgGraph to the SOURCE tenant (cloud-only users)**

Move users to the `.onmicrosoft.com` domain. Microsoft recommends PowerShell for hundreds or thousands of users so none are missed. Loop over your inventory CSV rather than typing each one.

```
Update-MgUser -UserId user@contoso.com -UserPrincipalName user@contoso.onmicrosoft.com
```

✓ **You should see:** Re-running the Get-MgUser command from Step 2 returns no users on contoso.com.

2

## Change primary addresses and remove aliases

**Where: PowerShell on your admin PC, connected with Connect-ExchangeOnline to the SOURCE tenant**

Set the primary SMTP address to the onmicrosoft.com domain, then remove any remaining proxy addresses on the custom domain. Repeat for shared and resource mailboxes.

```
Set-Mailbox -Identity user@contoso.onmicrosoft.com -WindowsEmailAddress
user@contoso.onmicrosoft.com
Set-Mailbox -Identity user@contoso.onmicrosoft.com -EmailAddresses
@{remove="smtp:user@contoso.com"}
```

✓ **You should see:** Get-Mailbox user@contoso.onmicrosoft.com | Select-Object -ExpandProperty EmailAddresses shows no contoso.com address.

3

## Change groups and distribution lists

**Where: PowerShell on your admin PC, connected with Connect-ExchangeOnline to the SOURCE tenant**

Microsoft 365 groups, Teams-connected groups and distribution lists all need a new primary address and their old aliases removed.

```
Set-UnifiedGroup -Identity sales@contoso.com -PrimarySmtpAddress sales@contoso.onmicrosoft.com
Set-UnifiedGroup -Identity sales@contoso.onmicrosoft.com -EmailAddresses
@{remove="smtp:sales@contoso.com"}
Set-DistributionGroup -Identity staff@contoso.com -PrimarySmtpAddress
staff@contoso.onmicrosoft.com
Set-DistributionGroup -Identity staff@contoso.onmicrosoft.com -EmailAddresses
@{remove="smtp:staff@contoso.com"}
```

✓ **You should see:** The groups show only onmicrosoft.com addresses.

4

### Remove mail contacts and mail users on the domain

**Where: PowerShell on your admin PC, connected with Connect-ExchangeOnline to the SOURCE tenant**

Delete or update any mail contacts or mail users whose external address is on the domain.

```
Get-MailContact -ResultSize Unlimited | Where-Object { $_.ExternalEmailAddress -like
"*@contoso.com" } | Remove-MailContact
Get-MailUser -ResultSize Unlimited | Where-Object { $_.ExternalEmailAddress -like "*@contoso.com"
} | Format-Table Name,ExternalEmailAddress
```

✓ **You should see:** No mail contact is left on the domain, and you have a list of mail users to update or remove.

5

### Re-run the inventory

**Where: The same Exchange Online and Graph PowerShell sessions**

Run the Step 2 commands again. Continue only when they return nothing.

✓ **You should see:** Get-Recipient, Get-MgUser and Get-MgDomainNameReference return no results for contoso.com.

## 5 Remove the domain from the source tenant

3 steps −

1

## Remove the domain in the admin center

**Where: Microsoft 365 admin center (admin.microsoft.com) of the SOURCE tenant > Show all > Settings > Domains**

Select the domain, then **Remove domain** in the properties pane, then **Remove domain** again in the **Remove domain?** pane. If the domain is the default, first select another domain and choose **Set as default**. Microsoft says removal can take five minutes if few objects reference the domain, or several hours up to a day if many do. Full detail is in remove a domain from Microsoft 365.

```
Remove-MgDomain -DomainId contoso.com
```

✓ **You should see:** The domain disappears from the Domains list.

2

## Use force delete only as a fallback

**Where: Microsoft Entra admin center (entra.microsoft.com) > Entra ID > Domain names > Custom domain names, or Microsoft Graph**

Entra ID can force delete a domain, renaming remaining users, groups and apps to the default domain. It only works with fewer than 1,000 references, Exchange-provisioned groups must be cleared in the Exchange admin center first, and it does not work for federated domains or domains bought through Microsoft 365. Force delete disables the renamed user accounts by default, which you probably do not want mid-migration; in Graph, set `disableUserAccounts` to false.

```
POST https://graph.microsoft.com/v1.0/domains/contoso.com/forceDelete
{ "disableUserAccounts": false }
```

✓ **You should see:** The operation runs in the background. A later GET for the domain returns HTTP 404.

3

### Confirm the domain is gone

**Where: PowerShell on your admin PC, connected with Connect-MgGraph to the SOURCE tenant**

Check that the domain no longer appears in the source tenant before you try to add it to the target.

```
Get-MgDomain | Select-Object Id,IsVerified
```

✓ **You should see:** contoso.com is not in the list.

**If the domain uses federation.** If the domain is federated (for example with AD FS), convert it to managed authentication in the source first. Force delete does not work on federated domains.

## 6 Add and verify the domain in the target tenant

4 steps

1

### Add the domain

**Where: Microsoft 365 admin center (admin.microsoft.com) of the TARGET tenant > Show all > Settings > Domains > Add domain**

Type the domain and select **Next**, following add a domain to Microsoft 365. Expect the target to refuse the domain, or fail verification, until the source tenant has fully released it.

✓ **You should see:** The wizard asks how you want to verify the domain.

2

## Verify with the TXT record

**Where: Add domain wizard, then your DNS host's control panel > DNS records > Add record**

Choose the TXT option and add the `MS=ms` TXT value the wizard shows (replace any old MS= record from the source tenant). Return to the wizard and select **Verify**. Microsoft says verification can take up to 30 minutes after the record is added. When asked about DNS records, choose **I'll add the DNS records myself**.

```
nslookup -type=txt contoso.com 8.8.8.8
```

✓ **You should see:** The new MS=ms value is returned and the wizard moves on to the DNS records page.

3

## Publish mail records

**Where: Microsoft 365 admin center (admin.microsoft.com) of the TARGET tenant > Settings > Domains > your domain > DNS records tab, then your DNS host**

Copy the MX, Autodiscover and SPF values from the target tenant. Do not assume the MX value matches the one the source tenant used. Change MX with change MX records, and keep one SPF record (set up SPF).

```
nslookup -type=mx contoso.com 8.8.8.8
nslookup -type=cname autodiscover.contoso.com 8.8.8.8
```

✓ **You should see:** MX returns the target tenant's mail.protection.outlook.com value and Autodiscover returns autodiscover.outlook.com.

4

### Assign addresses in the target

**Where: PowerShell on your admin PC, connected with Connect-MgGraph and PowerShell on your admin PC, connected with Connect-ExchangeOnline, both to the TARGET tenant**

Set the custom domain as the UPN and primary SMTP address on target users, shared mailboxes and groups. Set it as the default domain in **Settings** > **Domains** > select it > **Set as default** if you want new users to get it.

```
Update-MgUser -UserId user@fabrikam.onmicrosoft.com -UserPrincipalName user@contoso.com
Set-Mailbox -Identity user@fabrikam.onmicrosoft.com -WindowsEmailAddress user@contoso.com
```

✓ **You should see:** Users sign in as user@contoso.com and Get-Mailbox shows PrimarySmtpAddress user@contoso.com.

## 7 Re-create DKIM and check DMARC

2 steps

1

### Create DKIM keys in the target

**Where: PowerShell on your admin PC, connected with Connect-ExchangeOnline to the TARGET tenant, or Microsoft Defender portal (security.microsoft.com) > Email & collaboration > Policies & rules > Threat policies > Email authentication settings > DKIM**

DKIM keys belong to the tenant, so the source CNAMEs will not work. Create the config disabled, read the two CNAME values, publish them at your DNS host as CNAME records named `selector1._domainkey` and `selector2._domainkey`, then enable signing. See set up DKIM.

```
New-DkimSigningConfig -DomainName contoso.com -Enabled $false
Get-DkimSigningConfig -Identity contoso.com | Format-List Selector1CNAME,Selector2CNAME
Set-DkimSigningConfig -Identity contoso.com -Enabled $true
```

✓ **You should see:** Get-DkimSigningConfig shows Enabled True and Status Valid, and the Defender portal shows Signing DKIM signatures for this domain.

2

### Keep DMARC unchanged

**Where: Your DNS host (TXT record at _dmarc.contoso.com)**

Your DMARC record lives at `_dmarc.contoso.com` and does not depend on the tenant. If it is set to quarantine or reject, check SPF passes for the target before mail flows, because DKIM will not sign until the new CNAMEs are live.

```
nslookup -type=txt _dmarc.contoso.com
```

✓ **You should see:** One v=DMARC1 record is returned with the policy you expect.

## 8 Test mail flow and clean up

4 steps

1

### Send test messages both ways

**Where: An external mailbox (for example Gmail or Outlook.com) and Outlook on the web in the target tenant**

Send from an external mailbox to several target users, shared mailboxes and groups, and send out from the target. In Gmail open the message, select **More** next to Reply and choose **Show original** to check headers for SPF and DKIM pass.

✓ **You should see:** Messages arrive both ways and the Authentication-Results header shows spf=pass and dkim=pass.

2

## Run a final content sync

**Where: Your mailbox migration tool or migration batch in the target tenant**

Run the final pass of your mailbox migration so anything that arrived in the source before the cutover is copied across. For Microsoft's native method see the cross-tenant mailbox migration guide.

✓ **You should see:** The tool reports the final pass complete with no failed users.

3

## Reconnect clients

**Where: Each user's PC (Outlook and Teams), phone and any shared devices**

Users sign in with their usual address but to a new tenant, so Outlook profiles, mobile accounts and Teams sign-ins need to be set up again. Give users the steps in reset an Outlook profile.

✓ **You should see:** Users open the target mailbox in Outlook, and Teams shows the target organisation name.

4

## Tidy up the source

**Where: Microsoft 365 admin center of the SOURCE tenant > Billing > Licenses**

Remove the source licences and tenant only after you have confirmed nothing still depends on them, and after any retention or legal hold requirements are met.

✓ **You should see:** Source licences are unassigned on the agreed date, with written sign-off from your compliance owner.

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 –

### Planned cutover window: remove, then add

MEDIUM EFFORT

**Best for:** Most tenant moves, where a short gap in inbound mail is acceptable

+ The method Microsoft documents: clear the domain from source objects, remove it, verify it in the target
+ No extra services to buy or configure
– Mail to the domain cannot be delivered while it is in neither tenant
– Removal can take from minutes to about a day, depending on how many objects reference it

Read more →

### Cutover with a mail filtering or queuing service in front

HIGH EFFORT

**Best for:** Organisations that cannot accept senders seeing temporary failures during the window

+ Inbound mail is held and delivered once the target is ready
+ Takes pressure off the cutover timetable
– Another service to set up and test before the window, with MX changes on both sides of the cutover
– Vendor licence; check current pricing

### Adopt a different domain in the target

MEDIUM EFFORT

**Best for:** Rebrands, or divestitures where the old domain stays with the source organisation

+ No domain removal, so no gap in mail flow
+ Source and target can run side by side for as long as needed
– Users change email addresses and sign-in names
– Contacts, partners and systems must be told the new addresses

Read more →

**OUR ADVICE**

Most moves use the planned cutover window: clear the domain from every source object in advance so the removal is quick, and keep force delete as a fallback only. Add a queuing service if even a short gap in inbound mail is not acceptable. If the organisation is changing its name anyway, moving to a new domain avoids the gap altogether.

### Script the whole cutover and rehearse it

SAVES TIME –

Removal can take five minutes or up to a day depending on how many objects reference the domain. Every minute spent finding a forgotten alias is a minute where inbound mail has nowhere to go.

**WHAT TO DO**

Write the renaming commands from Step 3 as one script that reads your inventory CSV, and test it on a spare domain (or a subdomain) in the source tenant first. Run the Step 2 inventory again a day before the window so the script covers objects created since.

**TOOLS THAT CAN GET AROUND THIS**

A domain move tool does the renaming you would otherwise script: it removes the domain from each source object and adds it to the matched target object at cutover. You still change MX records when it prompts you.

**Quest On Demand Migration**

Domain Move works from your user and group matching, swaps addresses automatically and keeps inbound mail flowing through a relay service while proxy addresses move.

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

Microsoft Learn: Remove a domain

## Move a subdomain instead if that is all you need

REDUCES RISK

Microsoft lets a subdomain such as europe.contoso.com be verified in a different tenant from contoso.com. If only one business unit is moving, you can avoid removing the parent domain and the mail gap that comes with it.

**WHAT TO DO**

Check whether the moving users can live on a subdomain. If so, add and verify only the subdomain in the target and leave contoso.com where it is.

Microsoft Learn: Manage custom domain names in Microsoft Entra ID

## Avoid ForceDelete in a live migration

REDUCES RISK

ForceDelete renames remaining users, groups and apps to the onmicrosoft.com domain and can disable the renamed accounts. It refuses domains bought through Microsoft 365, federated domains, more than 1,000 references and multitenant apps.

**WHAT TO DO**

Plan to clear every reference yourself. Keep ForceDelete for a last resort, and if you use it through Graph set `disableUserAccounts` to false so source users can still sign in for the final sync.

Microsoft Graph: domain forceDelete

## Check whether users are synchronised from Active Directory

SAVES TIME

Cloud attributes of synchronised users are read-only. You cannot rename them in the source tenant, and Entra Connect will put the old domain back on the next sync if you try.

**WHAT TO DO**

Run `Get-MgUser -All -Property UserPrincipalName,OnPremisesSyncEnabled` and count synced users. Either change UPN and proxyAddresses in Active Directory ahead of the window, or turn off sync as a planned step of the tenant move.

### Do not let DMARC reject your own mail during the gap

REDUCES RISK

DKIM keys belong to the tenant. Until the target tenant's selector CNAMEs are published and signing is on, mail from the target is not DKIM-signed for your domain. With DMARC at p=reject and SPF not yet updated, your outbound mail can be rejected.

**WHAT TO DO**

Update SPF and pre-check the DMARC record before the window. If DMARC is at reject, consider moving to p=quarantine or p=none for the cutover weekend, then restore it once DKIM signs from the target.

Microsoft Learn: Set up DKIM for your custom domain

### Remember what the domain does not carry with it

USER IMPACT

SharePoint and OneDrive URLs use the tenant's onmicrosoft.com name, not your custom domain, so they change in a tenant move. Guest accounts, sharing links and Teams federation in other organisations still point at the source tenant.

**WHAT TO DO**

Tell partners who host your users as guests that the users will need fresh invitations. Plan link updates for files you share externally, and list them in your user communication pack.

### Budget for both tenants being licensed at once

COST LEVER

Users need a working mailbox in the target before the domain moves and a licensed source mailbox until the final sync and any retention period ends. The overlap is a cost driver.

**WHAT TO DO**

Agree with your licensing partner how long you need source licences and when to remove them, and put the removal date in the runsheet. Check retention or legal hold requirements before deleting source mailboxes.

### Native tools cannot hold mail while the domain is in neither tenant

REDUCES RISK

A domain can be verified in only one tenant at a time, so between removal from the source and verification in the target, Microsoft 365 accepts mail for it nowhere. Sending servers retry for a while, but a long removal or a slow DNS change turns delays into bounces.

**WHAT TO DO**

Decide in advance how long a gap is acceptable. If the answer is minutes, not hours, point MX at a queuing or relay service before the window and back to the target once the domain verifies.

**TOOLS THAT CAN GET AROUND THIS**

A short-term mail routing service accepts and queues inbound mail for the domain while it is detached, then delivers it to the target mailboxes once the domain is attached, so senders see no bounces.

**Cloudiway Mail Routing**

MX points to Cloudiway before you detach the domain, mail is queued during the transfer and MX returns to Microsoft 365 afterwards. Meant for windows of about 48 hours, and Cloudiway notes DMARC needs adjusting while it routes mail.

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

Microsoft Learn: Manage custom domain names in Microsoft Entra ID

FINISH SAFELY

## How do you check it worked, or roll back?

### Full validation checklist

8 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 |
| --- | --- | --- |
| **The domain is verified in the target and gone from the source** | Run `Get-MgDomain \| Select-Object Id,IsVerified` connected to each tenant with Connect-MgGraph. In the target Microsoft 365 admin center, Settings > Domains should show the domain as Healthy. | contoso.com is absent from the source and shows IsVerified True in the target, with no DNS record warnings. |
| **MX, Autodiscover and SPF point at the target** | Run `nslookup -type=mx contoso.com 8.8.8.8`, `nslookup -type=cname autodiscover.contoso.com 8.8.8.8` and `nslookup -type=txt contoso.com 8.8.8.8` and compare with the values on the target tenant's DNS records tab. | MX returns the target tenant's mail.protection.outlook.com value, Autodiscover returns autodiscover.outlook.com, and there is one SPF record. |
| **Every user, shared mailbox and group has its address back** | In the target run `Get-Recipient -ResultSize Unlimited \| Where-Object { $_.EmailAddresses -like "*@contoso.com" } \| Measure-Object` and compare with the count in `C:\migration\contoso-recipients.csv` from the source inventory. | The target count matches the source inventory, and no recipient that used the domain is missing. |
| **Users sign in with their usual address** | In the target run `Get-MgUser -All -Property UserPrincipalName \| Where-Object { $_.UserPrincipalName -like "*@contoso.com" } \| Measure-Object`, then sign in as a test user at https://www.office.com. | The count matches the users you renamed in the source, and the test user lands in the target tenant. |
| **Mail flows both ways with SPF and DKIM passing** | Send from an external mailbox to several target users, a shared mailbox and a group, and reply. Open the message headers and check Authentication-Results. Confirm `Get-DkimSigningConfig -Identity contoso.com` shows Enabled True. | All messages arrive, headers show spf=pass and dkim=pass, and DMARC is not quarantining or rejecting your own mail. |

| Check | How to check | What good looks like |
|---|---|---|
| **Final content sync is complete** | Open your mailbox migration tool or the target migration batch and check the final pass status for every user. | The final pass is complete with no failed users, so mail that reached the source before the cutover is in the target. |
| **Outlook, mobile and Teams use the target tenant** | On sample PCs open Outlook and Teams, and on sample phones check the mail account. | Outlook opens the target mailbox, Teams shows the target organisation name and phones sync new mail. |
| **The source no longer receives mail for the domain** | In the source Exchange admin center > Mail flow > Message trace, search the last 24 hours for recipients on contoso.com. | No new messages to contoso.com addresses are delivered in the source after the MX change. |

## Rollback plan

If it goes wrong

**ROLL BACK IF**

- The source tenant will not release the domain because objects still reference it and you cannot clear them inside the window
- The target tenant cannot verify the domain within the agreed time after removal from the source
- Inbound mail is being rejected or lost after the MX change and the cause cannot be found quickly
- Users cannot sign in to the target with their usual address and the business cannot work on onmicrosoft.com addresses

**POINT OF NO RETURN**

The point of no return is removing the domain from the source tenant. Before that, rollback is only putting addresses and UPNs back. After it, the domain cannot be in both tenants, so going back means removing it from the target and verifying it again in the source, which repeats the mail gap. Messages rejected or bounced

during the gap are not recovered. If you used force delete, the renames it made to users, groups and apps are not reversed automatically.

1

## Before removal: restore source addresses

**Where: PowerShell on your admin PC, connected with Connect-MgGraph and Connect-ExchangeOnline to the SOURCE tenant**

Use the inventory CSVs to set UPNs back with `Update-MgUser -UserId user@contoso.onmicrosoft.com -UserPrincipalName user@contoso.com` and primary addresses back with `Set-Mailbox -Identity user@contoso.onmicrosoft.com -WindowsEmailAddress user@contoso.com`, and re-add group addresses. For synced users, change the UPN in Active Directory and run a sync.

✓ **You should see:** The source inventory commands list every object on contoso.com again and users sign in as before.

2

## After removal: clear the domain from the target

**Where: PowerShell on your admin PC, connected to the TARGET tenant**

Move target users, mailboxes and groups back to the target onmicrosoft.com domain using the same commands as the release step, then remove the domain in the target Microsoft 365 admin center > Settings > Domains > Remove domain, or with `Remove-MgDomain -DomainId contoso.com`.

✓ **You should see:** Get-MgDomain in the target no longer lists contoso.com.

3

## Verify the domain in the source again

**Where: Microsoft 365 admin center (admin.microsoft.com) of the SOURCE tenant > Settings > Domains > Add domain, and your DNS host**

Add contoso.com, publish the new MS=ms TXT value the wizard shows (replace the target's value), and select Verify. Then publish the source MX, Autodiscover and SPF values from the source DNS records tab.

✓ **You should see:** The domain shows as verified in the source and nslookup returns the source MX value.

4

## Put addresses and DKIM back in the source

**Where: Exchange Online PowerShell and Graph PowerShell connected to the SOURCE tenant**

Restore UPNs and primary addresses from the inventory CSVs as in the first step. Re-enable DKIM for the domain with `Get-DkimSigningConfig -Identity contoso.com` and `Set-DkimSigningConfig -Identity contoso.com -Enabled $true`, publishing new CNAMEs if the selectors changed.

✓ **You should see:** Users send and receive as user@contoso.com from the source and headers show dkim=pass.

5

## Reconnect clients and record the outcome

**Where: Each user's PC and phone, then your Rollback plan**

Users restart Outlook and Teams, or recreate profiles if they were already set up for the target. Record the cause, the length of the mail gap and any lost messages before you reschedule.

✓ **You should see:** Users work in the source tenant again and the Rollback plan has a dated entry.

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

## Common problems and fixes

6 errors

`Target tenant says the domain is already in use or cannot be verified`

**Cause:** The domain is still verified in the source tenant.

**Fix:** Finish removing the domain from the source, confirm it no longer appears there, then verify again in the target.

`Domain removal stuck or fails in the source tenant`

**Cause:** An object still references the domain, often an alias, a group or an app ID URI.

**Fix:** Re-run the Get-Recipient and Get-MgUser checks, check app registrations, then retry. Contact Microsoft support if removal still fails.

`Force delete returns an error about too many objects`

**Cause:** More than 1,000 objects reference the domain, or a multitenant app uses it.

**Fix:** Rename objects in batches with PowerShell until the count is below the limit, and update the app ID URI.

`Users cannot be renamed in the cloud`

**Cause:** They are synchronised from on-premises Active Directory, so the cloud copy is read-only for those attributes.

**Fix:** Change the UPN and proxyAddresses in Active Directory and let sync run, or stop sync as part of the move.

`Set-DkimSigningConfig fails after the move`

**Cause:** The new selector CNAMEs from the target tenant are not published or have not propagated.

**Fix:** Publish the exact Selector1CNAME and Selector2CNAME values from the target, wait, then run the command again.

`External senders get bounces during the window`

**Cause:** The domain is in neither tenant, or MX still points to the old values.

**Fix:** Keep the window short, publish the target MX as soon as the domain verifies, and ask senders to resend anything that bounced.

Search the full error library →

FAQ

# Frequently asked questions

### Can a domain be in two Microsoft 365 tenants at once?

No. Microsoft does not allow a domain to be verified in more than one Entra tenant. Subdomains can be verified in a different tenant from their parent.

### How long does it take to remove a domain from Microsoft 365?

Microsoft says as little as five minutes if few objects use it, or several hours up to a day if many do.

### Will I lose email during the move?

There is a window where the domain is in neither tenant. Most sending servers retry temporary failures, but some mail may bounce, so plan a short, quiet window and tell people in advance.

### Do I need to change my MX record?

Yes. Use the MX value the target tenant shows for the domain, because it can differ from the one the source used.

### What happens to the old onmicrosoft.com addresses?

Users in the source revert to the onmicrosoft.com domain. That domain cannot be removed and stays with the source tenant.

SOURCES

## Official sources

### 7 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: Remove a domain
- Microsoft Learn: Manage custom domain names in Microsoft Entra ID
- Microsoft Graph: domain forceDelete
- Microsoft Learn: Add a domain to Microsoft 365
- Microsoft Learn: Information for DNS records
- Microsoft Learn: Set up DKIM for your custom domain
- Microsoft Learn: Set up DMARC