

LoomFabric and Microsoft Entra ID -- setup scenarios

Setup scenarios, portal steps, and plan coverage

Last updated 30 August 2026 | loomfabric.ai

Who this is for: consultancies, Microsoft Fabric partners, and internal data teams who want to know how LoomFabric fits their Microsoft Entra ID (formerly Azure AD) setup before they buy -- and exactly which buttons to press in the Azure portal afterwards.

How to use it: run the 30-second test in section 2, find your letter in section 4, follow that scenario's portal steps. You should not need any other document.

1. The 60-second answer

There are two separate Entra questions hiding inside "does this support multiple tenants", and they have different answers.

	The question	The answer
Your clients	Can I serve clients whose Fabric workspaces live in <i>their own</i> Entra tenants?	Yes. On every plan. This is the normal way partners use LoomFabric.
Your team	Can my own staff sign into LoomFabric from <i>two different</i> Entra tenants?	Not today. Pick one tenant as your account. Sections B and E show how, at no cost.

Almost everyone asking is asking the first question. If that is you, the answer is yes, and section 4-F is your setup guide.

Two facts that surprise people:

- **Your team's sign-in tenant and your clients' tenants are unrelated.** LoomFabric is a control surface your consultants drive from your own tenant. It reaches into each client's Fabric workspace using credentials that client issues. The two never have to match.
- **Your clients' report readers never sign into LoomFabric at all.** They open Power BI in their own tenant, under the row-level security roles LoomFabric generates for them.

2. Entra basics that decide everything

Most confusion here comes from one misconception, so it is worth being precise.

A tenant is a container. A domain is a label you attach to it.

- A **tenant** (also called a directory) is the container that holds your users, groups and app registrations. It has a permanent GUID called the **Tenant ID**.
- Every tenant is born with a built-in domain: `something.onmicrosoft.com`.
- A **custom domain** such as `yourfirm.com` is a DNS name you *attach* to a tenant, by proving you control the DNS zone with a TXT record.

A domain does not have, own, or lack a tenant. The relationship runs the other way: a tenant can hold many domains.

One domain lives in exactly one tenant, worldwide

Entra enforces global uniqueness. `yourfirm.com` can be verified in one tenant at a time across all of Microsoft. If it is already verified somewhere else, adding it fails with "the domain is already in use in another directory" until it is removed there first.

So when you see two domains in one tenant, it is because an administrator **chose** to attach both DNS names to the same directory -- not because those domains had nowhere else to go. Two tenants each holding one domain is simply the other choice, made at some point in the past, usually by whoever set up email.

What LoomFabric keys your account on

Your LoomFabric account is identified by your **Tenant ID**, taken from your sign-in. Not your email domain. This single fact explains every verdict in section 4:

- Two users in the **same tenant** are the same account, no matter which email domain each one uses.
- Two users in **different tenants** are two accounts, even if the same person owns both and even if the email addresses look related.

The 30-second test

Do this before anything else. It tells you which scenario you are in.

1. Go to **<https://entra.microsoft.com>** and sign in as an administrator.
2. **Overview** -- copy the **Tenant ID**. This is your account identity.
3. **Identity -> Settings -> Domain names** -- read the list.

Now:

- Every email domain your team uses appears in that one list -> **Scenario A or B. Nothing

to do.**

- You have to switch directories (top-right account menu -> Switch directory) to see one of your domains -> **Scenario C**. Read section 4-C.

Microsoft renames portal blades from time to time. If a path below does not match what you see, the item is usually one level up or renamed slightly; the names in bold are stable enough to search for in the portal search bar.

3. Operators and clients

Two populations, and keeping them separate makes everything else obvious.

	Operators	Clients
Who they are	The people who use LoomFabric -- your consultants and engineers	The end customer's Fabric estate: workspace, lakehouses, semantic models
Where they live	Your Entra tenant	The client's own Entra tenant (or yours, if you host -- see F1 vs F2)
What they are in the product	A sign-in	A client workspace , which is what your plan meters
Do they cost anything?	No. Every plan includes unlimited Entra users	Yes. This is the metered unit
How they authenticate	Interactive Entra sign-in	A service principal the client issues
Do they sign into LoomFabric?	Yes	Never

Operators are billed per account, not per head. Clients are the thing you buy capacity for.

4. Scenario catalog

Each scenario follows the same shape: when this is you, the verdict, a picture, the portal steps, what to write down, and what the error looks like if a step is missed.

Scenario A -- one tenant, one domain, many users

When this is you: everyone on your team has an @yourfirm.com address and there is one Entra directory.

Verdict: works on every plan. Nothing to configure.

Tenant: yourfirm.com	Tenant ID: 1111-1111
carlos@yourfirm.com	--+
maria@yourfirm.com	--+--> ONE LoomFabric account
dev@yourfirm.com	--+ one plan, one bill, one shared portfolio

Portal steps -- adding a colleague

1. **https://entra.microsoft.com -> Identity -> Users -> All users -> New user ->

Create new user**.

2. Fill in **User principal name** and **Display name**. Leave the domain dropdown on your domain.

3. **Review + create**.

4. Have them sign into LoomFabric. They immediately see the same clients you do.

What to record: nothing.

Every plan includes unlimited Entra users. Adding people never changes your bill.

Scenario B -- one tenant, two or more verified domains

When this is you: your team uses @domaina.com and @domainb.com, and both appear in the same **Domain names** list. Common causes: a rebrand where the old address still works, two trading brands under one IT department, an acquisition whose mailboxes were migrated into your directory, or per-country domains.

Verdict: works on every plan. Both addresses are the same account. Nothing to configure, nothing extra to pay.

Tenant: yourfirm.onmicrosoft.com	Tenant ID: 1111-1111
verified domains: domaina.com, domainb.com	
carlos@domaina.com	--+
carlos@domainb.com	--+--> ONE LoomFabric account (same Tenant ID)

Why: your account is keyed on the Tenant ID, and both users are issued tokens by the same tenant. The email suffix is not part of the identity.

Which businesses are actually in this shape

Situation	Example	Why it is one tenant
Rebrand	contoso.com became contosodata.com, and the old address still receives mail	IT never built a second directory -- they attached the new domain to the existing one
Two trading brands, one IT department	A consulting arm on domaina.com and a BI practice on domainb.com	One payroll, one directory, two go-to-market brands
An acquisition that was consolidated	An acquired BI shop's mailboxes were migrated in and their domain attached	The acquired directory was decommissioned. This is what turns an acquisition into Scenario B rather than Scenario C
Per-country domains	domaina.com, domaina.co.uk, domaina.de	One directory, country-specific email identity
Vanity plus the built-in domain	domaina.com alongside domaina.onmicrosoft.com	Every tenant has this from the day it is created, so most tenants already hold two domains
White-label or reseller front	Delivery under domaina.com, a productized offer under domainb.com	Same staff, same directory, different shop front

For a Fabric partner the common ones are the first three. If none of these describes you and your second domain sits in its own directory, you are in Scenario C.

Portal steps -- verifying a second domain (only if it is not already listed)

1. **Identity -> Settings -> Domain names -> Add custom domain.**
2. Type the domain, for example domainb.com, and click **Add domain**.
3. The portal shows a **TXT record** to publish, of the form
MS=ms#####. Note the host (usually @ or the bare domain) and the value.
4. At your DNS provider, add that TXT record to the zone. TTL 3600 is fine.
5. Wait for DNS to propagate -- usually minutes, occasionally up to an hour.
6. Back in the portal, open the domain and click **Verify**.
7. Optional: **Make primary** if you want new users to default to this suffix.

Portal steps -- giving a user the second suffix

- New user: **Identity -> Users -> All users -> New user -> Create new user**, then pick domainb.com from the domain dropdown beside **User principal name**.
- Existing user: open the user -> **Edit properties** -> change the domain part of the **User principal name**. They sign in with the new address afterwards.

What to record: nothing. Your Tenant ID has not changed, so your LoomFabric account has not changed.

If it goes wrong

Symptom	Cause and fix
"The domain is already in use in another directory"	The domain is verified in a different tenant. Remove it there first, or use Scenario E instead. This is Entra's global uniqueness rule.
Verify keeps failing	The TXT record is not visible yet, or it was added to the wrong zone. Check with <code>nslookup -type=TXT domainb.com</code> .

Scenario C -- two separate Entra tenants used for sign-in

When this is you: you had to switch directories in the portal to see your second domain. Two directories, two Tenant IDs. Typical cause: an acquisition that was never merged, a joint venture, or two businesses that grew up with separate IT.

Verdict: not offered on any published plan. Each tenant would be a separate LoomFabric account, with its own plan, its own client capacity and its own storage -- not one shared portfolio.

Tenant A: 1111-1111
carlos@domaina.com

|
v

LoomFabric account A
your plan, your clients

Tenant B: 2222-2222
carlos@domainb.com

|
v

LoomFabric account B
separate, starts empty

Signing in from the second tenant does not error -- it simply creates a second, unrelated account that starts on a fresh trial. That is usually not what anyone wants.

What to do instead. Treat this as a consolidation question, not a purchase question:

- **Preferred:** pick one tenant as your LoomFabric account, then use **Scenario E** to give the affected people an account in that tenant. Free, immediate, no IT project.
- **Cleanest long term:** if you intend to merge the directories anyway, verify the second domain in the surviving tenant -- that turns this into **Scenario B**. Note this requires removing the domain from the other tenant first, which affects email. Treat it as an IT migration, not a LoomFabric task.
- **If neither is acceptable,** contact us and describe the constraint. Do not assume a larger plan changes this answer -- it does not.

Important: this limitation is about **who signs in**. It has nothing to do with your clients' tenants. You can serve clients in dozens of different Entra tenants from a single sign-in tenant -- that is Scenario F, and it works on every plan.

Scenario D -- using a B2B guest invite to bridge two tenants

When this is you: you are in Scenario C and thinking "I will just invite carlos@domainb.com as a guest into tenant A."

Verdict: does not achieve what you want for LoomFabric sign-in.

```
carlos@domainb.com  invited as a guest of Tenant A
-> sign-in is routed to his HOME tenant (B) to authenticate
-> the token says Tenant ID 2222, not 1111
-> LoomFabric sees account B, exactly as in Scenario C
```

Why: when he types his address at the sign-in prompt, Microsoft routes him to the tenant that owns that domain -- his home tenant -- and that tenant issues the token. Guest status in tenant A grants him access to *resources* in A, but it does not change which tenant authenticates him.

What to do instead: Scenario E. A **member** account in tenant A is issued a token by tenant A, which is what makes it the same LoomFabric account.

Worth knowing: guest access *is* useful elsewhere. In Scenario F, a guest account in your client's tenant is one way for a consultant to reach that client's Fabric workspace by hand. It just cannot merge two LoomFabric sign-in accounts.

Scenario E -- an extra member account in your chosen tenant

When this is you: you are in Scenario C and want the cheapest fix today.

Verdict: works on every plan. Free, unlimited, takes two minutes per person.

```
Tenant A: 1111-1111
carlos@domaina.com      <- existing
carlos.b@domaina.com    <- new member, used for domainb.com engagements
...both are the same LoomFabric account
```

Portal steps

1. In the tenant you have chosen as your LoomFabric account:

https://entra.microsoft.com -> Identity -> Users -> All users -> New user -> Create new user.

2. Set **User principal name**, for example carlos.b, with your primary domain selected.
3. Set **Display name** so it is obvious which brand or engagement it is for.
4. **Review + create**, then share the credentials with the person.
5. They sign into LoomFabric with the new address and see the shared portfolio.

What to record: which brand or client each extra account is used for, so it is obvious later. This is purely for your own bookkeeping.

A practical note: one person per sign-in address. If two people use the same address at the same time, the second sign-in ends the first one's session. Give everyone their own account -- they are free on every plan.

Scenario F -- your clients in their own Entra tenants

When this is you: you are a partner or consultancy. Each client has their own Microsoft tenant, their own Fabric capacity, and their own data. You want to build and run their medallion pipeline without asking them to hand over anything but scoped access.

Verdict: works on every plan. This is the primary way LoomFabric is used. The only plan-dependent question is *how many* clients you can have running at once.



The bridge across the tenant boundary is one **app registration (service principal)** per client, created in that client's tenant by that client's administrator. You never need an account in their directory, and they never need one in yours.

Steps the CLIENT's administrator performs, in the CLIENT's tenant

Part 1 -- register the application

1. ****https://entra.microsoft.com -> Identity -> Applications -> App registrations -> New registration**.**
2. **Name:** something recognisable, for example LoomFabric Data Platform.
3. **Supported account types:** *Accounts in this organizational directory only (single tenant)*.
4. **Redirect URI:** leave empty.
5. Click **Register**.
6. On the app's **Overview** page, copy and keep:
 - **Directory (tenant) ID**
 - **Application (client) ID**

7. **Certificates & secrets -> Client secrets -> New client secret.** Add a description

and an expiry, click **Add**, then copy the **Value** immediately. It is shown only once. Note the expiry date in a calendar -- an expired secret stops the pipeline.

Part 2 -- give the application access to the Fabric workspace

8. **<https://app.fabric.microsoft.com>** -> open the client's workspace ->

Manage access -> Add people or groups.

9. Type the app registration's name, select it, and assign **Contributor** (or **Admin**).

10. Click **Add**.

Part 3 -- allow service principals to call Fabric APIs

11. A **Fabric administrator** must enable the tenant setting that permits service principals to use the Fabric APIs: **Fabric portal -> Settings (gear) -> Admin portal -> Tenant settings -> Developer settings**. Enable it for the whole organisation, or for a security group containing this app registration.

Confirm the exact wording of this setting in your own tenant before relying on it -- the Fabric admin portal labels change between releases. Without it, the app registration authenticates but Fabric refuses the API call.

Part 4 -- Key Vault for the source database credentials

12. Create or choose an Azure Key Vault in the client's subscription.

13. Add the secrets for the source system, and store this app registration's secret as `gold-app-reg-client-secret`.

14. Grant the **Key Vault Secrets User** role to the Fabric workspace **Managed Identity** (or to the identity that will run the notebooks).

Steps YOU perform, in LoomFabric

15. Create the client workspace and select it.

16. Open **Connection Settings -> Fabric Workspace Config** and fill in:

- `WORKSPACE_GUID` -- the client's Fabric workspace ID, from the workspace URL
- `GOLD_APP_REG_TENANT_ID` -- the Directory (tenant) ID from step 6
- `GOLD_APP_REG_CLIENT_ID` -- the Application (client) ID from step 6
- `GOLD_APP_REG_CLIENT_SECRET` -- the secret Value from step 7

17. Fill in the Key Vault name and secret names for the source connector.

18. Proceed with discovery and the rest of onboarding as normal.

What to record, per client

Value	Where it came from
Directory (tenant) ID	App registration Overview
Application (client) ID	App registration Overview
Client secret value + expiry date	Certificates & secrets, at creation
Fabric workspace GUID	The workspace URL
Key Vault name and secret names	The client's Azure subscription

Keep the secret in your own password manager as well as in the client's Key Vault. Diary the expiry.

The same app registration is reused for the Streamlit apps LoomFabric can generate for that client, so this is one registration per client tenant -- not one per feature.

If it goes wrong

Symptom	Cause and fix
AADSTS50020 -- user account from identity provider does not exist in tenant	The three GOLD_APP_REG_* values are not all filled in, so LoomFabric is trying to sign <i>you</i> into the client's tenant, where you have no account. Complete step 16.
401 or 403 on the workspace, though sign-in succeeded	Either the three values are empty (so your own tenant authenticated you and it has no such workspace), or the app registration was never added to the workspace. Check step 16, then steps 8-10.
AADSTS7000215 -- invalid client secret	The secret was mistyped, or the secret's ID was copied instead of its Value , or it has expired. Create a new secret and update step 16.
Fabric API calls refused for the service principal	The tenant setting in step 11 is not enabled, or the app is not in the security group it was scoped to.
Pipeline cannot read source credentials	The Key Vault role assignment in step 14 is missing, or the secret names do not match what you entered in step 17.

F1 or F2 -- who hosts the Fabric workspace?

Both work on every plan, and you can mix them across your clients.

	F1 -- client-owned	F2 -- partner-hosted
Fabric workspace lives in	The client's tenant	Your tenant, one workspace per client
Who owns the data	The client	You, on their behalf
Who pays for Fabric capacity	The client	You

	F1 -- client-owned	F2 -- partner-hosted
App registrations needed	One per client	One, reused
Client admin involvement	Steps 1-14 above	Almost none
Best for	Regulated clients, data residency requirements, long engagements	Proofs of concept, small engagements, clients with no Fabric capacity yet

Under F2 you are holding client data in your own tenant. Make sure your contract says so.

5. Scenario coverage by plan

Scenario	Free	Solo	Practice	Agency	Firm	Custom
A -- one tenant, one domain	Yes	Yes	Yes	Yes	Yes	Yes
B -- one tenant, several verified domains	Yes	Yes	Yes	Yes	Yes	Yes
C -- two tenants for sign-in	No	No	No	No	No	Talk to us
D -- guest invite to bridge tenants	Not possible	Not possible	Not possible	Not possible	Not possible	Not possible
E -- extra member account	Yes	Yes	Yes	Yes	Yes	Yes
F -- clients in their own tenants	Yes	Yes	Yes	Yes	Yes	Yes
Entra users included	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Client workspaces at once	1	1	4	10	30	Custom

The table is deliberately almost uniform. Every plan grants unlimited Entra users and the same Entra capabilities, so the only thing that changes as you move up is **how many client workspaces you can run at once** -- which is what caps how many client tenants you can serve simultaneously.

Scenario D is marked "not possible" rather than "not included": it is a property of how Microsoft routes sign-ins, not something a plan controls.

Free plan note: the free trial is one per Entra tenant. If your tenant has already used its trial, a new sign-in from the same tenant will not start a second one.

6. Required before you serve a client in another tenant

The **per-client service principal is mandatory, not optional**. If all three of `GOLD_APP_REG_TENANT_ID`, `GOLD_APP_REG_CLIENT_ID` and `GOLD_APP_REG_CLIENT_SECRET` are not filled in, LoomFabric falls back to asking *you* to sign in interactively -- and you are not a user in your client's directory.

What you have filled in	What happens
All three values	Silent service-principal authentication. Nobody needs an account in anybody else's tenant. This is the correct setup.
Tenant ID only; client ID or secret missing	The sign-in prompt is aimed at the client's tenant. You have no account there, so it fails immediately with AADSTS50020.
None of them	Sign-in succeeds -- against your own tenant -- and then the Fabric call fails with 401 or 403, because the workspace is in a different tenant. It looks like a permissions problem but it is a missing service principal.

The one case where the interactive fallback does work: if you hold a guest account in the client's tenant *and* a role on their Fabric workspace, the interactive sign-in succeeds. Some consultancies do have this. It is still not a good standing arrangement, because it is interactive every time, specific to one client tenant, subject to a sign-in timeout, and unusable for unattended or scheduled runs.

Use the service principal.

7. FAQ

Do my client's report readers need LoomFabric logins? No. They open Power BI in their own tenant. LoomFabric generates the row-level security roles; their administrator assigns their accounts to those roles. They never see LoomFabric.

One app registration for all my clients, or one per client? One per client tenant, created by that client. An app registration only exists inside one directory, so it cannot span clients. Under F2 (partner-hosted), where all workspaces are in your tenant, one registration can serve all of them.

What if a client refuses to create a service principal? Then the only route is a guest account for you in their tenant plus a role on their workspace, and interactive sign-in each session. Workable for a short engagement, poor for anything scheduled. It is usually easier to walk their administrator through section 4-F, which grants access to exactly one workspace and nothing else.

Does my client's data pass through my tenant? Under F1, no -- it stays in their tenant. Under F2, yes, because the workspace is yours. Choose deliberately and put it in the contract.

Can I mix F1 and F2 across clients? Yes. The plan counts client workspaces, not where they live.

Can my team sign in from two different Entra tenants? Not today. Consolidate onto one tenant using section 4-B or 4-E, or contact us to discuss the constraint.

We are mid-rebrand and both domains are live. Is that a problem? No -- that is Scenario B, and it needs no configuration as long as both domains are verified in the same tenant.

Does adding people to my team cost more? No. Every plan includes unlimited Entra users. You are billed for client workspaces.

What happens when a client engagement ends? Delete the client workspace to free capacity, and ask the client to remove the app registration or let its secret lapse. Freed capacity becomes available for a new client.

8. Glossary

Term	Meaning
Tenant (directory)	The container holding users, groups and app registrations for one organisation
Tenant ID	The tenant's permanent GUID. This is what identifies your LoomFabric account
Custom domain	A DNS name attached to a tenant after a TXT-record proof. Unique to one tenant worldwide
UPN (user principal name)	The sign-in address, for example carlos@domaina.com
Member	A user who belongs to the tenant and is authenticated by it
Guest (B2B)	A user from another tenant granted access to resources, but still authenticated by their home tenant
App registration / service principal	A non-human identity in a tenant, used by software to authenticate without a person present
Client workspace	One client's configuration and pipeline in LoomFabric. The unit your plan meters
Workspace GUID	The Microsoft Fabric workspace identifier, visible in the workspace URL
Operator	A person on your team who uses LoomFabric

Questions about a setup not covered here: contact us with your Tenant ID count and how many client tenants you expect to serve, and we will tell you which scenario applies.