eSolia

Teams Shared Channels with B2B Direct Connect: Setup Guide

March 17, 2026

eSolia

Contents

> eSolia INTERNAL — Not for distribution outside eSolia

Version: 2.1
Date: 2026-03-16
Author: Rick Cogley
Audience: eSolia consultants delivering M365 services

Overview

This guide covers how to set up **Teams shared channels** for clients who need to collaborate with external firms — auditors, legal counsel, partner companies — in a secure, auditable way.

Shared channels are the preferred approach over traditional guest access for inter-firm collaboration. The core difference: guest access creates an account inside the client's tenant (like handing out a building key), while shared channels use **B2B Direct Connect** to let external users participate from their own tenant (like opening a secured window between two buildings). External users never see the broader Teams environment, directory, or other channels.

For FSA-regulated and ISO 27001 clients, this distinction is the whole ballgame — data boundary control and auditability depend on it.

When to use shared channels vs. guest access

Use **shared channels** when:

- The client collaborates regularly with a known external organization that also uses M365/Entra ID.
- External participants should only see a specific channel, not the full team.
- You want to avoid guest account sprawl and lifecycle management overhead.
- The client needs audit trails for all cross-tenant activity.
- Compliance policies (DLP, retention, sensitivity labels) must apply from the host tenant.

Use **guest access** when:

- The external party does not have an Entra ID tenant (e.g., personal Gmail users, small vendors without M365).
- The external party needs access to multiple channels or the full team.
- The collaboration is short-term or one-off, and a guest account with expiration is simpler.

Use **external access (federation)** when:

- Only chat and calling are needed — no file sharing or channel participation.

What about personal M365, Outlook.com, and MSA users?

B2B Direct Connect requires an organizational Entra ID tenant on both sides. Personal M365 subscriptions (Family, Personal), Outlook.com, Hotmail, and Live.com accounts all authenticate through a **Microsoft Account (MSA)**, not Entra ID. No tenant means no cross-tenant access settings, and no shared

channels. Think of it as trying to set up a secure office-to-office intercom when the other party works from a park bench — the infrastructure doesn't exist on their end.

These users can still collaborate in Teams through regular guest access. They get invited to a team, a guest account is created in your Entra directory, and they participate in standard channels like any other guest. What they can't do is join a shared channel or a private channel.

The full picture:

External user type	Standard channels (guest)	Private channels	Shared channels
Organizational M365 (has Entra ID tenant)	Yes, as guest	No	Yes, via B2B Direct Connect
Personal M365 / MSA / Outlook.com	Yes, as guest	No	No
No Microsoft account at all	No	No	No

This creates a two-track approach to external collaboration:

- **Partner has a business/enterprise M365 tenant** → Shared channels via B2B Direct Connect. No guest sprawl, better audit trail, channel-level isolation.
- **Partner has only a personal account** → Traditional guest access. Guest account gets created, needs lifecycle management, and the guest can see all standard channels in the team (not just one).

Practical workaround for personal account guests: Create a dedicated team for that specific external collaboration — "EXT — Project Alpha — Tanaka-san" — so the guest only sees channels relevant to that engagement. It's not as surgical as a shared channel, but it keeps things contained and makes cleanup straightforward when the engagement ends (delete the team, the guest account gets flagged in your next access review).

Security note for FSA-regulated clients: A guest backed by a personal Microsoft account has no organizational security policies on their side — no managed device, no organizational MFA, no admin who can revoke their credentials if their laptop gets stolen. Your conditional access policies become the only security layer. For sensitive engagements, consider whether the collaboration is better handled through encrypted email (Purview Message Encryption) rather than persistent Teams/SharePoint access.

The gentle upsell: For freelance auditors, consultants, or small-firm partners who work with multiple organizations, M365 Business Basic starts at around ¥750/month and gives them a proper Entra ID tenant. This makes them compatible with shared channels at every firm they work with — and stops them from being a second-class citizen in everyone's directory. It's a conversation worth having.

How shared channels work

Shared channels use **Entra ID B2B Direct Connect**, which is a mutual trust relationship between two M365 tenants. Both sides must configure cross-tenant access settings before sharing works.

The host tenant — where the channel is created — owns all channel data. The host's compliance policies, sensitivity labels, retention rules, and DLP apply. The external organization's policies don't govern the data. This is the single most important point to communicate to compliance-conscious clients.

External users authenticate against their own home tenant. No guest account is created in the host tenant, which eliminates guest sprawl entirely. Each shared channel also creates its own dedicated SharePoint site, separate from the parent team's site — factor this into site inventory and backup planning.

Two things to plan around up front:

- Channel type is permanent. You can't convert a shared channel to/from standard or private after creation.
- B2B Direct Connect is blocked for all organizations by default. You must explicitly allow each partner tenant. This is the right default posture for zero-trust environments.

Setup procedure

Prerequisites

Both organizations need:

- Microsoft 365 with Teams enabled.
- Entra ID (formerly Azure AD). Entra ID Premium P1 is recommended for granular group-level controls and conditional access trust settings.
- A tenant administrator on each side to configure cross-tenant access.
- The partner organization's **tenant ID** (a GUID) or **primary domain name**.

Step 1: Add the partner organization

Perform this in the **host tenant** (the client whose channel will be shared).

1. Sign in to the Microsoft Entra admin center.
2. Navigate to **External Identities → Cross-tenant access settings**.
3. Click **Add organization**.
4. Enter the partner's tenant ID or domain name.
5. Click **Add**.

Repeat this in the partner's tenant, adding the host organization.

> **Reference:** Collaborate with external participants in a shared channel — Microsoft Learn

Step 2: Configure inbound access (host tenant)

This controls whether external users from the partner organization can participate in the host's shared channels.

1. In **Cross-tenant access settings**, click the **Inbound access** link for the partner organization.
2. Go to the **B2B direct connect** tab.

3. On the **External users and groups** tab: choose **Allow access**. Select either **All external users and groups** or limit to specific groups (recommended for tighter control).
4. On the **Applications** tab: choose **Allow access → Select applications → Add Microsoft applications → Office 365**. This covers Teams and SharePoint.
5. Click **Save**.

Step 3: Configure outbound access (host tenant)

This controls whether the host's users can participate in the partner's shared channels (the reverse direction).

1. Click the **Outbound access** link for the same partner organization.
2. Go to the **B2B direct connect** tab.
3. On **Users and groups**: choose which of the host's users/groups can access the partner's channels.
4. On **Applications**: allow **Office 365**.
5. Click **Save**.

Step 4: Configure trust settings (host tenant)

Still within the partner organization's settings:

1. Open **Trust settings**.
2. Choose whether to trust the partner's **MFA claims** and **device compliance claims**.

- Trusting MFA avoids double-prompting external users if they've already completed MFA in their home tenant.
- Trusting device compliance lets you require compliant devices even when managed by the partner.

3. Click **Save**.

> **Tip:** For FSA-regulated clients, consider not trusting external MFA by default. This forces re-authentication under the host's conditional access policies.

Step 5: Mirror configuration in the partner tenant

The partner organization must perform equivalent steps (Steps 1–4) from their side. B2B Direct Connect is a mutual trust — it only works when both sides have enabled it.

> **Important:** Cross-tenant access setting changes can take **up to 6 hours** to propagate. Plan accordingly and set expectations with the client.

Step 6: Configure Teams admin policies

In the Teams admin center:

1. Go to **Teams → Teams policies**.
2. Ensure the relevant policy allows users to **create shared channels** and **invite external users to shared channels**.
3. Optionally, configure an **internal help link** (under **Teams → Teams settings**) that appears when users try to share with organizations that don't have a B2B Direct Connect relationship set up yet. Point this to an internal request form or support page.

> **Reference:** Shared channels in Microsoft Teams — Microsoft Learn

Step 7: Create the shared channel

This is done by the team owner in the Teams client:

1. Right-click the team → **Add channel**.
2. Set channel type to **Shared**.
3. Name the channel descriptively (e.g., "Joint Project Alpha — Acme Corp").
4. Add internal members.
5. Click **Share channel → With people from another org** and invite external users by email.

Who should create the channel

Whoever creates the shared channel becomes the **host tenant** — and that determines where data lives, whose compliance policies apply, and who holds the audit trail.

The general principle

The organization with the stricter compliance requirements should host the channel.

All messages, files, and the associated SharePoint site live in the creating tenant. If a regulated client creates the channel and invites their auditor, the fund data stays under the client's DLP, sensitivity labels, and retention policies. If the auditor creates the channel and invites the client, that same data now lives in the auditor's tenant — and the client has no visibility into whether the auditor's policies are adequate. The audit trail follows the same logic: the host gets every log entry, the external participant's home tenant gets nothing about channel activity.

For a regulated client, losing either data ownership or the audit trail is a non-starter.

Decision by scenario

Scenario	Who should create the channel	Why
Client collaborating with their external auditor	Client	Client retains data ownership and audit trail for compliance
Client collaborating with legal counsel	Client	Attorney-client privilege is easier to assert when the client controls the data
Two peer firms on a joint project	Whichever has stricter compliance obligations	The regulated party should own the data
Vendor providing ongoing support to a client	Client	Client retains control over what the vendor sees and when access ends
eSolia delivering a project to a client	Usually the client — see below	

The eSolia-specific judgment call

When we're delivering a project, there's a choice. If we create the channel in our tenant, we control the data and the lifecycle — convenient for us, but the client loses visibility and audit control. If the client creates the channel and invites us, the data stays in their environment, their policies apply, and they keep the collaboration record.

For most client engagements, **the client should create the channel.** They're the ones with the compliance obligations, they're the ones auditors will ask about data handling, and they should own the collaboration record. Our role is to help them set up the B2B Direct Connect relationship and configure the channel correctly — then join as external participants.

The exception: internal prep work or cross-eSolia coordination about a client engagement belongs in our own tenant. The client doesn't need to see our internal coordination, and we don't want internal notes living in their environment.

Channel ownership rules

Regardless of which tenant hosts the channel:

Every shared channel needs at least two owners. Single-owner channels become unmanageable when that person goes on leave or changes roles. The channel owner should be someone with decision authority over the collaboration — typically a project lead, not an IT admin. IT sets up the B2B Direct Connect plumbing; the business owner manages who's in the channel and what's shared.

Add a one-liner to the channel description documenting its purpose and expected lifespan: "FY2026 audit collaboration with [Auditor Firm]. Review/archive by March 2027." This prevents orphaned channels and gives whoever runs the quarterly access review the context they need to make a keep-or-delete decision.

For naming, use the conventions from the operational considerations section — `EXT – [Partner Name] – [Project/Purpose]`. When someone is scanning a team's channel list six months later, the external relationship should be immediately visible without clicking into the channel.

Security controls and conditional access

Shared channels inherit conditional access policies from the host tenant. You can require MFA for all guest and external users scoped to the Office 365 / SharePoint Online cloud app, require compliant or Entra hybrid-joined devices, and enforce IP-based restrictions at the SharePoint file level. That last one is worth explaining to clients: an external user can access the channel conversation from any location, but they'll be blocked from opening files if they're on a restricted IP.

With **Entra ID Premium**, you can restrict collaboration to specific individuals or security groups rather than allowing an entire partner organization, and choose per-organization whether to trust the partner's MFA and device compliance claims — or force re-authentication under your own policies.

DLP policies that cover Teams chats, channel messages, and SharePoint sites apply to shared channels automatically. The host tenant's sensitivity labels also apply. For FSA clients, this means the existing "Highly Confidential — Fund Information" and "Highly Confidential — Investor Data" labels from the

security guidelines will enforce encryption and restrict sharing within shared channels, with no additional configuration needed.

Audit and compliance capabilities

Shared channels log membership changes, channel lifecycle events, cross-tenant sign-ins, and file access — exactly the kind of audit trail FSA and ISO 27001 auditors ask for.

What is logged

Audit area	What is captured	Where to find it
Channel lifecycle	Create, delete shared channel	Teams audit logs (Purview compliance portal)
Membership changes	Add, remove, promote, demote members (in-tenant and cross-tenant)	Teams audit logs
Cross-tenant sign-ins	B2B Direct Connect authentication events	Entra ID sign-in logs
Policy changes	Cross-tenant access settings created, updated, deleted	Entra ID audit logs
File access	SharePoint file operations in the channel's site	SharePoint audit logs
Message content	Chat and channel messages	Communication compliance (if configured)

Important audit caveat

Audit logs for shared channel activity are only available in the **host (resource) tenant**. The external user's home tenant does not receive audit logs related to their activity in another organization's shared channel. Make sure the client (host) understands they hold the complete audit record.

Access reviews

Entra ID access reviews can detect B2B Direct Connect users in shared channels. Create periodic access reviews scoped to "guest and external users" to recertify who has access. One current limitation: access reviews can detect individual external users but not entire external teams that have been added to a shared channel. (For eSolia's own use of access reviews, see the billing risk discussion in the "Cleaning up existing guest accounts" section below.)

Compliance tools supported

Shared channels support the full Purview compliance stack: eDiscovery (content search and holds), legal hold, communication compliance, information barriers, retention policies, and DLP. One limitation worth flagging to clients: legal hold can be applied to channel-only members from the host organization, but external participants can't be placed on hold. If the client anticipates litigation involving external collaborators, the hold must come from the external party's own tenant.

> **Reference:** B2B Direct Connect overview — Microsoft Learn

Operational considerations

SharePoint site management

Each shared channel creates a separate SharePoint site. This catches people off guard.

For clients with many shared channels, site sprawl becomes a real management issue. Include shared channel sites in the regular SharePoint site inventory, apply backup policies explicitly (they won't inherit the parent team's backup configuration in most third-party tools), and review them during quarterly security reviews. We recommend adding shared channel site audits to the standard quarterly review template rather than treating them as an afterthought.

Naming conventions

Establish a naming convention for shared channels that makes the external relationship obvious:

- `EXT — [Partner Name] — [Project/Purpose]`
- `Shared — Audit 2026 — [Auditor Firm]`

Lifecycle management

Use Entra access reviews or manual quarterly reviews to verify membership is still appropriate. When a project ends or a partner relationship concludes, delete the shared channel rather than leaving it dormant. Archive the associated SharePoint site content per the client's retention policy first. Dormant shared channels with active external membership are exactly the kind of thing that shows up in ISO 27001 surveillance audits.

User communication

Shared channels display visual cues indicating external members and whether a channel comes from another organization. Don't rely on these alone — most users won't notice them.

During onboarding, explicitly tell users: "This channel includes people from [Partner Name]. Treat it like a meeting room with visitors present." That framing sticks better than a policy document. Also advise against screen-sharing entire desktops in shared channel meetings — sharing individual windows prevents accidental exposure of unrelated client data or internal chats.

How eSolia's own tenant handles external sharing today

This section documents our current setup and what we might tighten further. It doubles as a useful reference when clients ask "how do you do it?"

Background

We configured these settings in late 2023, when B2B Direct Connect was still relatively new — Microsoft was recommending it but many tenants hadn't adopted it yet. Some of the SharePoint sharing settings required PowerShell at the time because the admin UI didn't expose them all. The controls have matured

considerably since then, which is why shared channels (the main subject of this guide) are now a realistic option for regular partner relationships.

Current configuration

Our tenant is tighter than a default M365 setup. Here's what's in place:

SharePoint sharing level: Set to **"New and existing guests"** — the second-most-permissive option. This does auto-create guest accounts when sharing with new external users, but several controls below limit who can trigger this and with whom.

Domain allowlist is active. External sharing is restricted to a specific list of approved domains. Sharing with domains not on the list is blocked. This is the "allowlist only" approach our own tenant setup checklist recommends for SMB clients.

External sharing restricted to specific security groups. Only members of "sg External Sharers" and "sg All Users Except Guests" can share externally. A random member of the organization can't invite guests on their own — they need to be in one of these groups.

Guest directory visibility is locked down. In Entra, guest user access is set to the most restrictive option: "Guest user access is restricted to properties and memberships of their own directory objects." Guests can't browse the eSolia directory, search for other users, or see group memberships. They can only see their own profile.

Guest invite permissions are scoped. Entra allows "Member users and users assigned to specific admin roles" to invite guests — the second-most-permissive option. In practice, the SharePoint security group restriction layers on top of this, so even though Entra allows any member to invite, only members of "sg External Sharers" can actually trigger a share that creates a guest.

Guests can remove themselves. The "Allow external users to remove themselves from your organization" setting is enabled. This is Microsoft's recommendation — it reduces stale account buildup from the guest's side.

Guest access auto-expires after 30 days. Guests lose access to SharePoint sites and OneDrive automatically unless the content is re-shared. This is a significant control — it means stale access doesn't persist indefinitely even without manual cleanup.

Verification codes expire after 9 days. External users authenticating via one-time passcode must re-verify frequently.

Guests can't reshare. "Allow guests to share items they don't own" is disabled. A guest can access what was shared with them but can't widen the circle.

Default sharing link type is "Specific people" with View permission. Conservative defaults — users have to deliberately choose a wider audience or grant Edit access. Nobody accidentally creates an "Anyone with the link" situation.

OneDrive is more restrictive than SharePoint. Correct hierarchy — personal storage is locked down tighter than team sites.

Where domain filtering happens

One architectural detail worth understanding: the domain allowlist lives at the **SharePoint layer**, not at Entra. The Entra collaboration restrictions are set to "Allow invitations to be sent to any domain (most

inclusive).” SharePoint’s “Limit external sharing by domain” setting with the approved domain list is what actually enforces the restriction.

This means someone could theoretically create a guest account through a non-SharePoint path — like inviting directly from the Entra admin center or from Teams — to a domain that’s not on the SharePoint allowlist. The SharePoint security group restriction makes this unlikely in practice (most users don’t have Entra admin access), but mirroring the domain allowlist at the Entra level would close the gap completely. That’s noted as a potential improvement below.

What governs each layer

Setting	Where to find it	What it controls	Our current state
Guest user access restrictions	Entra admin center → External Identities → External collaboration settings	What guests can see in the directory	Most restrictive — own directory objects only
Guest invite settings	Same page	Who can invite guest users	Member users + users assigned to admin roles
Collaboration restrictions (domain filtering)	Same page	Which domains can receive guest invitations at the Entra level	"Allow invitations to any domain" — **not restricted at this layer**
SharePoint domain allowlist	SharePoint admin center → Policies → Sharing → More external sharing settings	Which domains can receive shares at the SharePoint level	Active — specific domain allowlist enforced
SharePoint sharing security groups	Same page	Which users can share externally	"sg External Sharers" and "sg All Users Except Guests"
SharePoint tenant sharing level	SharePoint admin center → Policies → Sharing	Whether sharing creates new guest accounts automatically	"New and existing guests"
Guest access expiration	Same page	Automatic expiration of guest site/OneDrive access	30-day expiration enabled
Verification code reauthentication	Same page	How often OTP users must re-verify	9-day expiration
Default link type	SharePoint admin center → Policies → Sharing → File and folder links	What kind of sharing link is pre-selected	"Specific people" with View permission
External user self-removal	Entra admin center → External Identities → External collaboration settings	Whether guests can remove themselves	Enabled
Cross-tenant access settings	Entra admin center → External Identities → Cross-tenant access settings	Per-organization B2B collaboration and B2B Direct Connect policies	B2B collaboration: all allowed (default). B2B Direct Connect: all blocked (default). Trust settings: disabled. One org listed (SB C&S — CSP distributor) inheriting defaults. No client-specific overrides configured yet.
Teams guest access	Teams admin center → Settings & policies → Guest access settings	Whether guests can join Teams, and what they can do	On. Messaging locked down: guests can't edit/delete messages (preserves audit trail). Giphy, memes, stickers [illegible] off. Full meeting capabilities except [illegible] external participants
[illegible]	Teams admin center → [illegible] settings	[illegible]	[illegible]

What's working well

The layered controls are effective across all three systems. Entra locks down guest directory visibility to the tightest setting. SharePoint restricts who can share, with which domains, and auto-expires guest access after 30 days. Teams allows guest participation but with audit-friendly restrictions — guests can't edit or delete their messages, which preserves a complete conversation record.

The external access policies in Teams are worth noting: rather than a single org-wide on/off, there are per-user policies (NoFederationAndPIC, FederationAndPICDefault, FederationOnly) that control who can chat and call externally. This is more granular than most SMB setups.

Shared channels are blocked at both the Teams and Entra levels — the correct posture until you're ready to enable them for specific partner organizations. When that time comes, both layers need to be configured: Entra cross-tenant access settings for the B2B Direct Connect trust, and the Teams external collaboration settings to allow shared channels.

What to be aware of when enabling shared channels

Two settings to revisit before enabling shared channels with a client:

Guest screen sharing is set to "Entire screen." The doc's user communication section recommends advising users to share individual windows instead. Consider changing this to "Single application" at the Teams policy level, especially for shared channels where external participants are present. This prevents accidental exposure of other client data or internal chats visible on the desktop.

Copilot for B2B members is on. This means external users joining your shared channel meetings could use Copilot capabilities. For FSA-regulated clients, verify whether this is acceptable — Copilot summarization of meeting content involving fund data or investor information may have compliance implications.

What could still be improved

Mirror the domain allowlist at the Entra level. The SharePoint domain allowlist is the primary control today, but adding the same list under Entra → External Identities → External collaboration settings → "Allow invitations only to the specified domains" would close the gap for non-SharePoint invitation paths (Teams, direct Entra invitations). Low effort, and it means the domain restriction applies regardless of how the guest account gets created.

Entra directory cleanup. The 30-day expiration removes access to SharePoint sites, but the guest account objects in Entra persist indefinitely. Over years of client engagements, the directory accumulates guest entries from dozens of organizations. They're not a security risk (their access has expired), but they're noise — and an ISO 27001 auditor asking "who are all these external identities?" deserves a clean answer.

Reducing future guest creation

The 30-day access expiration handles the security side. The real improvement is creating fewer guest accounts in the first place. Several collaboration paths don't touch the Entra guest directory at all:

Shared channels (B2B Direct Connect) — the main subject of this guide. External users participate from their own tenant, no guest account created. For the client domains already on your SharePoint allowlist, most probably have Entra ID tenants and qualify. This is the highest-value change for frequent collaborators.

Teams federation (chat and calls) — already enabled. When you chat with an external user via federation, no guest account is created. Limited to conversations — you can't share files through federated chat the way you can in a team channel. But for quick coordination that doesn't need document collaboration, it's clean.

Encrypted email via Purview Message Encryption — send sensitive files as encrypted attachments. The recipient authenticates with a one-time passcode to open the message, no guest account created anywhere. For one-directional file delivery ("here's your report"), this is often good enough. Already included with E3/E5 licensing.

External file sharing outside M365 — you already have the Cloudflare stack. A lightweight Workers app generating time-limited download links from R2 storage would sidestep M365 guest accounts entirely. Overkill for most situations, but if the M365 governance billing becomes a recurring irritation at scale, it's a legitimate architectural escape hatch.

Cleaning up existing guest accounts

The tenant has **235 guest accounts** as of March 2026. No access reviews have been configured. Here's the approach, with a clear-eyed look at why we're recommending PowerShell over Microsoft's built-in governance tools.

Primary approach: quarterly PowerShell cleanup ($0, no billing risk)

A script against Microsoft Graph exports all guest accounts with creation dates and last sign-in activity. Review the list, remove accounts from completed engagements, keep the ones that are still active. Schedule this quarterly.

```
Get-MgUser -Filter "userType eq 'Guest'" -All `
  | Select-Object DisplayName, Mail, CreatedDateTime, SignInActivity `
  | Sort-Object CreatedDateTime
```

For 235 guests, this takes about 30 minutes of admin time per quarter. No governance features touched, no Azure subscription required, no billing surprises. The 30-day SharePoint access expiration already handles the security side — this script is purely directory hygiene, removing the Entra objects left behind after access expired.

Why not Entra access reviews? The billing risk.

Access reviews are the "proper" Microsoft solution for guest lifecycle management, and our E5 licenses include the P2 entitlement to use them. The catch: as of January 15, 2026, Microsoft requires a linked Azure subscription to use Entra ID Governance features for guest users, with MAU-based billing.

The Entra admin center currently displays this banner on the Access Reviews page: "Beginning January 15, 2026, a linked Azure subscription is required to use Entra ID Governance features for guest users. Billing is based on unique guest users included in Entra ID Governance features during the month."

Microsoft's documentation says guests are only charged when they "actively use" governance-exclusive features. But the banner's phrasing — "included in" rather than "actively use" — is ambiguous enough to be a concern. If creating an access review scoped to guest users counts all 235 guests as "included," the bill could be ~~$176/month~~ ($2,100/year) just for the privilege of automating what a PowerShell script does for free.

This is a pattern worth recognizing: Microsoft's own sharing architecture creates guest accounts automatically, then Microsoft charges you to manage the sprawl with their governance tools. The guest objects in Entra are a side effect of their system, not something we chose. A 15-line PowerShell script sidesteps the entire billing model.

When access reviews would make sense: If eSolia's guest count grows into the thousands (unlikely at our scale), or if we need automated enforcement that removes access without human review (the 30-day SharePoint expiration already does this), or if a client requires it for compliance certification purposes.

Recommended next steps

1. **Mirror domain allowlist to Entra (quick win):** Copy the SharePoint domain allowlist into Entra → External Identities → External collaboration settings → "Allow invitations only to the specified domains." Takes minutes, closes the non-SharePoint invitation path gap.
2. **Run the first PowerShell guest cleanup (this quarter):** Export the 235 guest accounts. Remove accounts from completed engagements — expect to cut this list significantly. Save the script for quarterly reuse.
3. **Migrate frequent partners to shared channels (ongoing):** For the client domains on your allowlist that you collaborate with most frequently, begin setting up cross-tenant access and B2B Direct Connect. Each partner migrated to shared channels is a relationship that stops creating guest accounts.
4. **Use encrypted email for one-off file delivery:** When a client or partner just needs a document, Purview Message Encryption avoids creating a guest account for a single file share.

Licensing and cost summary (eSolia-specific)

eSolia runs M365 E3 (most staff) and M365 E5 (a couple of admin/IT users). E3 includes Entra ID P1. E5 includes Entra ID P2.

Capability	License required	Covered by E3?	Covered by E5?	Extra cost for eSolia
SharePoint sharing level settings	Any M365 plan	Yes	Yes	None
Entra external collaboration settings (domain allow/block)	Any M365 plan	Yes	Yes	None
Cross-tenant access settings (B2B Direct Connect)	Any M365 plan with Entra ID	Yes	Yes	None
Conditional access for guests (basic)	Entra ID P1	Yes	Yes	None
Conditional access for guests (risk-based)	Entra ID P2	No	Yes	None if scoped to E5 admins
PowerShell/Graph API guest cleanup	Any M365 plan	Yes	Yes	**None — recommended approach**
Purview Message Encryption	E3 or E5	Yes	Yes	None
Shared channels (B2B Direct Connect)	Any M365 plan with Entra ID	Yes	Yes	None
Access reviews (create and review)	Entra ID P2	No	Yes	**Billing risk:** Azure subscription + ~$0.75/guest/month MAU if guests are "included." At 235 guests, worst case ~$176/month.
Access reviews (E3 user as reviewer)	Entra ID P2	No	No	~$9/user/month P2 add-on per reviewer
Entitlement management (access packages)	Entra ID Governance add-on	No	No	~$7/user/month on top of P2

Bottom line: The recommended approach (PowerShell cleanup + shared channels + encrypted email) costs **$0** beyond existing licensing. Access reviews are available through E5 but carry billing risk for guest users since January 2026. At 235 guests, the risk isn't worth it when the free alternative takes 30 minutes per quarter.

References:

- Entra ID Governance licensing fundamentals — Microsoft Learn
- Entra ID Governance licensing for guest users — Microsoft Learn
- Manage guest access with access reviews — Microsoft Learn
- Adding an expiration date for Entra ID guest accounts — Practical365 (DIY PowerShell approach)
- Entra ID Governance levies charges for guest accounts — Office 365 IT Pros

Integration with existing eSolia service guides

This guide connects to several existing eSolia M365 service documents:

Related guide	Connection
M365 Tenant Setup Checklist v2 — Section 6.3 (External Sharing Policy Decision)	Shared channels are the Teams-native implementation of the "Allowlist Only" recommendation. Cross-tenant access settings serve as the allowlist.
M365 Security Guidelines for Financial Services v1 — Section 4.4 (Teams and SharePoint Security)	For clients where guest access is set to "Off," shared channels provide a controlled alternative for necessary external collaboration.
M365 Security Guidelines for Financial Services v1 — Section 5.1 (Sensitivity Labels)	Host tenant sensitivity labels apply to shared channels automatically. No separate configuration required.
M365 Security Guidelines for Financial Services v1 — Section 5.2 (DLP)	DLP policies covering Teams chats, channels, and SharePoint apply to shared channels. Verify coverage includes "Teams channel messages" location.
Cloudflare Zero Trust SMB Guide	Not directly related, but for clients using Cloudflare Access to protect internal apps, shared channels can replace ad-hoc file sharing with external partners for project collaboration.

Quick reference: key portal URLs

Portal	URL / Navigation
Microsoft Entra admin center (cross-tenant access)	https://entra.microsoft.com → External Identities → Cross-tenant access settings
Microsoft Entra admin center (external collaboration)	https://entra.microsoft.com → External Identities → External collaboration settings
Teams admin center (guest access)	https://admin.teams.microsoft.com → Settings & policies → Guest access settings
Teams admin center (external collaboration overview)	https://admin.teams.microsoft.com → External collaboration → Overview
Teams admin center (external access / federation)	https://admin.teams.microsoft.com → External collaboration → External access
Teams admin center (B2B member access)	https://admin.teams.microsoft.com → Settings & policies → B2B member access settings
Teams admin center (Teams policies)	https://admin.teams.microsoft.com → Teams → Teams policies
Purview compliance portal (audit logs, DLP, eDiscovery)	https://compliance.microsoft.com
SharePoint admin center (sharing policies)	https://admin.microsoft.com/sharepoint → Policies → Sharing

Source material and further reading

- Shared channels in Microsoft Teams — Microsoft Learn
- Collaborate with external participants in a shared channel — Microsoft Learn
- B2B Direct Connect overview — Microsoft Entra External ID — Microsoft Learn
- Security guide for Microsoft Teams — Microsoft Learn
- Microsoft Teams security: collaboration settings (2025) — Solutions2Share
- Full guide: Cross-Tenant Access (B2B Direct Connect) — PlexHosted
- Managing Microsoft Teams governance and compliance — Orchestry
- Shared Channels and B2B Direct Connect — Intelogy

Contact Us

eSolia Inc. Shiodome City Center 5F (Workstyling) 1-5-2 Higashi-Shimbashi, Minato-ku Tokyo 105-7105, Japan

Phone	03-4577-3380
Email	hello@esolia.co.jp
Web	https://esolia.co.jp/en
Hours	Monday-Friday, 9:00-18:00 JST