

CLIENT IT / PRODUCTION SETUP

Deploy Microsoft 365 for your Evidize organization

An IT administrator's guide to Microsoft sign-in, user provisioning, Outlook deployment, delegated drafts, and Teams interview transcripts in Evidize.

Configure each capability independently. Use your own Microsoft tenant and an Evidize organization administrator account. Features appear only when their production configuration is available. Keep a working recovery sign-in method until your IT team completes acceptance.

Your setup path

1. Prepare identities and deployment scope
2. Review the permissions
3. Connect Microsoft sign-in
4. Configure Entra provisioning
5. Deploy Evidize for Outlook
6. Enable portal drafts and calendar holds
7. Permit transcript import for named organizers
8. Operate, recover, and complete acceptance

Updated 23 September 2026

This PDF and the public guide share the same maintained source. Complete your own acceptance before broad rollout.

1. Prepare identities and deployment scope

Use Settings > Team & access > Microsoft 365 in <https://portal.evidize.com>. Record your Directory (tenant) ID, the immutable Microsoft user object IDs of your recruiters, and the object IDs of organizers whose meetings may be imported. Email addresses are display and contact details; they do not establish identity ownership.

Create a dedicated recruiter deployment group. Manage Evidize sign-in assignment, provisioning scope, Outlook installation, and transcript organizer policy separately. Removing one assignment does not automatically remove every other capability.

Your administrators grant Microsoft consent and configure deployment using their existing administrative roles. Evidize itself does not need a customer Azure subscription role, a directory administrator role, or permission to administer your tenant. Outlook requires a compatible Microsoft 365 client and Exchange Online mailbox; Teams transcription must be permitted by your licensing and meeting policies.

1. Select the intended Evidize organization and confirm you are its administrator.
2. Record the production client IDs displayed in Evidize. Keep development and staging registrations, credentials, redirects, and deployment manifests separate.
3. Decide which recruiters need sign-in, provisioning, portal drafts, Outlook installation, and transcript import. Start with a defined deployment group.
4. Retain an authorized recovery administrator and document your organization's retention and AI preferences.

2. Review the permissions

Evidize Portal (Production) is the identity application. It uses openid, profile, and email for sign-in. The production SSO client ID is a7172fc0-085c-4295-8721-188cb05def35. Identity access does not grant mailbox or transcript access.

Evidize for Outlook uses Office.js ReadWriteItem to work with the currently open Outlook item. Installing the add-in does not authorize background mailbox access.

The separate delegated mailbox connection requests Mail.ReadWrite only when email drafts are enabled, and Calendars.ReadWrite only when calendar holds are enabled, with offline_access for renewal of that connection. Microsoft grants broader mailbox access than a drafts-only permission; Evidize restricts its operations to tracked draft messages and attendee-free holds created by Evidize. Users review and send invitations themselves in Outlook.

The separate transcript service uses application OnlineMeetingTranscript.Read.All and OnlineMeetings.Read.All. Restrict it in Microsoft Teams to explicitly approved organizers, and enter the same organizer IDs in Evidize. Evidize only requests meetings explicitly linked to an interview occurrence. Microsoft organizer policy covers an organizer's meetings, so the additional interview linkage is enforced by Evidize.

SCIM uses an Evidize-issued, organization-scoped bearer credential. Microsoft Entra pushes user changes to Evidize; Evidize does not read your directory to provision users. Administrator roles remain explicitly managed in Evidize.

The integration does not request Mail.Send, application mailbox permissions, recordings, SharePoint access, directory write permissions, or Azure subscription access. Review each consent screen against the displayed capability before granting it.

[Microsoft: Teams application access policies](#)

3. Connect Microsoft sign-in

Connect the organization's tenant and bind each existing member to their immutable Microsoft user object ID. Evidize validates tenant and identity bindings; matching email text does not link an account. Follow the guided consent, verification, and activation controls shown in the portal.

Publisher verification is a separate Microsoft verification process. Check the actual publisher status shown on the Microsoft consent screen. Do not assume a logo or an evidize.com publisher domain means that Microsoft has verified the publisher.

1. In Microsoft 365 settings, enter your Directory (tenant) ID and save the tenant connection.
2. Use the guided Microsoft consent action and confirm that the correct tenant and Evidize identity application are displayed.
3. Link existing Evidize users using their Microsoft object IDs, or complete SCIM provisioning as described below. Resolve identity conflicts explicitly instead of relinking by email.
4. During your human acceptance, use the built-in sign-in verification control with a linked user, review the result, and activate SSO when the portal permits it.
5. Keep your recovery sign-in method available. If SSO is the only permitted method, restore an authorized recovery path before disconnecting it.

[Detailed SSO setup guide](#)

[Microsoft: publisher verification](#)

4. Configure Entra provisioning

Create a separate non-gallery enterprise application named Evidize Provisioning. Configure automatic provisioning using the SCIM tenant URL copied from Evidize. The URL is organization specific: `https://api.evidize.com/scim/v2/{organization_id}`. Never substitute another organization's ID.

Provision `userName`, `externalId`, `active`, `name.givenName`, `name.familyName`, and the primary work email. Map Microsoft's `objectId` to `externalId`. Scope provisioning to assigned users and groups. Group assignment controls which users are provisioned; SCIM group objects and group-to-administrator role mapping are not used.

Disabling or deleting a provisioned user revokes that user's Evidize access and mailbox connection. Removing provisioning credentials stops future synchronization but does not delete existing users. Explicitly offboard users before stopping provisioning when immediate revocation is required.

1. Create or rotate a provisioning token in Evidize. Copy it immediately; Evidize only shows the secret once.
2. In Entra > Enterprise applications > Evidize Provisioning > Provisioning, select Automatic, paste the tenant URL and secret token, and configure the attribute mappings above. Under Mappings, keep Provision Microsoft Entra ID Users enabled and disable Provision Microsoft Entra ID Groups; group assignment scopes users without provisioning group objects.
3. Select Sync only assigned users and groups. Assign the intended recruiter group and review its direct members; do not rely on nested group expansion.
4. During human acceptance, use Entra's connection and on-demand provisioning controls, inspect its provisioning logs, and confirm ordinary user access in Evidize before starting broad provisioning.
5. For rotation, create a new credential, replace the secret in Entra, and complete human verification during the one-hour overlap. Revoke old credentials after confirmation. Check the expiry displayed by Evidize and rotate before it expires. Before removing the administrator who issued a token, rotate it from a retained administrator account; issuer removal revokes that administrator's provisioning credentials.
6. For reconciliation or delayed updates, review Entra provisioning logs, resolve the reported safe error, then use Entra's retry/restart provisioning controls. Do not create duplicate accounts to bypass an immutable identity conflict.

Microsoft: provisioning with SCIM

5. Deploy Evidize for Outlook

The production manifest is <https://portal.evidize.com/outlook-manifest.xml>. Keep its add-in ID stable when updating an existing deployment. The portal and task pane use production HTTPS assets. Use the Microsoft 365 Integrated apps portal to deploy it to the intended recruiter users or group.

Installation is independent of Entra SSO assignment and provisioning. The deployment confirmation checkbox in Evidize records your administrator's attestation; it is not proof that the add-in has reached every device. Allow for Microsoft deployment propagation before your human acceptance.

1. Download the production XML from Evidize Microsoft 365 settings.
2. Open the Microsoft 365 admin center > Settings > Integrated apps, choose Upload custom apps, and upload the Office add-in XML manifest.
3. Review ReadWriteItem access, select the recruiter deployment scope, and complete deployment using your organization's authorized administrator.
4. During human acceptance, open Outlook as an assigned recruiter and check the Evidize commands in an appointment. Confirm the organizer reviews the Evidize handoff and controls the final invitation.

5. Mark deployment complete in Evidize after your administrator has completed the rollout. To withdraw the add-in, remove its deployment or assignment in Integrated apps.

Production Outlook manifest

Microsoft: centralized Office add-in deployment

6. Enable portal drafts and calendar holds

Enable delegated Outlook access in organization Microsoft 365 settings and select email drafts, calendar holds, or both. Each recruiter connects their own Microsoft account from an interview's Outlook drafts panel. A tenant administrator may need to grant consent according to your Microsoft consent policy. Save your capability choices before starting the consent action.

The connection must belong to the user's bound identity in the organization's configured tenant. The portal tracks the owner, request ID, Microsoft item ID, and version. Only the owner can edit their tracked item. Repeating the same creation request does not intentionally create another item.

A calendar hold has no attendees. It is not a sent invitation. A draft email is not sent by Evidize. If an item is changed in Outlook, refresh it before editing again. Sent messages and meetings with attendees are no longer editable through this draft workflow.

Changing enabled draft or hold capabilities revokes stored Evidize connection tokens and requires recruiters to reconnect with the new permission selection. Existing Outlook items remain. Microsoft may retain an earlier broader tenant consent grant; your IT administrator can revoke that grant separately when removing a permission.

1. Enable the Microsoft connection, select email drafts and/or calendar holds, and save the organization's settings. Grant only the selected delegated scopes when administrator consent is needed.
2. In an authorized interview, choose Connect Microsoft in Outlook drafts and review the delegated consent screen.
3. Prepare an email draft or attendee-free calendar hold. Review the saved item in Outlook before sending or inviting anyone.
4. If the portal reports a version conflict, refresh the item and reconcile your changes instead of overwriting another edit.
5. Disconnect a recruiter's mailbox in the portal to stop Evidize access. For incident response, also revoke the applicable Microsoft delegated grant or user sessions using your normal IT process.

7. Permit transcript import for named organizers

Consent to the separate Evidize Transcript Service application using the production client ID displayed in settings. Grant only OnlineMeetingTranscript.Read.All and OnlineMeetings.Read.All. Configure a Teams application access policy for named organizer object IDs; do not grant a global organizer policy.

If an organizer already has an application access policy, preserve its other approved applications. Have your Teams administrator review the combined policy before assignment. Policy propagation can take up to 30 minutes. The following example is for a new dedicated policy; replace all placeholders with values from your own tenant and Evidize settings.

Enter the same approved organizer object IDs in Evidize and enable transcript import. Link each Teams interview occurrence with its organizer, join URL, start, and end. Evidize's scheduled worker checks linked meetings every two minutes, persists work in SQL, and applies throttling and bounded retries for 24 hours. A two-minute schedule is not a guarantee that Microsoft has published a transcript.

Teams must actually produce a transcript. Evidize does not start recording, transcribe a recording, or create missing speech. Missing transcription, denied access, expired sources, or removed connections produce an actionable import state. Recurring meetings must be linked with the correct occurrence times.

1. Review the separate transcript application's client ID and grant the two application permissions in the intended Microsoft tenant.
2. Use MicrosoftTeams PowerShell to configure the organizer application policy and assign it only to approved organizers.
3. Save the organizer allowlist in Evidize and enable import. Configure organization AI preferences separately; ingestion does not require AI credits.
4. During human acceptance, conduct an approved Teams interview with transcription enabled, link that occurrence in Evidize, and review the imported text and source details.
5. To revoke access, disable transcript import in Evidize, remove the service from the applicable organizer policies, and revoke its Microsoft application grant if no longer required. Stored evidence remains subject to your retention and preservation rules.

```
Connect-MicrosoftTeams -TenantId '<customer-tenant-id>'
New-CsApplicationAccessPolicy -Identity 'Evidize-Transcripts' `
  -AppIds '<production-transcript-client-id>' `
  -Description 'Approved Evidize interview organizers'
Grant-CsApplicationAccessPolicy -PolicyName 'Evidize-Transcripts' `
  -Identity '<approved-organizer-object-id>'
```

[Microsoft: organizer application access policy](#)

[End-user transcript and analysis guide](#)

8. Operate, recover, and complete acceptance

Imported transcripts are private interview evidence. Viewing and download follow session-specific access. Preserve source versions and citations when reviewing analysis. Missing speaker names or timestamps are shown as unavailable; they are not guessed.

Analysis is currently unavailable; transcript import and review remain independent. Import, viewing, technical retries, and automatic late-segment refreshes are uncharged. When analysis becomes available and organization AI settings permit it, the initial completed interview analysis costs 10

credits. A deliberate reanalysis of changed assessment context requires a separate quote. AI output does not change human scorecards, rankings, integrity verdicts, or hiring decisions.

Retention, preservation holds, exports, and deletion apply to transcripts and their analysis. Deleting transcript evidence suppresses automatic reimport. Cross-organization transfer of interviews containing Microsoft bindings or transcripts is initially blocked.

When reporting a problem, provide the organization and interview reference, approximate time, affected capability, and safe error code. Never include bearer tokens, authorization codes, private keys, transcript text, or candidate details in ordinary support messages.

- 1.** Complete human acceptance for SSO and recovery, provisioning/deprovisioning, credential rotation, Outlook deployment, draft ownership and concurrent edits, organizer restrictions, transcript import and citations, and retention/export/deletion.
- 2.** After analysis is separately enabled, confirm AI billing and output using approved interview data and an authorized credit budget. This is not required to import or read transcripts.
- 3.** Check denied access with unauthorized users and organizers. A same-tenant deployment cannot establish cross-tenant isolation; schedule a separate customer-tenant validation before relying on that assurance.
- 4.** For authorization failures, check the capability's consent, bound tenant, organizer allowlist and policy, revoked credentials, and the displayed provisioning or import error before retrying.
- 5.** Disable the affected capability while investigating. Revoking an integration does not erase records already retained under your policy or preservation hold.

[Contact Evidize](#)