Diktiro

GUIDE FOR IT ADMINISTRATORS

Deploying Diktiro in your organisation

Installation and software distribution (MDM), firewall and proxy, permissions, Microsoft Entra ID and user management — everything your IT needs for the rollout.

Contents

1	Installers and system requirements	Downloads, signatures, operating systems
2	Installing on Windows	Manual, silent, Intune, GPO/SCCM/RMM, updates
3	Installing on macOS	Manual, Terminal, MDM, privacy profile
4	Central settings via Group Policy	ADMX template, registry values (Windows)
5	Network, firewall and proxy	Allowlist, proxy/PAC, TLS inspection, test
6	Rights and permissions	Administrator rights, macOS privacy, storage
7	Connecting Microsoft Entra ID (optional)	Two applications, sign-in, SCIM, troubleshooting
8	Inviting users and licences	Roles, invitations, removal, billing
9	Data protection and security	Data flows, audio, server locations

1 Installers and system requirements

There is one installer for Windows and one each for Macs with Apple silicon and with an Intel processor. Files with `latest` in their name are always the newest published version.

All files are located at:

```
https://releases.diktiro.ai/
```

PLATFORM	FILE (ALWAYS THE LATEST VERSION)
Windows 64-bit (x64)	`Diktiro-AI-Setup-latest-x64.exe`
macOS Apple silicon (M1 and later)	`Diktiro-AI-latest-arm64.pkg`
macOS Intel processor	`Diktiro-AI-latest-x64.pkg`

The file names stay the same; these addresses always hold the current version. The current version number is in `latest.yml` in the same folder.

1.1 Signatures

PLATFORM	SIGNATURE
Windows	Signed by **AI Union UG (haftungsbeschränkt)**, Althengstett, Germany, via Microsoft Trusted Signing (issuer "Microsoft ID Verified CS AOC CA 03"), with a timestamp. The signing certificates are each valid for only a few days and therefore change regularly. Please base AppLocker or WDAC rules on the **publisher**, not on a single certificate or a file hash.
macOS	App and package are signed with an Apple Developer ID (Linus Meister Magsino, managing director of AI Union UG; **Team ID** `GXHT57R6GR`) and notarised by Apple. Gatekeeper allows the installation without any exception.

1.2 System requirements

PLATFORM	REQUIREMENT
Windows	Windows 10 (version 1809 or later) or Windows 11, 64-bit (x64). There is currently no version for Windows on ARM.
macOS	macOS 12 (Monterey) or later. Recording system audio in the Notetaker (meeting notes) requires macOS 13 or later.
All	A microphone (built-in, headset or USB), internet access as described in chapter 5, and a default browser for signing in.

2 Installing on Windows

The setup installs Diktiro for **all users of the device** into `C:\Program Files\Diktiro AI`. This requires administrator rights once; afterwards the app runs with standard user rights. No restart is needed.

2.1 Manual

1. Run `Diktiro-AI-Setup-<version>-x64.exe` and confirm the User Account Control prompt.
2. Follow the wizard. The target folder can be changed.
3. Open Diktiro from the Start menu ("Diktiro AI") and sign in.

2.2 Silent (unattended)

Run as administrator or in the system context:

```
Diktiro-AI-Setup-<version>-x64.exe /S

:: different target folder (/D= must be the last parameter, without quotes)
Diktiro-AI-Setup-<version>-x64.exe /S /D=D:\Programs\Diktiro AI
```

- A running Diktiro app is closed before the installation.
- After a silent installation the app does not start by itself. People open it once from the Start menu.
- Exit code `0` means success.

2.3 Microsoft Intune (Win32 app)

1. Create the package with the *Microsoft Win32 Content Prep Tool*:

   ```
   IntuneWinAppUtil.exe -c <source> -s Diktiro-AI-Setup-<version>-x64.exe -o <output>
   ```

2. In Intune: *Apps → Windows → Add → Windows app (Win32)* and upload the `.intunewin` file.
3. Use the following settings:

SETTING	VALUE
Install command	`Diktiro-AI-Setup-<version>-x64.exe /S`
Uninstall command	`"%ProgramFiles%\Diktiro AI\Uninstall Diktiro AI.exe" /S` If Intune does not find the file: `"%ProgramW6432%\Diktiro AI\Uninstall Diktiro AI.exe" /S`
Install behavior	System
Device restart behavior	No specific action
Return codes	`0` success, `3010` success (soft reboot)
Requirements	64-bit, Windows 10 1809 or later
Detection rule	Registry: key `HKEY_LOCAL_MACHINE\Software\Diktiro`, value `Version`, detection method "Version comparison", **greater than or equal to** the deployed version. "Associated with a 32-bit app on 64-bit clients": **No**.

2.4 Group Policy, SCCM/ConfigMgr, RMM tools

Any tool that runs a program in the system context (for example ConfigMgr, NinjaOne, Datto RMM, PDQ Deploy or a Group Policy startup script) uses the silent command from 2.2. As detection criterion, use the same registry value `HKLM\Software\Diktiro\Version`. It contains the installed version number; next to it, `InstallLocation` holds the installation folder.

2.5 Updates

Diktiro checks every 15 minutes whether a new version exists, downloads it from `releases.diktiro.ai` and installs it when the person agrees. Because Diktiro is installed for all users, Windows asks for **administrator rights** during the update.

> **Recommendation for managed devices**
>
> If your staff work without administrator rights, turn off automatic updates with the policy **"Disable in-app auto-update"** (`DisableAutoUpdate`, chapter 4). You then distribute new versions through your software distribution, for example as a new version of the Intune app with an adjusted detection rule. The current version number is always available at `https://releases.diktiro.ai/latest.yml`.

2.6 Uninstalling

- Manual: *Settings → Apps → Installed apps → Diktiro AI → Uninstall*.
- Silent: `"%ProgramFiles%\Diktiro AI\Uninstall Diktiro AI.exe" /S`
- Users' settings and local history are kept (`%APPDATA%\@diktiroai\desktop`). If nothing should remain, delete this folder as well.

3 Installing on macOS

The package installs `Diktiro AI.app` into `/Applications`. Choose the package that matches the processor: **arm64** for Macs with Apple silicon, **x64** for Intel Macs. A running Diktiro app is closed before the installation.

3.1 Manual

1. Open `Diktiro-AI-<version>-arm64.pkg` (or `-x64.pkg`) and follow the installer. An administrator password is required.
2. Start Diktiro from the "Applications" folder and sign in.
3. On the first dictation, macOS asks for the microphone; for the keyboard shortcut and for inserting text, the app opens the "Accessibility" setting (see chapter 6).

3.2 Terminal or script

```
sudo installer -pkg Diktiro-AI-<version>-arm64.pkg -target /
```

3.3 Distribution via MDM

The package is signed and notarised by Apple. It can therefore be distributed like any other package, for example in Microsoft Intune as a "macOS app (PKG)" or in Jamf Pro as a package in a policy. The package identifier is `diktiro.ai.app`.

> **Note**
> macOS currently has no centrally managed settings (no configuration profiles for the app's settings). The policies in chapter 4 apply to Windows only. Diktiro has not yet tested distribution via MDM on the Mac itself. Please test it with a small group of devices first.

3.4 Pre-approving permissions (PPPC profile)

With a "Privacy Preferences Policy Control" (PPPC) profile you can pre-approve Accessibility on managed Macs, so staff are not prompted for it. The values:

FIELD	VALUE
Identifier (bundle ID)	`diktiro.ai.app`
Code requirement	`identifier "diktiro.ai.app" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = GXHT57R6GR`
Accessibility	**Allow**. Needed for the keyboard shortcut (e.g. the Fn key) and for inserting the text.
Apple Events (Automation)	**Allow** for the receiver "System Events": identifier `com.apple.systemevents`, code requirement `identifier "com.apple.systemevents" and anchor apple`. Diktiro uses it to determine the active program and to insert the text.

- **Microphone** and **Screen Recording** cannot be pre-approved via MDM; Apple only allows denying them. Staff confirm the microphone once themselves. Screen Recording is needed only by the Notetaker, to record the sound of a meeting.
- You can check the code requirement on a Mac with the app installed: `codesign -dr - "/Applications/Diktiro AI.app"`
- The code requirement depends on the Team ID `GXHT57R6GR`. Should the Team ID change in future, the profile must be updated.

3.5 Updates

Diktiro checks for a new version every 15 minutes and installs it when the person agrees. This replaces `/Applications/Diktiro AI.app`. Whether that works without administrator rights depends on the file permissions of the app. On managed Macs we recommend distributing new versions via your MDM: a new package with the same package identifier replaces the existing version. There is no policy to turn off updates on the Mac.

3.6 Uninstalling

```
osascript -e 'quit app "Diktiro AI"'
sudo rm -rf "/Applications/Diktiro AI.app"
sudo pkgutil --forget diktiro.ai.app
# optional, per user: settings and local history
rm -rf ~/Library/Application\ Support/@diktiroai/desktop
```

4 Central settings via Group Policy (Windows)

On Windows devices, some settings can be set centrally and locked for staff. Diktiro reads them at every start from the registry under `HKEY_LOCAL_MACHINE\Software\Policies\Diktiro`.

POLICY IN THE TEMPLATE (REGISTRY VALUE)	TYPE AND VALUES	EFFECT
Disable in-app auto-update `DisableAutoUpdate`	DWORD `1` = updates off	No update check, no update notices, no installation from within the app. You then distribute new versions yourself.
Restrict sign-in to Microsoft SSO `SsoOnly`	DWORD `1` = on	The app offers only "Sign in with Microsoft"; Google and e-mail/password are hidden.
Launch Diktiro at login `LaunchAtLogin`	DWORD `1` = on, `0` = off	Sets whether Diktiro starts at sign-in and locks the switch in the app. Takes effect from the app's first start.
Diktiro app language `DefaultUiLanguage`	String `de` or `en`	Sets the interface language and locks the selection.
Dictation history storage `HistoryMode`	String `CLOUD_ONLY`, `LOCAL_ONLY`, `SYNC`	Where the recognised text is stored: `CLOUD_ONLY` (default) in the Diktiro account on EU servers; `LOCAL_ONLY` encrypted on the device only, the text is never sent for storage; `SYNC` on the device and in the account.

4.1 How to set the policies

- **Group Policy (GPO):** You receive the templates `Diktiro.admx` and `en-US\Diktiro.adml` from Diktiro support. Copy them into the central store (`PolicyDefinitions`). The settings then appear under *Computer Configuration → Administrative Templates → Diktiro AI*.
- **Microsoft Intune:** Upload the template under *Devices → Configuration → Import ADMX* and create a profile from "Imported Administrative templates". Alternatively, set the registry values by script.
- **Directly in the registry**, for example by script or RMM tool:

```
reg add "HKLM\Software\Policies\Diktiro" /v DisableAutoUpdate /t REG_DWORD /d 1 /f
reg add "HKLM\Software\Policies\Diktiro" /v SsoOnly /t REG_DWORD /d 1 /f
reg add "HKLM\Software\Policies\Diktiro" /v DefaultUiLanguage /t REG_SZ /d en /f
reg add "HKLM\Software\Policies\Diktiro" /v HistoryMode /t REG_SZ /d LOCAL_ONLY /f
```

The app reads the values at start-up with `reg.exe`. If `reg.exe` is blocked for users, the policies have no effect. Older versions of the template also contained fields for tenant ID, domain hint and API address. These had no effect and have been removed; please use the current template.

5 Network, firewall and proxy

Diktiro needs outbound HTTPS connections only. There are no inbound ports, no port forwarding and no local server reachable from the network.

5.1 Allowlist

Please allow the following destinations — by **host name** (FQDN) wherever possible, not by IP address. All connections use TCP port 443 (TLS).

DESTINATION	PORT	PURPOSE	NEED
`api.diktiro.ai`	443 HTTPS	Everything the app does: sign-in, dictation (audio transfer), notes, dictionary, settings, models for on-device transcription, technical diagnostics	REQUIRED
`releases.diktiro.ai`	443 HTTPS	Automatic updates, installers, introduction video	RECOMMENDED

In addition, the app opens some pages in the staff member's **default browser**. These destinations therefore concern your browser policies, not the app itself:

DESTINATION	PORT	PURPOSE	NEED
`admin.diktiro.ai`	443 HTTPS	Diktiro portal (users, licences, invoices), accepting invitations, resetting passwords	REQUIRED
`login.microsoftonline.com`	443 HTTPS	"Sign in with Microsoft" (work account, Microsoft Entra ID)	WITH MICROSOFT SIGN-IN
`accounts.google.com`	443 HTTPS	"Sign in with Google"	OPTIONAL
`checkout.stripe.com`, `billing.stripe.com`	443 HTTPS	Buying licences and managing invoices (only whoever pays in the portal)	ADMIN
`diktiro.ai`	443 HTTPS	Website, help, privacy and contract pages	OPTIONAL

IP addresses

`api.diktiro.ai` runs in Microsoft Azure, region Germany West Central (Frankfurt), and currently resolves to `4.185.185.168`. This address is not contractually guaranteed and may change. Please use FQDN rules. `releases.diktiro.ai` is delivered through Microsoft Azure Front Door, whose addresses change; only FQDN rules are possible here.

5.2 Proxy and PAC

- The app uses the **operating system's proxy settings**: fixed proxy, automatic detection (WPAD) and PAC scripts. There is no separate proxy setting in the app, and none is needed.
- **Proxy authentication is currently not supported** (Basic, NTLM, Kerberos). If your proxy requires authentication, the app shows "Der Proxy Ihrer Kanzlei verlangt eine Anmeldung." (your proxy requires a sign-in). Please allow `api.diktiro.ai` and `releases.diktiro.ai` **without proxy authentication**, for example as an exception in the PAC file or in the proxy rule.
- The app uses the **operating system's certificate store** (Windows certificate store, macOS keychain).

5.3 TLS inspection (SSL break and inspect)

If your firewall inspects encrypted traffic, Diktiro works as long as your firewall's root certificate is in the operating system's certificate store. If it is missing, the app reports that the firewall is inspecting the traffic.

Recommendation: exempt api.diktiro.ai from inspection

While dictating, the app sends the audio as a continuous stream over one HTTPS connection and receives the recognised text on the same connection. Devices that buffer requests completely before forwarding them delay the text recognition. The app then falls back to a slower transfer after the recording. Dictation still works, but the text appears later.

5.4 Long-running connections

- A dictation or notes connection stays open for the duration of the recording, which can be several minutes. The server sends a keep-alive signal every 15 seconds.
- Please set idle timeouts for `api.diktiro.ai` to **at least 60 seconds**. Do not limit the total duration of a connection to less than the longest expected recording.
- WebSockets (`wss://`) are not currently used. Future versions may use them; we therefore recommend not blocking WebSocket upgrades to `api.diktiro.ai`.

5.5 Testing the connection

From the workstation, in the context of a standard user. Each test should show a successful connection or the status code **200**.

Windows (PowerShell)

```
Test-NetConnection api.diktiro.ai -Port 443
(Invoke-WebRequest https://api.diktiro.ai/health -UseBasicParsing).StatusCode
```

macOS (Terminal)

```
curl -sS -o /dev/null -w "%{http_code}\n" https://api.diktiro.ai/health
```

Note: `Test-NetConnection` checks only the direct connection and ignores the proxy. `Invoke-WebRequest` and `curl`, like the app, use the system's proxy settings.

6 Rights and permissions

Only the installation needs administrator rights. In operation, Diktiro runs with the rights of the signed-in person, without a service, without a driver and without system-wide keyboard hooks.

6.1 Windows

WHAT	WHY, AND WHAT TO CONSIDER
Administrator rights	Only for installation, updates from within the app and uninstalling (installation for all users into `C:\Program Files`).
Microphone access	Under *Settings* → *Privacy & security* → *Microphone*, "Microphone access" and "Let desktop apps access your microphone" must be turned on.
`powershell.exe`	Diktiro inserts the text via the clipboard and the key combination Ctrl+V into the active program. For this, the app briefly calls PowerShell: it determines the active window and triggers Ctrl+V. PowerShell must be executable for users, in full language mode (not "Constrained Language Mode"). If PowerShell is blocked, the text stays on the clipboard and can be pasted manually with Ctrl+V.
`reg.exe`	Reads the policies from chapter 4 at start-up and checks the default browser.
Default browser	Signing in opens the default browser. The app then returns via the `diktiro://` link, which the setup registers.
Keyboard shortcuts	The app only queries the state of the configured keys (default for "hold to talk": Ctrl+Windows key). It installs no keyboard hook and does not record keystrokes.
AppLocker / WDAC	Please phrase rules via the publisher "AI Union UG (haftungsbeschränkt)" (see chapter 1.1).

6.2 macOS

macOS asks each person for these permissions (*System Settings* → *Privacy & Security*). Accessibility and Automation can be pre-approved via MDM (chapter 3.4).

PERMISSION	WHAT FOR	PRE-APPROVE VIA MDM
Microphone	Dictation. macOS asks on the first dictation.	NOT POSSIBLE
Accessibility	Keyboard shortcuts such as the Fn key, and inserting the text into the active program.	POSSIBLE
Automation ("System Events")	Determining the active program and inserting the text. macOS may ask once whether Diktiro may control "System Events".	POSSIBLE
Screen Recording	Only for the Notetaker, to capture the sound of a meeting (macOS 13 or later). Not needed for dictation.	NOT POSSIBLE
Input Monitoring	Not needed.	—

6.3 Where Diktiro stores data

PLATFORM	FOLDER
Windows	`%APPDATA%\@diktiroai\desktop`: settings, local history, logs `%LOCALAPPDATA%\@diktiroaidesktop-updater`: downloaded updates

PLATFORM	FOLDER
macOS	`~/Library/Application Support/@diktiroai/desktop`: settings, local history, logs `~/Library/Caches/@diktiroaidesktop-updater`: downloaded updates

- The sign-in is stored encrypted: on Windows with the Windows Data Protection API (DPAPI), on the Mac in the keychain.
- In operation, the app writes nothing outside the user profile. On Windows, it only registers the `diktiro://` link and, if enabled, the auto-start under `HKEY_CURRENT_USER`.

7 Connecting Microsoft Entra ID OPTIONAL

Microsoft Entra ID (formerly Azure AD) connects two things: **sign-in with Microsoft** (staff sign in with their work account) and **automatic provisioning** (SCIM: Entra creates people in Diktiro and removes them again). Today this takes two enterprise applications in your Entra. This chapter explains why, and in which order to proceed.

7.1 Two enterprise applications: why?

For applications from the Microsoft Entra gallery, a single enterprise application is usually enough. Diktiro is not listed there yet, so today there are two, with separate jobs:

APPLICATION	HOW IT IS CREATED	WHAT IT DOES
Diktiro AI Application ID 7ed52d24-…	Microsoft creates it by itself as soon as someone in your organisation consents to sign-in with Microsoft (chapter 7.2).	Only **sign-in**: Microsoft confirms to Diktiro who is signing in. This application creates nobody in Diktiro.
Your provisioning app Name of your choice	You create it yourself, as your own non-gallery application (chapter 7.3).	Only **provisioning**: Entra sends the assigned people to Diktiro (`https://api.diktiro.ai/scim/v2`) and reports when someone has left.

The assistant in the portal suggests the name "Diktiro AI" for the provisioning app. Both applications then carry the same name. You tell them apart by the application ID: the sign-in app always has `7ed52d24-eec6-4794-a9e7-d530a993fa2f`, your provisioning app has its own. A distinct name such as "Diktiro AI Provisioning" makes it easier; the name has no technical effect.

Assign the same group to both applications

Create a group in Entra for everyone who should use Diktiro, and assign **the same group to both applications** (*Enterprise applications → application → Users and groups → Add user/group*):

- In the **provisioning app**, the group decides who is created in Diktiro.
- In **Diktiro AI**, the group takes effect once you set "Assignment required?" to **Yes** under *Properties*. Then only members of the group can sign in to Diktiro with Microsoft. Others get an error from Microsoft instead of creating a private Diktiro account by mistake (see 7.5). Anyone who signs in to the portal with Microsoft must then be in the group as well.
- Entra only considers **direct members** of the assigned group. Members of nested subgroups are not provisioned.

> **In preparation**
>
> One single Diktiro entry in Entra (via the Microsoft Entra app gallery) is in preparation. Until then, the two-application setup described here applies.

7.2 Sign in with Microsoft

The app and the portal offer the button **"Sign in with Microsoft"**. It works with work and school accounts from any Microsoft Entra tenant. You do not need to register anything: on the first consent, Microsoft creates the enterprise application "Diktiro AI" in your tenant.

ITEM	VALUE
Application	**Diktiro AI** (multi-tenant)
Application (client) ID	`7ed52d24-eec6-4794-a9e7-d530a993fa2f`
Requested permissions	`openid` , `profile` , `email` , `User.Read` : sign-in, name and e-mail address. No access to mail, files or calendars.

Administrator consent

The application is not yet listed by Microsoft as a verified publisher. If your tenant does not allow users to consent to apps themselves, staff will see "Need admin approval" on their first sign-in. An administrator then grants consent once for everyone, in one of these ways:

- **On their own first sign-in** with an administrator account: tick the box "Consent on behalf of your organization".
- **Via link**, with your tenant ID in place of `<ID>` (open in the browser):

  ```
  https://login.microsoftonline.com/<ID>/adminconsent?client_id=7ed52d24-eec6-4794-a9e7-d530a993fa2f
  ```

- **In the Microsoft Entra admin center**, after the first sign-in attempt: *Enterprise applications → Diktiro AI → Permissions → Grant admin consent*.

Anyone signed in with Microsoft does not need to maintain a separate Diktiro password. On Windows devices, the policy **"Restrict sign-in to Microsoft SSO"** (`SsoOnly`, see chapter 4) hides the other sign-in options in the app.

7.3 Setting up automatic provisioning (SCIM)

With SCIM, Microsoft Entra takes over user management. People you assign to the provisioning app appear in Diktiro. Anyone who loses the assignment or is disabled loses access. Diktiro registers your domains for it; you create the secret token yourself in the Diktiro portal. Diktiro changes nothing in your Entra.

What Diktiro sets up for you

- Your e-mail domain(s), for example `yourcompany.com`. Entra can only create people with a registered domain. Free-mail domains are excluded.
- Your Microsoft tenant ID (*Entra admin center → Overview → Tenant ID*). It permanently links your company to your tenant and cannot be changed afterwards.

What you do in the Diktiro portal

- In the portal under **Users**, click **"Connect Entra ID"**. A small window opens beside the portal with the steps below, the **tenant URL** `https://api.diktiro.ai/scim/v2` and the **secret token**, both ready to copy. When Entra tests the connection, the window shows "Connection tested ✓" and stays open; once Entra has provisioned the first person, it reports "Connected ✓" and closes.
- "*Create new token*" replaces the token; the old one stops working at once and must be replaced in Entra.

What you set up in Microsoft Entra

1. *Entra admin center → Enterprise applications → New application → Create your own application*, option "Integrate any other application you don't find in the gallery (Non-gallery)". Name for example "Diktiro AI Provisioning" (see 7.1).
2. In the new application: *Provisioning → Provisioning Mode* "*Automatic*". Enter the tenant URL and secret token, *Test Connection*, save.
3. *Mappings → Provision Microsoft Entra ID Users*: for the attribute `externalId`, choose **`objectId`** as the source. The default is `mailNickname`; please change it.
4. Please **disable** the mapping *Provision Microsoft Entra ID Groups*, unless agreed otherwise with Diktiro. This only concerns sending groups as entries of their own; provisioning people through an assigned group keeps working.
5. *Users and groups*: assign the same group as for "Diktiro AI" (see 7.1). Under *Provisioning → Settings*, keep the scope "Sync only assigned users and groups".
6. Test with *Provision on demand* and a single person (see 7.4). Then set *Provisioning Status* to **On** and save.

Tip: in the provisioning app, set "Visible to users?" to **No** under *Properties*. Otherwise assigned people see a second Diktiro tile in "My Apps" that they do not need.

7.4 Provisioning cycles and "Provision on demand"

Entra does not send people instantly but in **cycles**. The first cycle after switching on reads all assigned people and can take longer when there are many. After that, a cycle runs about **every 40 minutes** and sends only changes. Newly assigned or removed people therefore reach Diktiro with a delay of up to about 40 minutes.

Provision on demand (in the provisioning app under *Provisioning*) sends a single person at once, without waiting for the next cycle: select the person, click *Provision*. Entra then shows step by step what happened, including Diktiro's answer. This is useful for a first test and for troubleshooting. The person must be assigned, directly or as a direct member of the group.

7.5 What Diktiro does with every provisioned person

Diktiro takes every person Entra sends into your company. Three things must be right for that:

- The person's address (in Entra the user principal name, UPN) belongs to a domain Diktiro has registered for your company.
- `externalId` is mapped to `objectId` (7.3, step 3).
- A licence is free. With a fixed number of places, Diktiro refuses further people once all places are taken; with per-person billing, a maximum agreed with you applies.

Then the following happens:

- The person becomes a **Member** of your company and gets a licence of your company at once. In the portal they are listed under **Users** with the note "Managed in Entra". They do not need an invitation e-mail.
- With per-person billing, every newly provisioned person is charged pro rata on the next invoice.
- The person signs in to the app with **"Sign in with Microsoft"**. Password and Google sign-in are blocked for people from Entra. The only exception: your company's Admin (chapter 8.1) keeps a password as the emergency key.

> **Provision first, then sign in**
>
> If someone signs in to Diktiro with Microsoft **before** Entra has provisioned them, Diktiro does **not** assign them to your company. They get a private Diktiro account of their own, without your company's licence, and do not appear in your portal. To Diktiro they look like a private individual sign-up.
>
> When Entra provisions the person later, Diktiro finds the existing account by its e-mail address and takes it into your company. From then on your licence applies, and no second account is created. This only works if the address Entra sends (UPN) is the same one Microsoft reports at sign-in (the person's e-mail address). If the two differ, two Diktiro accounts are created and sign-in with Microsoft fails. Diktiro support will help in that case.
>
> **The right order:** 1. Assign the group to both applications. 2. Wait for provisioning, or use "Provision on demand". 3. Check that the person is listed in the portal under **Users**. 4. Only then "Sign in with Microsoft" in the app.

7.6 Removing people

- Remove the person from the group, remove the assignment, or disable or delete the user account in Entra. Entra reports this to Diktiro in the next cycle.
- Diktiro then deactivates the membership and signs the person out on all devices at once. Their **licence becomes free**; their existing data is kept. Places already paid for are not refunded but stay free for others until the end of the billing period.
- If the person is assigned again, Diktiro reactivates them, provided a licence is free.
- People from Entra are removed and restored only in Entra, not in the portal.

7.7 Troubleshooting

WHAT YOU SEE	CAUSE AND FIX
A person does not arrive	Check the *Provisioning logs* of the provisioning app, or run *Provision on demand* for this person. Both show Diktiro's answer. Common causes: • No cycle has run yet: wait up to about 40 minutes, or use "Provision on demand". • The person is out of scope: Provisioning Status "On", scope "Sync only assigned users and groups", person a direct member of the assigned group. • "Email domain is not verified for this organization": the domain of their address is not registered with Diktiro. Tell Diktiro support the domain. • "Map Entra objectId to SCIM externalId and configure the tenant ID": switch `externalId` to `objectId` (7.3, step 3). • "Seat limit reached" or "Licence maximum for Entra provisioning reached": all licences are taken. Contact us for more places. • Error 401 (unauthorized): the token was replaced in the portal. Enter the new token in Entra. After many errors, Entra puts provisioning into quarantine. After the fix, restart provisioning.
A person appears twice or outside your company	Usually they signed in before provisioning and use a private account (7.5). Anyone who can sign in but is missing in the portal under **Users** has not been provisioned yet: run "Provision on demand". If the person's UPN and e-mail address differ, or two accounts already exist, contact Diktiro support.
"Need admin approval" at sign-in	Administrator consent is missing (7.2).
Microsoft says the person is not assigned to the application	"Assignment required?" is set to Yes on "Diktiro AI", and the person is not in the group (7.1).
The app does not connect or shows certificate warnings	Provisioning runs directly between Microsoft and Diktiro; your firewall is not involved. The app on the devices, however, needs `api.diktiro.ai` on port 443 (HTTPS, see 5.1). If your firewall inspects encrypted connections (TLS inspection), exempt `*.diktiro.ai` from it (see 5.3).

The tenant URL and the token are always shown in the portal under **Users** → **"Connect Entra ID"**.

8 Inviting users and licences

You manage users, licences and invoices in the **Diktiro portal** in the browser; Diktiro sends the link to your Admin. The app itself is only for dictating.

8.1 Roles

ROLE	MAY
Admin	Everything a Manager may, plus the invoice-copy address and accepting an IT partner. Cannot be removed or changed in the portal.
Manager	Invites, removes and restores people, switches them between Member and Manager, and sees usage, billing and the sign-in settings.
Member	Uses Diktiro in the app; no access to the portal.

8.2 Inviting people

1. In the portal, open **Users** → **Invite user**.
2. Enter first name, last name, e-mail address and role (Member or Manager) and choose **Invite**. If your company has its own domain, you type only the part before the @.
3. The person receives an e-mail in German, **"Einladung zu <your company> auf Diktiro"** (invitation to <your company> on Diktiro), with the button **"Einladung annehmen"** (accept invitation).
4. Company, e-mail address and role are fixed in the form. The person sets a password (at least 8 characters) or uses Microsoft or Google with the same address. Existing Diktiro users sign in and join.
5. The person then opens the Diktiro app and signs in with exactly this account.

Good to know

- **Company addresses only:** if Diktiro registered domains for your company (see chapter 7) or the Admin's address is not from a public provider such as gmail.com or gmx.de, invitations go only to those domains.
- The link is valid for **7 days**. Under *Users*, switch the list from *Active* to *Invited*: each invitation's ⋯ menu has **Send again** (7 days again) and **Withdraw invitation**.
- An invitation takes up a licence only once it has been accepted; open invitations cost nothing.
- With automatic provisioning via Microsoft Entra (chapter 7.3), no invitations are needed.
- The invitation e-mail contains no download link. If the app was not distributed centrally, give your staff the download link from chapter 1.

8.3 Removing people

Under **Users**, the bin on a person's row removes them: they lose access at once, their records are kept, and under *Deactivated* you can **restore** them later. Their licence is free for someone else at once; paid periods are not refunded. People from Microsoft Entra are removed in Entra.

8.4 Licences and invoices

- Under **Billing**, a company without a valid licence chooses **Add payment**: **Monthly**, **Yearly** or **Every 2 years**, and pays in Stripe for as many licences as there are active people (for example by credit card). Afterwards, changes and cancellation go through **Manage billing**, and each invoice has **Open** and **PDF**.
- A person added later first takes a licence already paid for this period (for example one freed by a removal); otherwise one more licence is added when the person accepts, charged pro rata on the next invoice.
- With a fixed number of places (purchase on invoice), nobody else can join once all places are taken; contact us for more. Invoices then come directly from Diktiro.
- **Copy of every invoice to**: with card payment, the Admin enters, for example, your accounting department; Diktiro sends a copy of every new invoice there.
- Under **Usage**, choose 7, 30 or 90 days or *All time* and see each person's word count (dictation and Notetaker), last use and *Inactive for 30 days*, plus a daily chart and **Export CSV**. Dictated text is never shown.

9 Data protection and security

The key technical facts for your data-protection and security review. The data processing agreement (DPA, German "AVV") is available at `diktiro.ai/avv`.

9.1 How Diktiro handles audio

Diktiro records only while a person is dictating and never stores audio on its servers. On the device, the app keeps an encrypted safety copy of each recording until the text has arrived, so that no dictation is lost if the connection drops.

1. **Safety copy.** When the person stops dictating, the app saves the recording in an encrypted database on the device (`recoverable.db` in the app data folder, chapter 6.3). The key is protected by the operating system: the Windows Data Protection API (DPAPI) or the macOS keychain.
2. **Recognition.** The app sends the recording over HTTPS to `api.diktiro.ai`, which passes it to Microsoft Azure AI Speech (West Europe). The Diktiro server writes no audio to disk or to a database, and Azure's optional audio logging is not switched on. The server keeps only technical records, such as a checksum of the recording and the word count for billing.
3. **Deletion.** As soon as the text has been inserted and saved, the app deletes the safety copy.

The copy stays on the device only if a dictation **fails** (for example without a connection) or is **cancelled**. The person can then send it again from the app:

- It can be sent again for **7 days**. After that it is only listed as expired and is deleted **after 14 days at the latest** (if the app is not running that day, at its next start).
- At most the **50 most recent** recordings are kept; older ones are deleted.
- The person can delete any recording at any time. Only the same user account on that computer can decrypt them, and they are erased when the Diktiro account is deleted.

With **on-device transcription** (optional for Pro accounts), speech is recognised on the device: the recording is not sent to Diktiro, only its word count. The **Notetaker** (meeting notes) keeps no audio: the meeting is recognised in the same way and only the text is saved.

9.2 Where the other data goes

DATA	WHAT HAPPENS
Recognised text	Optionally polished linguistically and inserted into the active program. The history is stored in the Diktiro account by default; on Windows, a policy can keep it on the device only (chapter 4).
Usage in the portal	Admins and IT partners see only the number of words and the time of last use, never the content of a dictation.
Technical diagnostics	At start-up the app sends technical information to Diktiro, for example version, operating system and the state of microphone, keyboard shortcut and proxy. No audio, no text.
Third parties	The app itself contains no third-party analytics, advertising or crash-reporting services and connects only to the destinations in chapter 5.

9.3 Server locations

SERVICE	LOCATION
Diktiro service (`api.diktiro.ai`)	Microsoft Azure, Germany West Central (Frankfurt am Main)
Speech recognition	Microsoft Azure AI Speech, region West Europe (Netherlands)
Text polishing and meeting summaries	Microsoft Azure OpenAI, EU data zone (resource in France Central, Paris)
Account and history data (database)	MongoDB Atlas on Microsoft Azure, region West Europe (Netherlands)
Updates and installers (`releases.diktiro.ai`)	Microsoft Azure Storage, region West Europe (Netherlands), delivered via Azure Front Door