REMOTLY · INTEGRATION GUIDE

Remotly — Microsoft Entra ID Integration

A step-by-step guide: connecting Remotly to your Microsoft organization, deploying the Remotly QuickHost agent (manually or through Microsoft Intune), and managing device access.

Table of contents

After completing the steps described in this document:

- user accounts from your Microsoft organization will be imported into Remotly together with licenses,
- the **Remotly QuickHost** agent will be installed on the selected computers,
- support staff will be able to connect remotely to devices according to the permissions defined by security groups and administrative units in Entra ID.

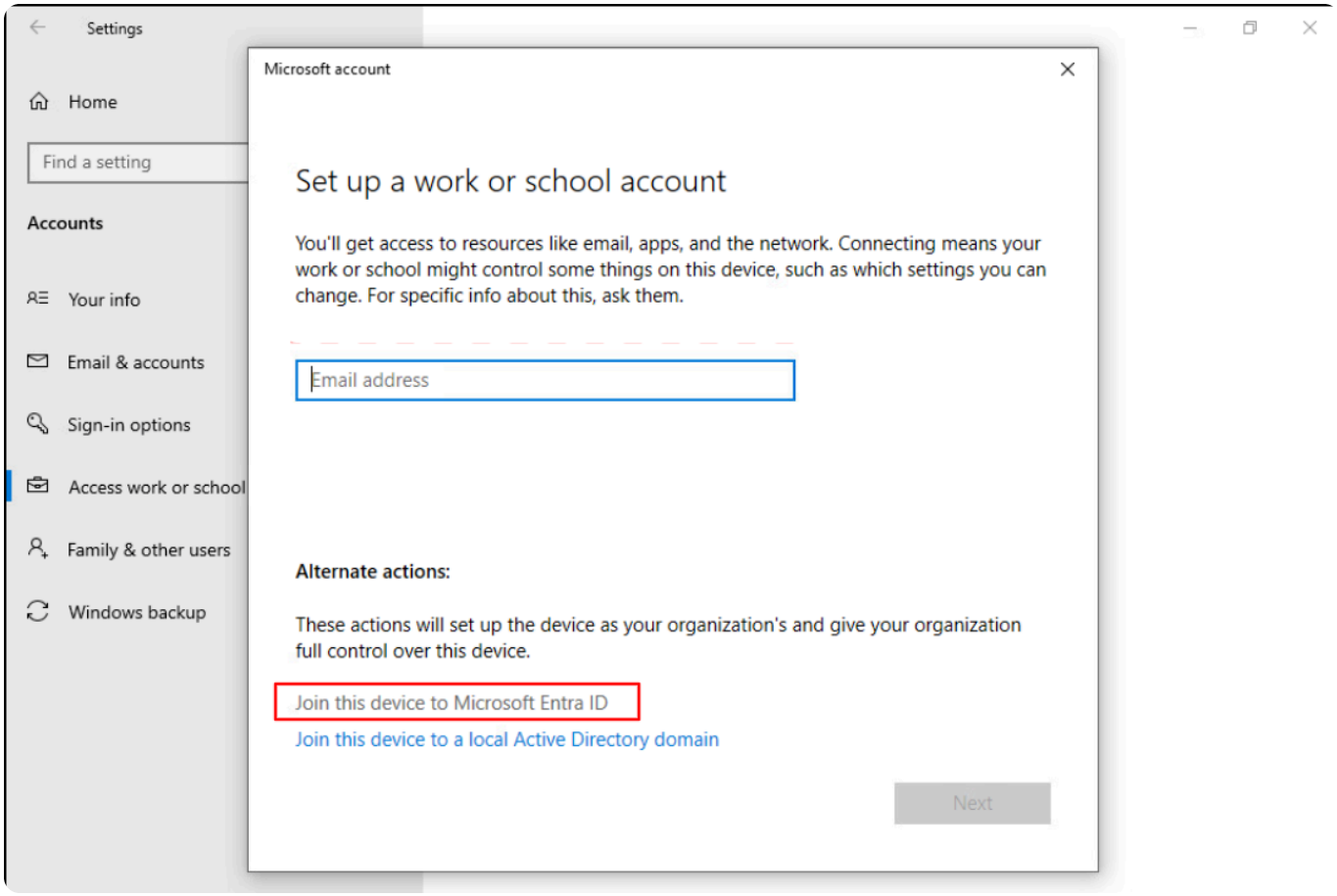
Prerequisites

Before you start the integration, make sure that:

- you have access to your Microsoft organization's **administrator account** (with permission to grant *admin consent*),
- you have access to the **Microsoft Intune** portal (intune.microsoft.com) — required only for automatic deployment,
- the computers on which the Remotly QuickHost agent will be installed are **joined to Entra ID (Entra Joined)** and users are signed in with their **work accounts**.

> ⚠️ **IMPORTANT:** Joining devices to Entra ID is a hard requirement. The QuickHost agent reads the *device ID*, which is available only on Entra Joined devices.

A device can be joined to Entra ID in Windows settings: **Settings → Accounts → Access work or school → Connect → Join this device to Microsoft Entra ID**.



Joining a device to Microsoft Entra ID in Windows settings

You can verify the join status by running the following command in the command prompt:

```
dsregcmd /status
```

In the *Device State* section, the `AzureAdJoined` value should be `YES`.

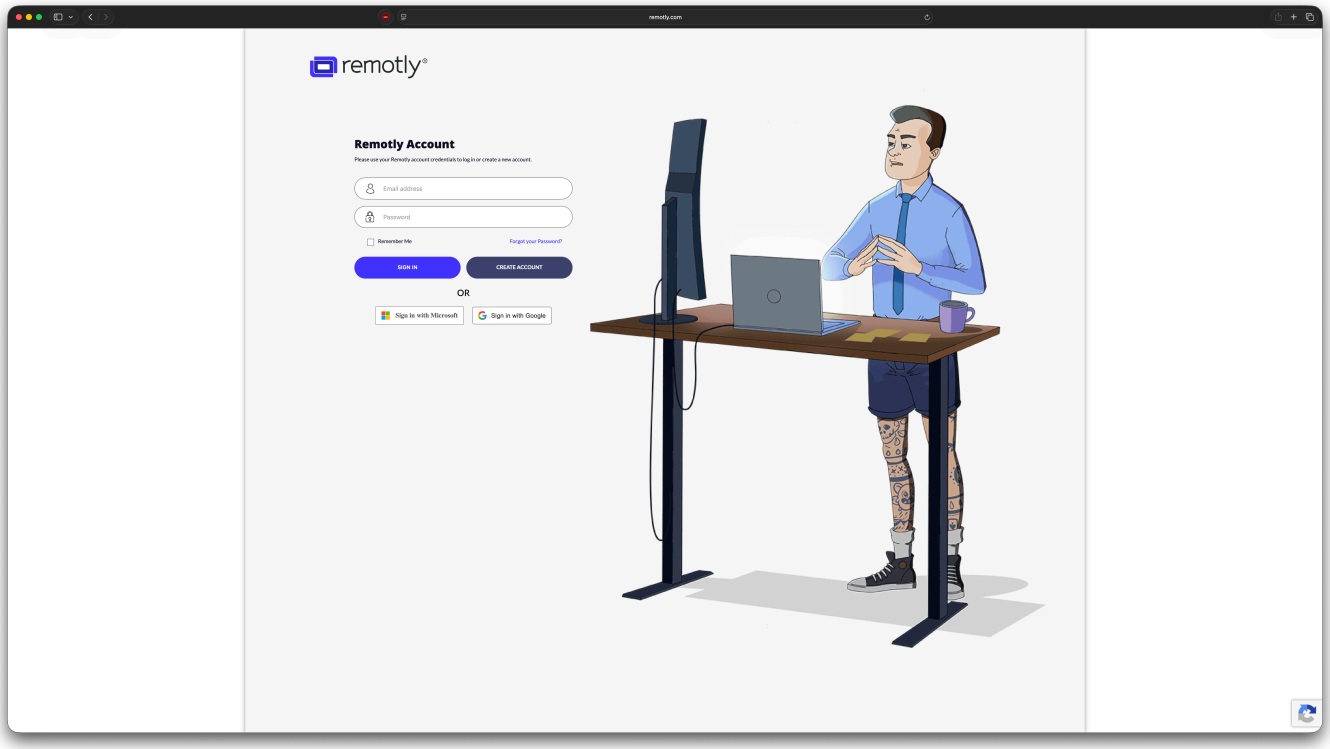
PART 1

Remotly administrator panel

The Remotly administrator panel is the starting point of the whole integration. It involves three steps: signing in, integrating with Entra ID, and preparing the QuickHost installer.

1 Administrator sign-in with a Microsoft account

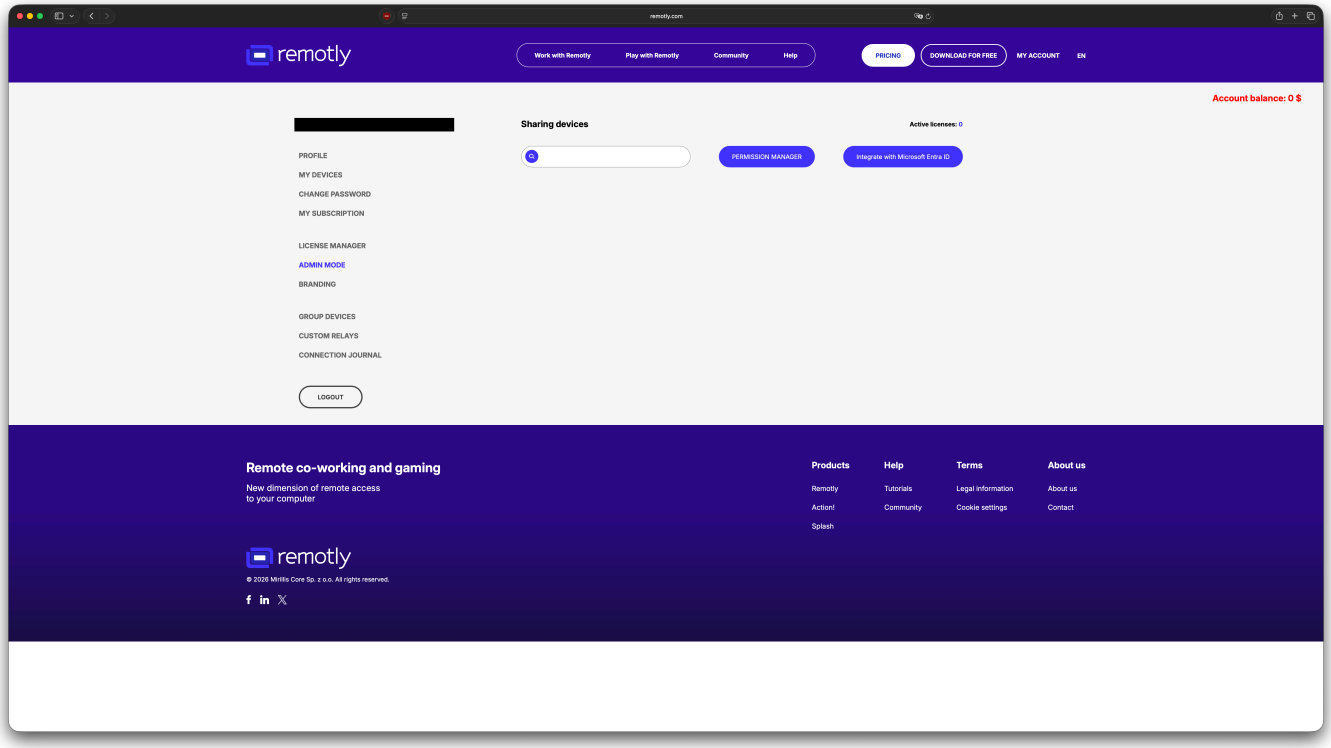
On the Remotly sign-in page, choose **Sign in with a Microsoft account** and sign in with your organization's administrator account.



Remotly sign-in screen — signing in with a Microsoft account

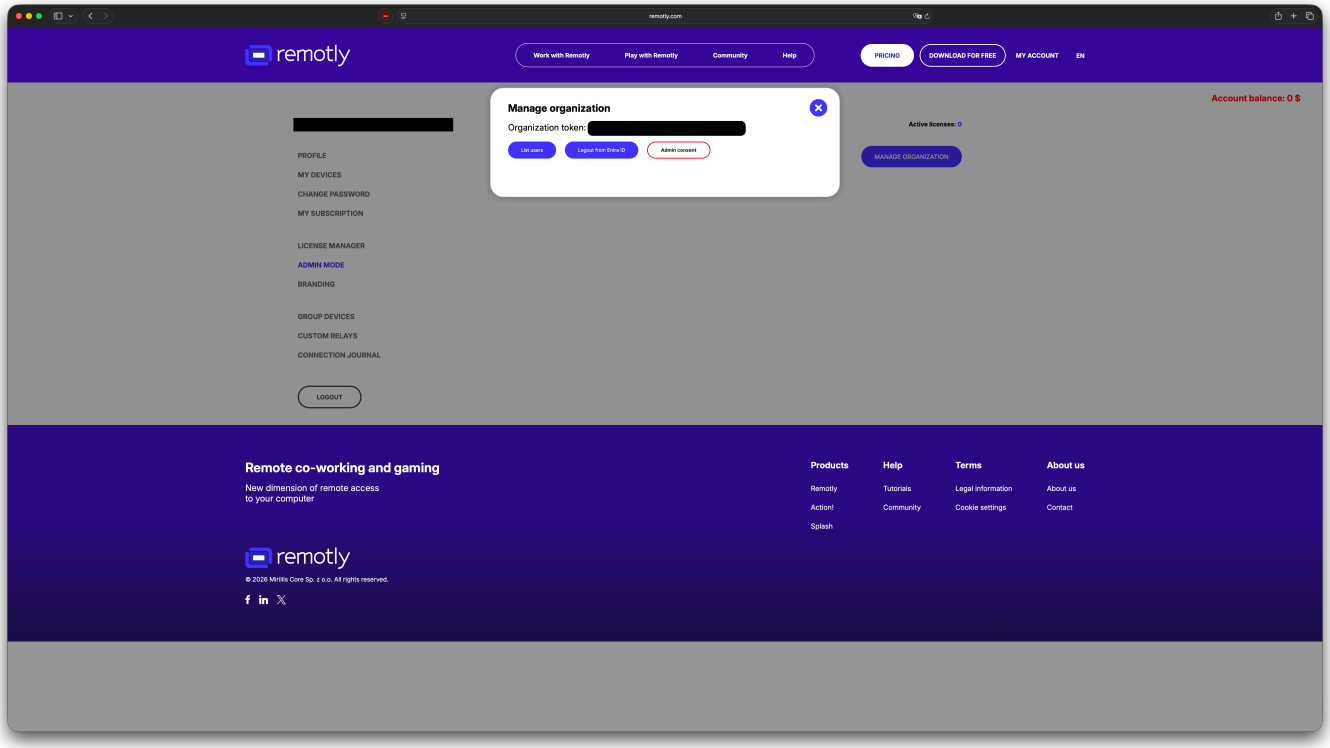
2 Entra ID integration

Go to the **Administrator Mode** tab and click the **Microsoft Entra ID integration** button, then grant *admin consent* in the Microsoft window.



Administrator Mode tab with the "Microsoft Entra ID integration" button

Once consent has been granted, the button changes to **Manage organization**. Clicking it opens a window showing your **unique organization token** — you will need it in the QuickHost installation command.



The "Manage organization" window with the organization token

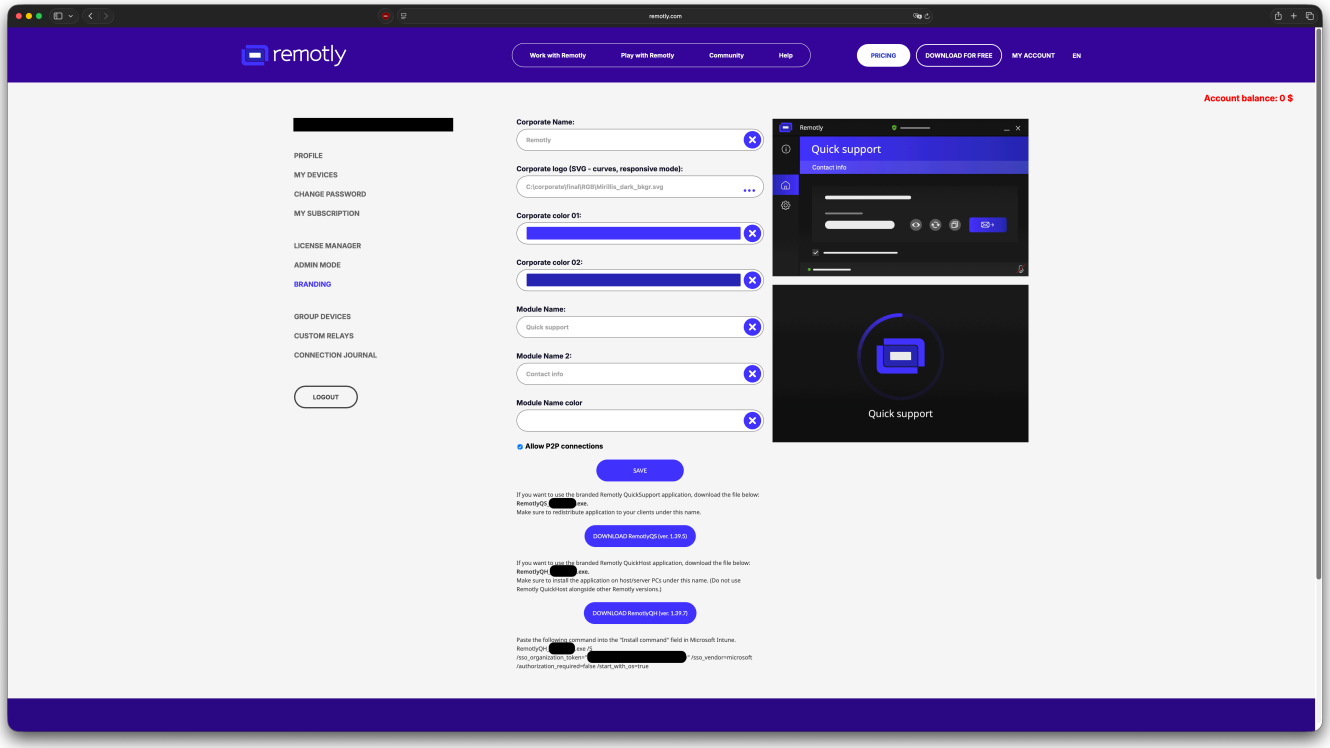
Clicking **User list** loads the *security groups* from your organization. Expanding a group intended for import loads the list of its members — individual users can be selected and deselected one by one.

After clicking **Save**, the selected users are imported into Remotly and **automatically receive licenses**.

> ⚠️ **IMPORTANT:** Import the accounts of users who **will be connecting** to remote devices (e.g. support staff). Do not import the accounts that are signed in on the devices where the QuickHost agent will be installed.

3 Customizing and downloading the QuickHost installer

In the **Branding** tab you can customize the look of the Remotly QuickHost agent (company colors, module names) and then download a personalized installer using the **DOWNLOAD RemotlyQH** button.



Branding tab — customizing and downloading the RemotlyQH installer

Below the download button you will find a ready-made **installation command** pre-filled with your organization's identifiers. Using it is required so that, after installation, the QuickHost agent correctly registers with the Remotly server and stores the *connection string* in the device data in Microsoft Intune. The same command is used both for manual installation and for Intune deployment (described in Part 2).

Example command (your panel shows the actual values for your organization):

```
RemotlyQH_<id>.exe /S /sso_organization_token="<your_organization_token>" /sso_ven
dor=microsoft /authorization_required=false /start_with_os=true
```

Parameter	Description
`/S`	Silent installation (no dialog windows)
`sso_organization_token`	Unique organization token (from the **Manage organization** window)
`sso_vendor`	Integration provider (`microsoft`)
`authorization_required`	Whether the connection requires authorization on the host side (`false` = not required)
`start_with_os`	Start the agent automatically with the operating system

PART 2

Installing the Remotly QuickHost agent

The QuickHost agent can be installed in two ways: **manually** on individual computers, or **automatically** on many devices through Microsoft Intune.

Option A — Manual installation (command prompt)

1. Download the Remotly QuickHost installer (Part 1, Step 3) onto the target computer.
2. Run the **command prompt as administrator**.
3. Go to the directory containing the downloaded file and run the installation command from Step 3.

> ⚠️ **IMPORTANT:** The command prompt must be running with administrator privileges.

Option B — Automatic deployment (Microsoft Intune)

Preparing the .intunewin package

Intune requires the application to be delivered in the `.intunewin` format. The package is prepared with the **Microsoft Win32 Content Prep Tool** (download version 1.8.7).

> ⚠️ **IMPORTANT:** Before you start, create a **new, empty folder** and place only the RemotlyQH installer file in it. The tool packages the entire specified directory — skipping this step could result in packaging, for example, the whole contents of your Downloads folder.

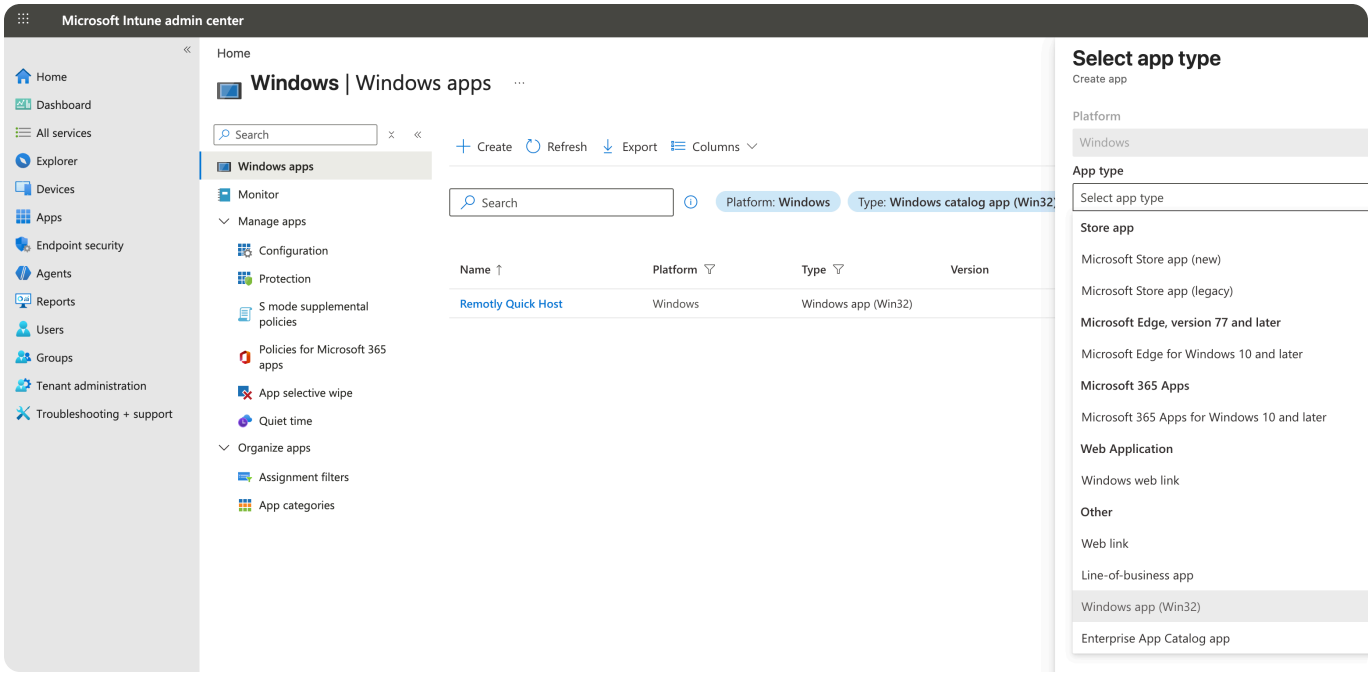
1. Download and unpack the archive with the tool.
2. Run the `IntuneWinAppUtil.exe` executable — a terminal window will open.
3. Answer the tool's questions in order:
   - **Source folder** — path to the directory containing the RemotlyQH file,
   - **Setup file** — path to the RemotlyQH installer file,
   - **Output folder** — path where the `.intunewin` package should be created,

- **Do you want to specify catalog folder** — `N` (no).

The resulting `.intunewin` file is ready to be uploaded to Intune.

Creating the app in Intune

In the Intune portal (intune.microsoft.com) go to: **Apps → Windows → Create** and select **Windows app (Win32)** as the app type.



Creating an app in Intune — selecting the "Windows app (Win32)" type

The wizard will guide you through the configuration tabs:

1 App information

Select the prepared `.intunewin` file and fill in the basic information about the app (name, description, publisher). It is worth filling in the **App Version** field — it makes managing future updates easier.

App information | Program | Requirements | Detection rules | Review + save

Select file to update *

Name * Remotly Quick Host

Description *

Get help with markdown supported for descriptions.

Remotly Quick Host agent for remote desktop access

Preview

Remotly Quick Host agent for remote desktop access

Publisher * Mirillis Ltd.

App Version Enter the app version

Category 0 selected

Show this as a featured app Yes No

Information URL Enter a valid url

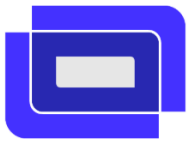
Privacy URL Enter a valid url

Developer

Owner

Notes

Logo Change image



App information tab

2 Program

The most important tab. Set:

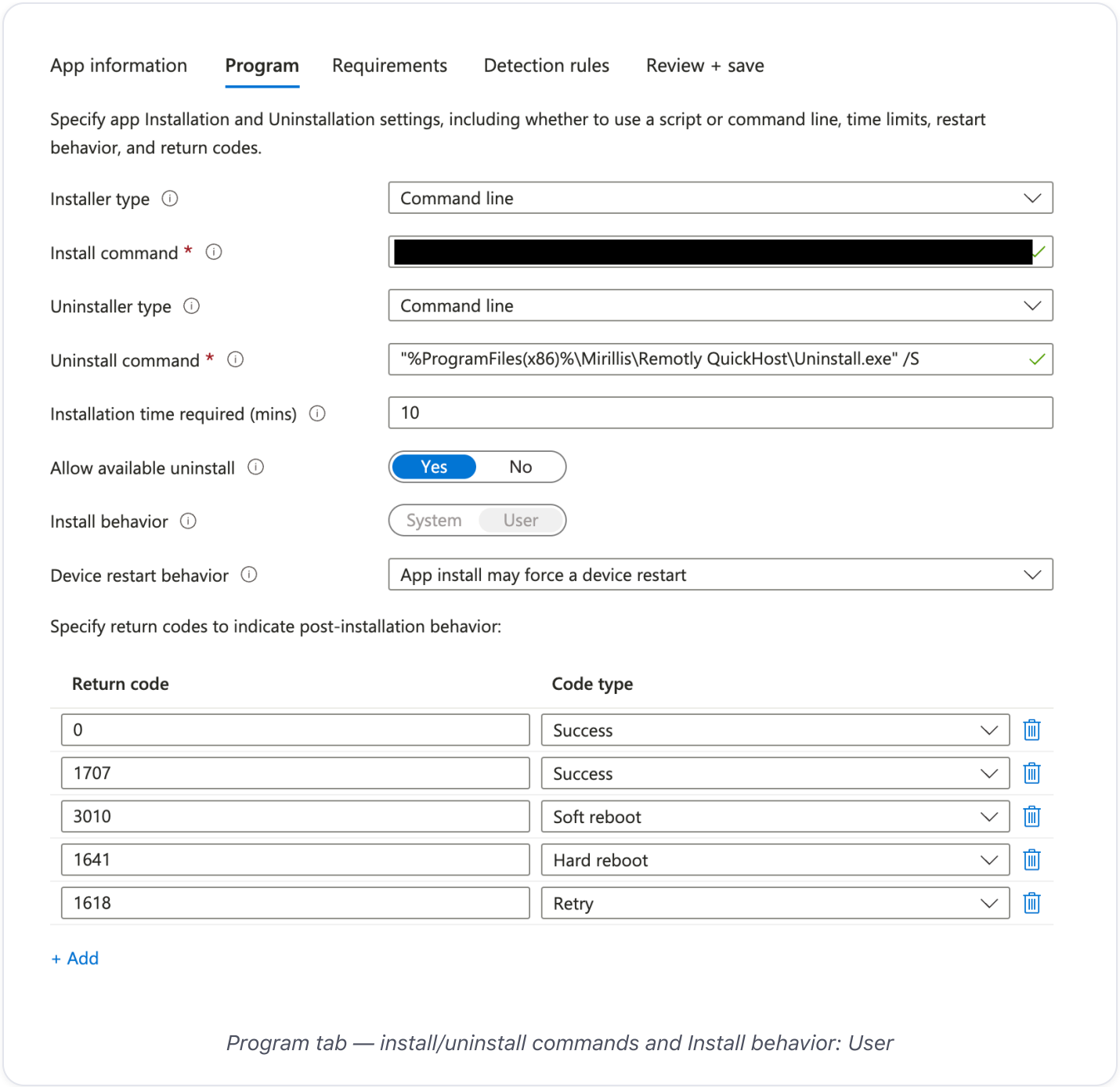
- **Installer type:** `Command line`

- **Install command:** the installation command from Part 1, Step 3 (with your organization token)
- **Uninstaller type:** `Command line`
- **Uninstall command:**

```
"%ProgramFiles(x86)%\Mirillis\Remotly QuickHost\Uninstall.exe" /S
```

- **Install behavior:** `User`

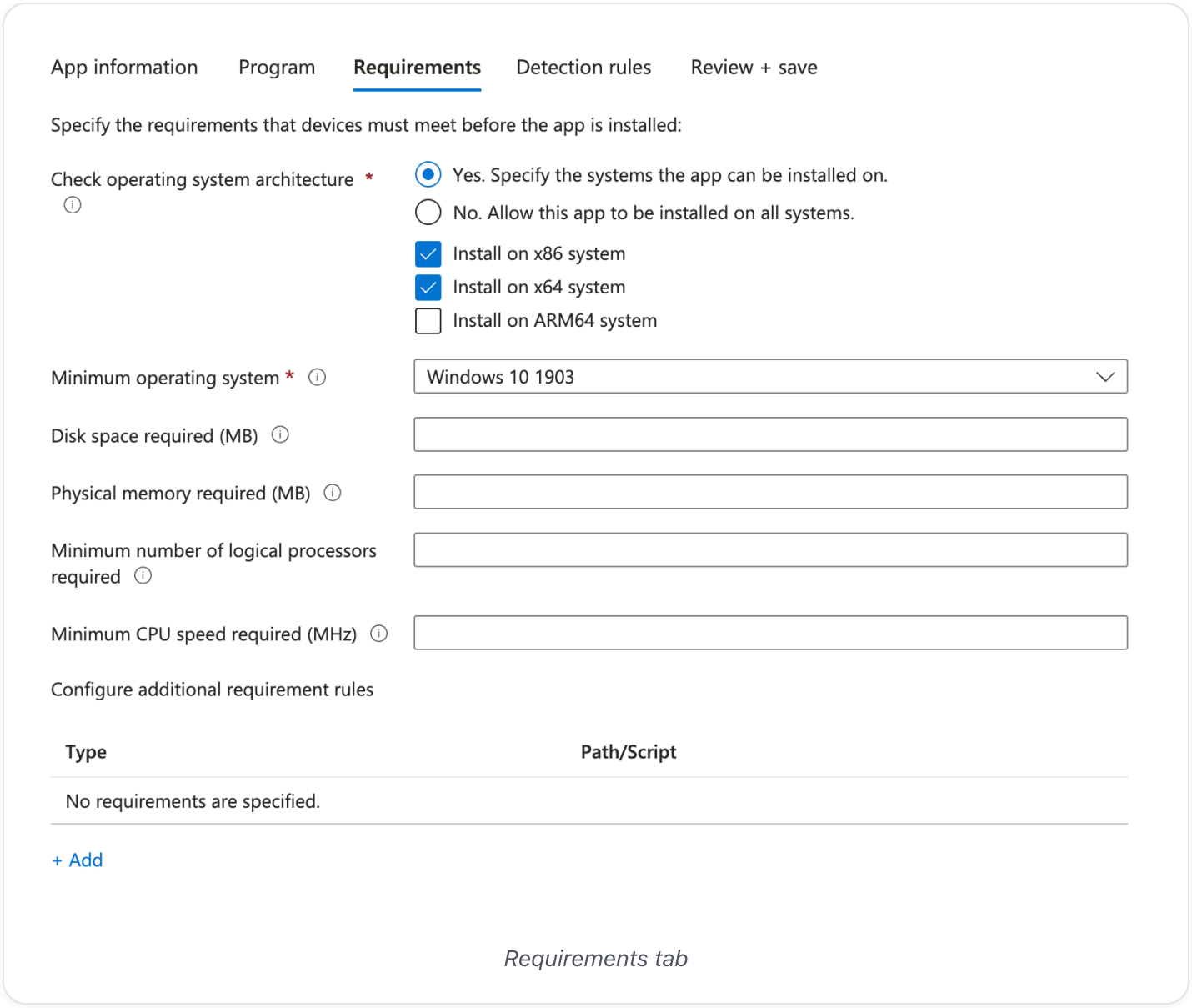
> ⚠️ **IMPORTANT:** The application must be installed in user mode (**Install behavior: User**). With a system-mode installation, the installer will hang the first time the graphical interface starts.



Program tab — install/uninstall commands and Install behavior: User

3 Requirements

- **Architecture:** `x86` and `x64`
- **Minimum operating system:** `Windows 10 1903` (the version required by the virtual display driver)



Requirements tab

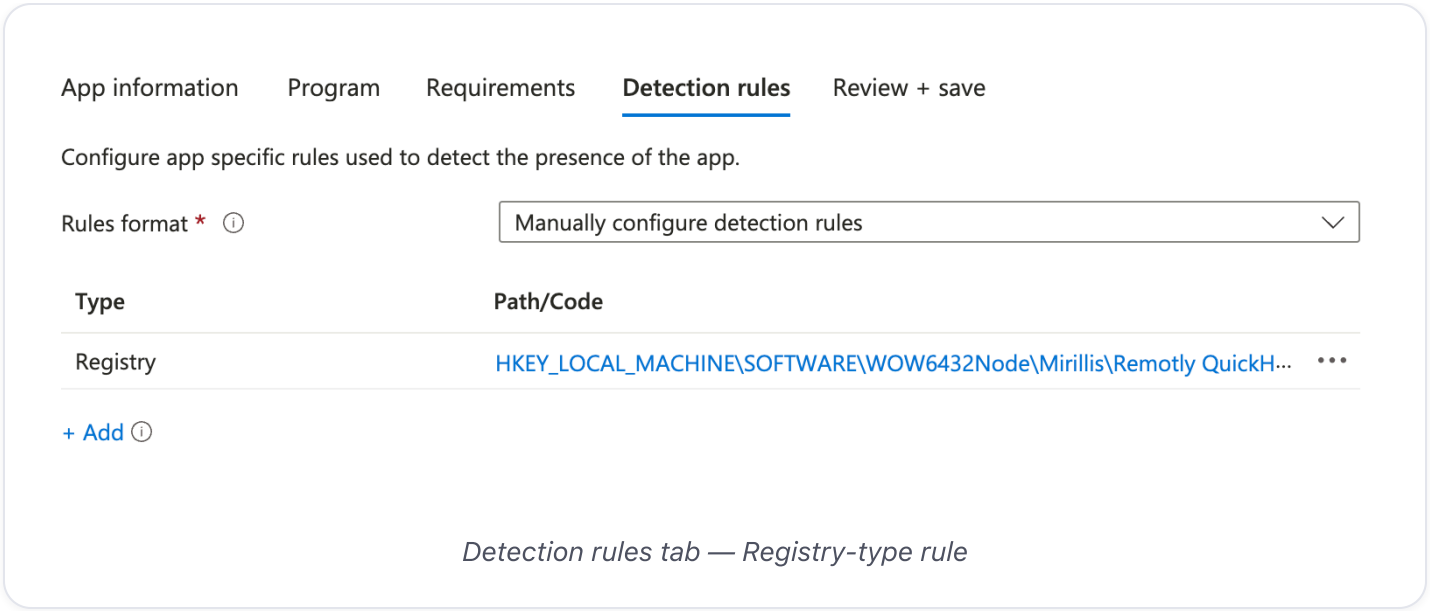
4 Detection rules

Choose **Manually configure detection rules** and add a rule of type **Registry**:

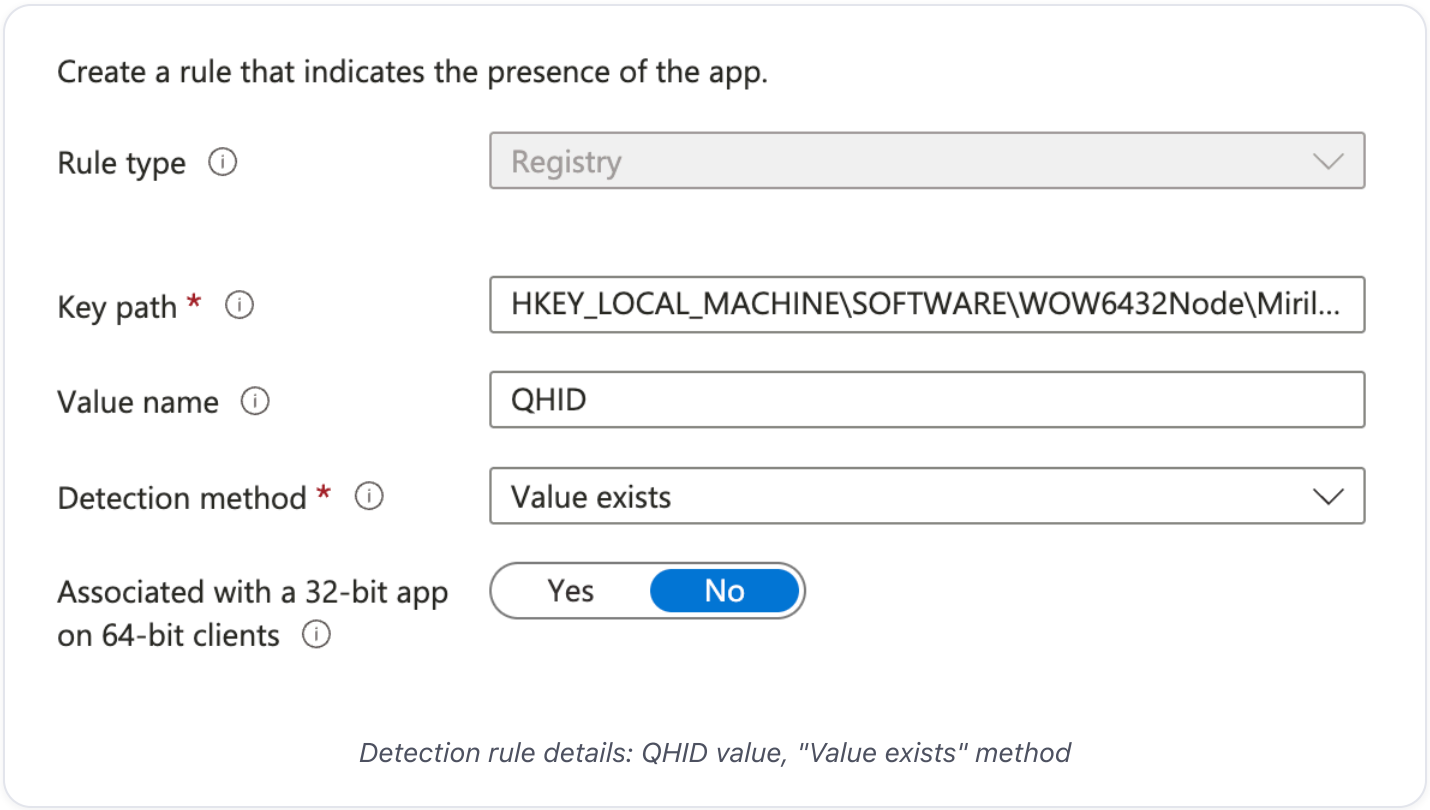
- **Key path:**

```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mirillis\Remotly QuickHost
```

- **Value name:** `QHID`
- **Detection method:** `Value exists`



Detection rules tab — Registry-type rule



Detection rule details: QHID value, "Value exists" method

5 + 6 Dependencies and Supersedence

Leave the default settings.

7 Assignments

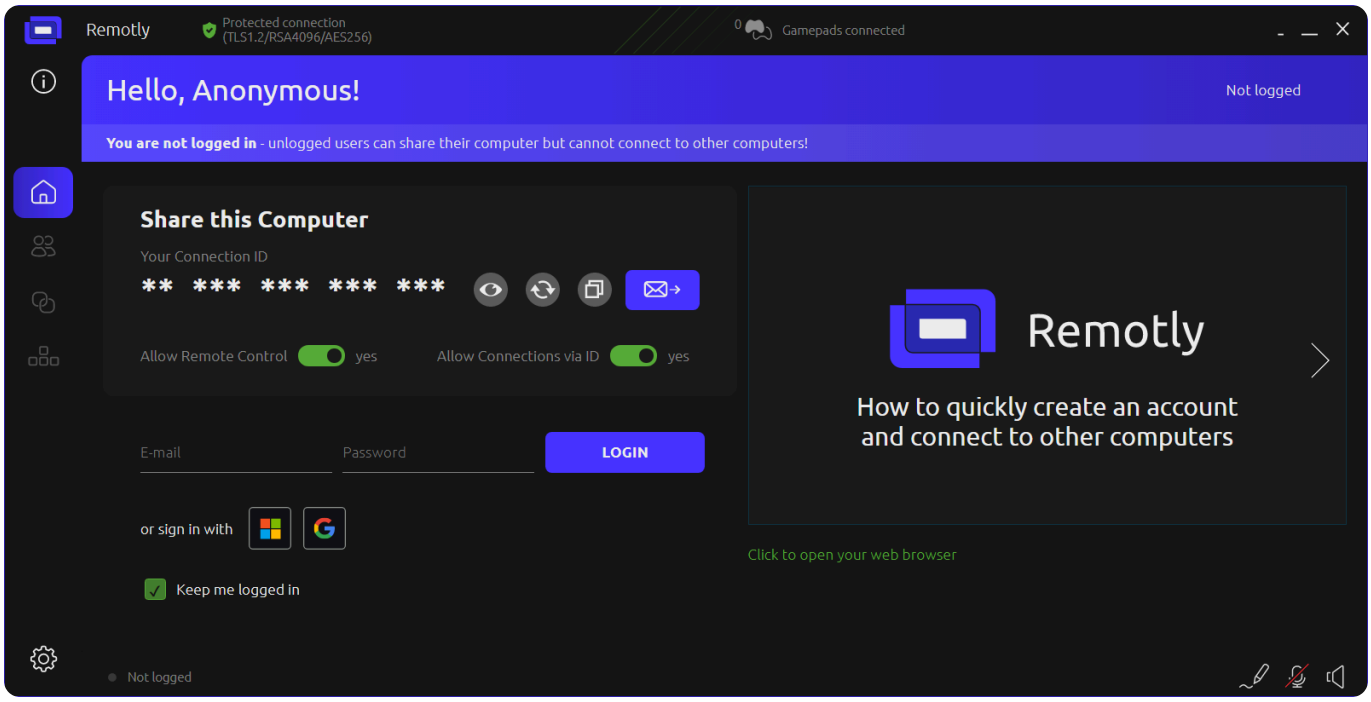
Select the devices (or device groups) the app should be assigned to.

Finally, review the configuration in the **Review + create** tab and save the app. The Remotly QuickHost agent will be installed automatically on the selected devices.

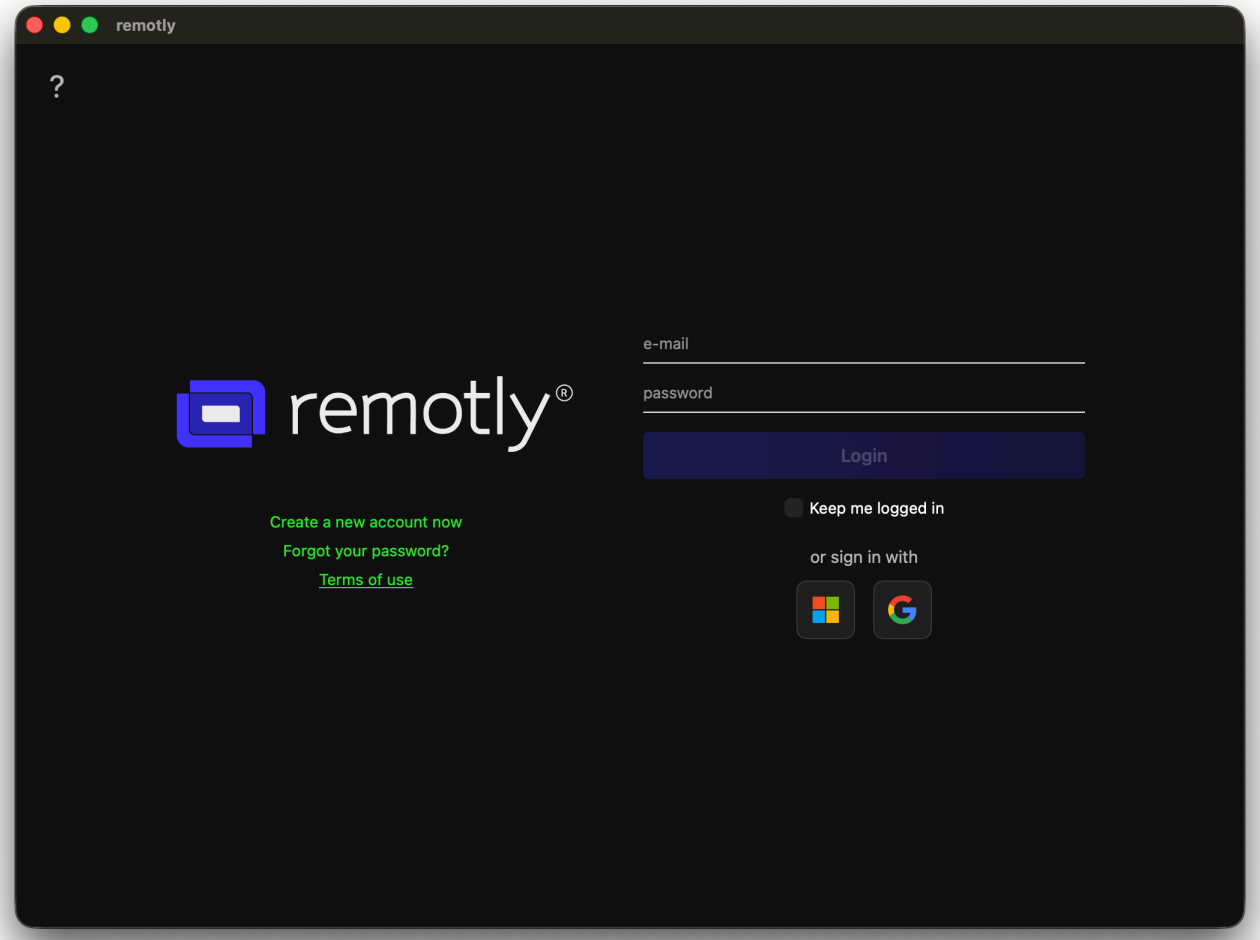
> **Reminder:** The devices are assumed to be already joined to Entra ID (see Prerequisites). The QuickHost agent reads the device ID, which is available only on Entra Joined devices.

Installing the Remotly client (support workstation)

The Remotly client — used by support staff to connect to remote devices — is downloaded and installed in the standard way (it can also be deployed automatically through Intune). After installation, the support employee signs in to the application with their **Microsoft account**.



Remotly client on Windows — signing in with a Microsoft account



Remotly client on macOS — signing in with a Microsoft account

After signing in, the device list shows all machines the user has access to (according to the rules described in Part 3). A correct QuickHost installation can additionally be verified in the Intune portal — the Remotly QuickHost app details show the installation status on individual devices.

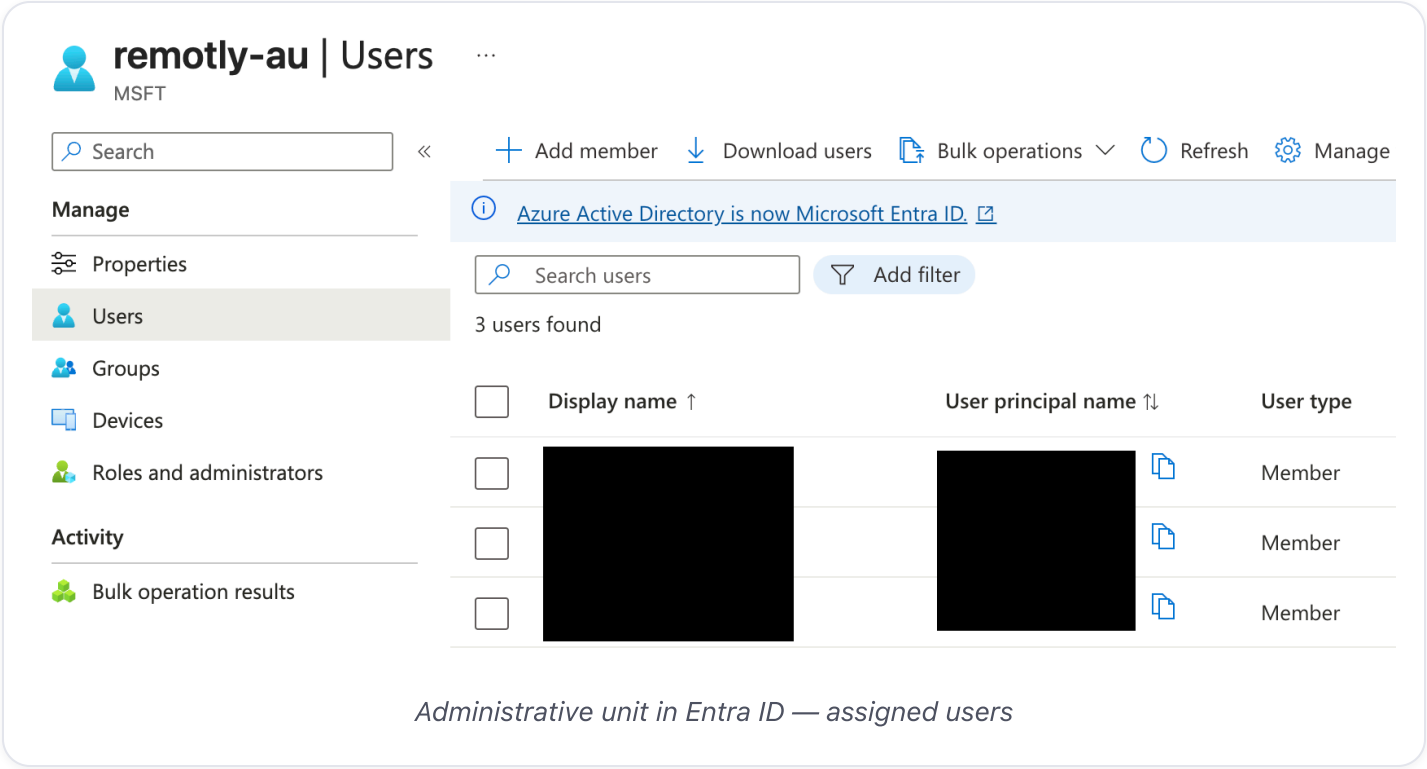
PART 3

Managing device access

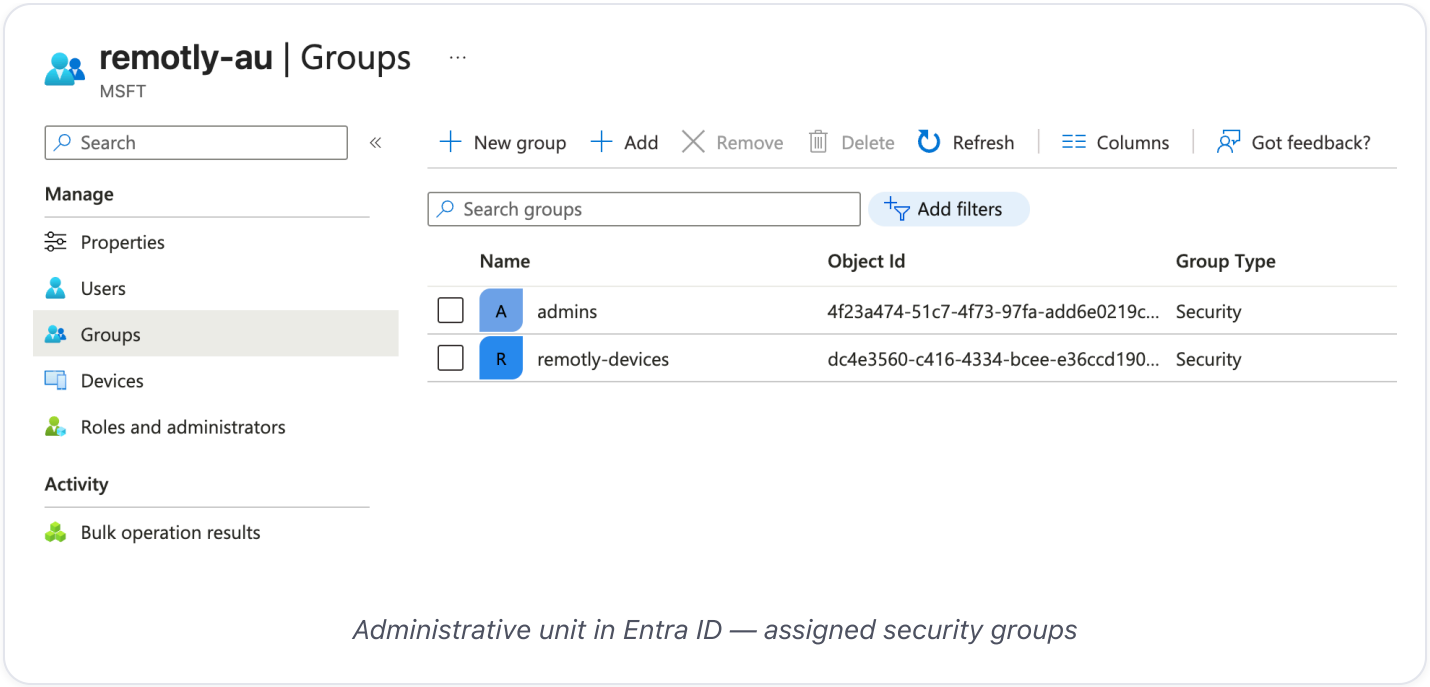
Device access is managed on the Microsoft Entra ID side using *security groups* and *administrative units*.

Remotly considers a user to have access to a device (i.e. to be able to establish a connection with it) when **any** of the following conditions is met:

1. The user's work account is **signed in on that machine** (Entra Joined device).
2. The user and the device belong to **the same security group**.
3. The user and the device belong directly to **the same administrative unit** (*Administrative Unit*).
4. The user and the device belong to **different security groups that are assigned to the same administrative unit**.



Administrative unit in Entra ID — assigned users



Administrative unit in Entra ID — assigned security groups