CONNECT YOUR SOLUTION

# Microsoft 365 and Azure

Connect your Microsoft Entra ID tenant to REVIEWIT, for Microsoft 365 as for Azure: a dedicated app registration, read-only application permissions, a secret or a certificate.

VERSION
1.0 · November 2026

DURATION
Forty-five minutes, in four steps

DISTRIBUTION
Confidential · REVIEWIT customers

## WHAT YOU NEED

01 **A Global Administrator or Cloud Application Administrator** of the Entra ID tenant, able to create an app registration and **grant admin consent**; for Azure, an **Owner** of the subscriptions to review.

02 **A REVIEWIT account** with the subscription administrator role, to open the Subscription Manager.

03 **The time stated**, in the order of this guide: first the credential at Microsoft 365 and Azure, then the REVIEWIT wizard, in four steps.

THE WIZARD, IN FOUR STEPS

| STEP 1 | STEP 2 | STEP 3 | STEP 4 |
|---|---|---|---|
| **Solution** | **Prepare** | **Credential** | **Verification** |
| Pick Microsoft 365 and Azure from your subscription's catalog. | Tick what REVIEWIT must collect; the wizard derives the rights to grant. | Enter what Microsoft 365 and Azure handed you; REVIEWIT verifies it before saving. | One verdict per resource: what is covered, what remains to be granted. |

IN THIS GUIDE


1 How REVIEWIT connects to Microsoft 365 and Azure

2 What REVIEWIT will read, and the rights it takes

3 Create the credential at Microsoft 365 and Azure

4 What you will enter in the wizard

5 The connection wizard, in four steps

6 What REVIEWIT receives, and what it never receives

7 After the connection

8 Troubleshooting and checklist


## 01 How REVIEWIT connects to Microsoft 365 and Azure

REVIEWIT reviews **access**: who can reach what, and whether it is still justified. To do so it reads, **read-only**, the inventory of your resources and their rights at Microsoft 365 and Azure, from your hosting region. It never writes on your side, never reads any content, and keeps the credential you hand it in a vault that only the collector opens.

ON YOUR SIDE
**Microsoft 365 and Azure**
You create a technical credential, limited to the read rights the wizard lists.

→

YOUR REGION
**REVIEWIT collector**
Verifies the credential with a real call, then reads the inventory at the frequency of your collection plans.

→

YOUR CONSOLES
**Workspace Manager**
Campaigns, reviews and reports: never a direct call to Microsoft 365 and Azure.

GUIDING PRINCIPLE

REVIEWIT believes only what it has observed by calling: a right granted but not verified stays "unverified" until the next health pass. What a connection cannot collect is stated **resource by resource**; a resource that cannot be collected can still be imported as a report.

SUPPORT

Microsoft 365 and Azure of one Entra ID tenant: one connection per solution, which may share the same app registration. Azure reads the subscriptions where the **Reader** role is granted to the app; Exchange and Power BI each require their own administration gesture (section 2).

## 02 What REVIEWIT will read, and the rights it takes

The wizard computes the exact list of rights from the resources you tick at the **Prepare** step, and hands it to you ready to copy ("Copy the plan"). The table below gives the rights of the most commonly retained resources; your plan may hold fewer.

| RIGHT OR GESTURE | RESOURCES IT OPENS |
|---|---|
| `Directory.Read.All` | Users, groups, roles, SharePoint sites, teams, channels, communities: the base of everything |
| `Sites.Read.All` · `Sites.FullControl.All` | SharePoint sites and OneDrive, their permissions and sharing links (FullControl is only requested to read site role assignments) |
| `Reports.Read.All` | Usage reports: last activity of sites, OneDrive, teams, communities and shared mailboxes |
| `ReportSettings.Read.All (optional)` | Read the usage reports' concealment setting: the collection says whether it hides names. Without it, nothing is blocked |
| `Channel.ReadBasic.All` · `ChannelMember.Read.All` | Teams channels and their members |
| `Community.Read.All` | Viva Engage communities |
| `Exchange.ManageAsApp (Office 365 Exchange Online)` | Shared mailboxes and public folders, with the Exchange gesture below |
| `Global Reader (directory role)` | Access package catalogs, app registrations (Azure) |

ADMINISTRATION GESTURES

| RIGHT OR GESTURE | RESOURCES IT OPENS |
|---|---|
| **Grant admin consent** | Every application permission above: without it, each call returns 403. |
| **Assign an Exchange administration role to the app** | Shared mailboxes, public folders — **Global Reader** or "View-Only Organization Management" on the service principal. |
| **Open the Power BI read-only admin API to a group containing the app** | Power BI workspaces — Admin portal › Tenant settings › "Allow service principals to use read-only admin APIs". |
| **Show real names in usage reports** | Microsoft 365 admin center › Settings › Org settings › Services › Reports: untick "Display concealed user, group, and site names in all reports". While it is ticked, no activity date is set. |
| **Assign the Reader role on at least one Azure subscription** | Role assignments, custom roles, virtual machines, App Service, disks, IP addresses, storage accounts, scopes and resources. |

# 03 Create the credential at Microsoft 365 and Azure

A tenant administrator creates, in the Microsoft Entra admin center, **an app registration dedicated to REVIEWIT**, grants it read **application permissions** (not delegated), consents for the organisation, then hands it a secret or a certificate. The Exchange, Power BI and Azure gestures complete the plan according to the retained resources.

01 **In `entra.microsoft.com`, open Identity › Applications › App registrations › New registration**

Name "REVIEWIT Collector", accounts **in this organizational directory only**, no redirect URI: the app opens no session.

02 **Note the Application (client) ID and the Directory (tenant) ID on the Overview page**

Two GUIDs: they are the wizard's first two fields.

03 **API permissions › Add a permission › Microsoft Graph › Application permissions**

Tick the permissions of the plan copied from the wizard (Directory.Read.All, Sites.Read.All, Reports.Read.All, Channel.ReadBasic.All, ChannelMember.Read.All, Community.Read.All, ReportSettings.Read.All, optional, and Sites.FullControl.All if you review SharePoint permissions). Add **Office 365 Exchange Online** › **Exchange.ManageAsApp** for shared mailboxes and public folders.

04 **Click Grant admin consent for <your organisation>**

Every row turns to "Granted". A permission not consented returns 403 at collection: the wizard will name it.

05 **Certificates & secrets: create a client secret (12 to 24 months) and note its value and expiry date**

The value is never shown again in Entra. Or upload the **public certificate (.cer)** of your key pair: the `.pfx` goes into REVIEWIT.

06 **Exchange, if you review shared mailboxes or public folders**

**Identity** › **Roles and administrators** › **Global Reader** (or "View-Only Organization Management" in the EAC) › Add assignment › pick the "REVIEWIT Collector" app.

07 **Power BI, if you review its workspaces**

Create a security group containing the app; in the **Power BI admin portal** › **Tenant settings**, enable "Allow service principals to use read-only Power BI admin APIs" for that group.

08 **Azure, for the Microsoft AZURE solution**

On each **subscription** to review: **Access control (IAM)** › **Add role assignment** › **Reader** › the "REVIEWIT Collector" app. The **Global Reader** directory role covers catalogs and app registrations.

ONE REGISTRATION, TWO CONNECTIONS

Microsoft 365 and Microsoft AZURE are two solutions in REVIEWIT, each with its connection and its rights plan. They may share the same app registration and the same secret: one plan adds to the other in Entra.

## 04 What you will enter in the wizard

The **Credential** step only shows the fields Microsoft 365 and Azure declares to REVIEWIT. The connection name is the one you will read in tables and alerts.

| WIZARD FIELD | VALUE |
|---|---|
| **Connection name** | Free — for instance "Microsoft 365 · <your tenant>". |
| **Authentication method** | **Client secret** or **Certificate**: one method per credential, never both. |
| **Tenant ID** | The Directory (tenant) ID noted at step 2 — the connection's external identifier. |
| **Application (client) ID** | The Application ID noted at step 2. |
| **Client secret · Expires on** | The secret's value, entered once, and its expiry date: Entra does not return it at verification, read it in the portal. REVIEWIT warns you before it expires. |
| **Certificate (.pfx) · Certificate password** | The **key pair**, not the public certificate: the `.cer` is in Entra, the `.pfx` comes here. Empty password if the file carries none. |

THE SECRET NEVER COMES BACK ON SCREEN

Entered once for verification, it is stored in the vault and referred to by reference. To change it: "Add a credential", never an overwrite.

# 05 The connection wizard, in four steps

In the Subscription Manager, open **Data sources** › **Connections**, then **Connect a solution** (or **Connect an instance** on the solution's tile if it is already present). Nothing is saved before Microsoft 365 and Azure answers.

## STEP 1 Solution

The catalog lists only what is not connected yet. A "probe available" solution is verified by a real call; a "declarable" one is recorded on your word, at the level you choose.

## STEP 2 Prepare

Tick the resources to collect: the list of rights to grant follows. Copy the plan, grant it at Microsoft 365 and Azure, then come back. The wizard never applies that plan itself.

## STEP 3 Credential

Name the connection and fill in the fields. **Verify the connection** calls Microsoft 365 and Azure; **Save without verifying** keeps the connection inactive, to verify later.

Microsoft types its identity (the Tenant ID): "Save without verifying" opens as soon as the non-secret fields are filled; verification requests a token from Entra and reads the tenant.

## STEP 4 Verification

Microsoft 365 and Azure answered: the wizard shows the identity it read and, resource by resource, a verdict. **Save and activate** puts the connection in service; **Save inactive** keeps it for later.

The per-resource verdict says exactly which permission or gesture is missing: Graph, Exchange, Power BI or Azure. Grant it, then "Check rights": nothing is retyped.

## 06 What REVIEWIT receives, and what it never receives

| RECEIVED FROM MICROSOFT 365 AND AZURE | USE AT REVIEWIT |
|---|---|
| `Tenant ID · tenant name` | The connection's identity and display name. |
| `Microsoft Graph` | Users, groups, roles, sites, teams, channels, communities, applications: the objects, their owners, members and permissions — never their content. |
| `Usage reports` | The last activity of sites, OneDrive, teams and mailboxes: one date per object, never a document. |
| `Power BI activity log` | A person's last action on each workspace, over the 28 days Power BI keeps: a date, never a report or a query. |
| `Exchange Online (Get-* cmdlets)` | Shared mailboxes, public folders, delegations: lists, never an e-mail. |
| `Azure Resource Manager (read)` | Subscriptions, resource groups, resources and role assignments — never a key, a secret or stored data. |
| `"Everyone" permissions · "People in your organization" links` | The **Overshared** signal: audience, broad groups, organisation links counted and dated. |

NEVER RECEIVED, NEVER REQUESTED

**No user password**
The credential is technical, created for REVIEWIT; no person's account is used.

**No content**
No message, file or e-mail: REVIEWIT reads lists of objects and rights, never what they contain.

**No write**
The rights requested are read rights; remediation, where it exists, is a separate module, enabled separately.

**No secret shown again**
The secret is entered once, stored in the vault and referred to by reference; no screen or log shows it again.

## 07 After the connection

The connection is managed from **Data sources › Connections**. A health pass replays the verification **every 24 hours**; "Verify all connections" runs it on demand. Each tile states how many resources are ready, to configure or unverified.

| | |
|---|---|
| **A right is missing** | The resource stays "unverified" and the wizard says which one. Grant it at Microsoft 365 and Azure, then "Check rights". |
| **Renew the secret** | Create a **new secret** in Entra (Certificates & secrets), note its expiry date, enter it under "Connections › Add a credential" with the date, verify, then delete the old secret. To stop renewing: switch to a **certificate** — the `.cer` in Entra, the `.pfx` in REVIEWIT; some tenants' policy requires it. |
| **A resource that cannot be collected** | Import its report from **Data sources › Collect › Choose a report**: the exact CSV contract downloads from the drawer. |
| **Disconnect** | Deactivate the connection; then revoke the credential at Microsoft 365 and Azure. Collection plans that relied on it stop. |

# 08 Troubleshooting

| WHAT YOU SEE | CAUSE | WHAT TO DO |
|---|---|---|
| `AADSTS7000215` **"Invalid client secret"** | Secret copied wrong, or the secret's ID copied instead of its value. | Create a new secret and copy its **value** when entering it. |
| `AADSTS700016` **"Application not found in the directory"** | The Tenant ID or Application ID belongs to another tenant. | Read both GUIDs on the registration's Overview page, in the right tenant. |
| `AADSTS7000222` **"The provided client secret keys are expired"** | The secret has expired. | New secret in Entra, "Add a credential" in REVIEWIT with its date. |
| **A resource returns 403** `Authorization_RequestDenied` | Application permission missing or not consented. | Add it, grant admin consent, then "Check rights". |
| **Shared mailboxes or public folders "unverified"** | Exchange.ManageAsApp consented but no Exchange administration role assigned to the app. | Assign Global Reader (or View-Only Organization Management) to the app. |
| **Power BI workspaces "unverified"** | The read-only admin API is not open to the app's group. | Power BI tenant settings: enable the option for a security group containing the app. |
| **Notice "the tenant conceals names in usage reports"** | The concealment setting is on: the reports replace names with hashes and nothing matches. | Untick the box in the Microsoft 365 admin center (Org settings › Services › Reports); the next collection dates the objects. |
| **Notice "usage reports' concealment setting unreadable"** | ReportSettings.Read.All is not consented. | Add it and grant admin consent. It is optional: without it, the collection carries on. |
| **Azure: "no subscription" or missing resources** | The Reader role is not assigned on the subscription, or only on one resource group. | Assign **Reader** at the level of each subscription to review. |

### CHECKLIST BEFORE OPENING THE WIZARD

6 items

- [ ] I can create an app registration and grant admin consent in the tenant.
- [ ] The "REVIEWIT Collector" registration exists: accounts in this directory only, no redirect.
- [ ] The plan's **application** permissions are added and **consented** for the organisation.
- [ ] I have a secret (value and expiry date) or a `.pfx` key pair whose `.cer` is uploaded in Entra.
- [ ] Exchange, Power BI and Azure: the gestures matching the retained resources are done.
- [ ] I noted the Tenant ID and the Application (client) ID, and I open the Subscription Manager as a subscription administrator.

This guide is provided to REVIEWIT customers to connect their solutions. Menu paths are those of the vendors' consoles at publication date; they may change. In case of discrepancy, the REVIEWIT wizard prevails: it shows the exact plan computed for your subscription.