Recyber

Republic Installation Guide

Deploying the Teams app and the Outlook add-in across your organisation.

WHAT'S INSIDE

AUDIENCE
Microsoft 365 administrators

TEAMS APP
v2.1.0

PUBLISHED
24 August 2026

OVERVIEW

Before you begin

Republic is published in the Microsoft Teams store, so most organisations never need a manifest file — you allow the app and push it out with a setup policy.

Manifest files are included here for tenants that deploy custom app packages, and for the Outlook add-in, which is deployed from the Microsoft 365 admin centre.

You will need

- A **Teams Administrator** or **Global Administrator** account for the Teams work.
- A **Global Administrator** account to deploy the Outlook add-in organisation-wide.
- Your Republic tenant provisioned by Recyber — your onboarding contact confirms this before rollout.
- A decision on scope: the whole organisation, or a pilot group first.

> **Roughly ten minutes of admin work**
> The clicking is quick. What takes time is Microsoft propagating the change: app setup policies can take up to 24 hours to reach every Teams client, and a centrally deployed Outlook add-in up to six hours to reach every mailbox. Schedule your staff communications accordingly.

What you are deploying

Republic reaches your people across four surfaces. The two that need an administrator are covered in this guide.

NEEDS AN ADMIN

Teams bot

Weekly knowledge-check questions and curated micro-video lessons, delivered in chat.

NEEDS AN ADMIN

Outlook add-in

A Report Phishing button on the message ribbon, for simulations and real threats alike.

INCLUDED

Republic web app

A tab inside Teams for sector news and reporting anything that looks wrong. Arrives with the Teams app.

INCLUDED

Admin dashboard

Organisation-level reporting, user management and rollout controls, on the web.

MICROSOFT TEAMS · RECOMMENDED

Deploy the Teams app from the store

This installs Republic for everyone in scope, so your people do not have to find or add anything themselves.

1. **Open the Teams admin centre**
   Sign in at admin.teams.microsoft.com with an account holding the Teams Administrator or Global Administrator role.

2. **Find Republic in Manage apps**
   Go to **Teams apps → Manage apps** and search for **Republic**. Open the app to review its details and the permissions it requests.

3. **Allow the app**
   If your organisation blocks third-party apps by default, set the app's status to **Allowed**. Where a permission policy is assigned to your users, make sure that policy also permits Republic.

4. **Add Republic to a setup policy**
   Go to **Teams apps → Setup policies** and open the policy your users are assigned to — usually **Global (Org-wide default)**. Under **Installed apps** select **Add apps** and add Republic. Add it under **Pinned apps** too, so it appears in the Teams sidebar rather than behind the ellipsis.

5. **Scope and save**
   Save the policy. For a pilot, create a separate setup policy and assign it to a group instead of editing the org-wide default.

6. **Grant consent and confirm**
   The first time a user opens Republic they sign in with their work account. If your tenant requires admin consent for new applications, approve the request in **Microsoft Entra ID → Enterprise applications** so users are not blocked at first launch.

MICROSOFT TEAMS · CUSTOM UPLOAD

Deploy from the manifest instead

Use this route only where your organisation deploys Teams apps as custom packages rather than from the store.

> **Custom uploads do not update themselves**
> A store-installed app updates automatically when we publish a new version. A custom upload stays on the version you uploaded until an administrator uploads the next one. Prefer the store route wherever your policies allow it.

1. **Download the app package**
   Upload the zip exactly as downloaded — do not unzip it first.
   Download republic-teams-app.zip ↗
2. **Upload it as a custom app**
   In the Teams admin centre go to **Teams apps → Manage apps**, select **Actions → Upload new app**, and choose the zip.
3. **Wait for it to appear**
   Depending on the size of your organisation the app can take up to an hour to show in the list.
4. **Allow it and add it to a setup policy**
   Set the app's status to **Allowed**, then add it to the relevant setup policy under **Installed apps** and **Pinned apps**, exactly as with the store route.

MICROSOFT TEAMS · SELF-SERVE

Letting people install it themselves

If your organisation already allows users to add apps from the Teams store, no admin action is needed.

- In Microsoft Teams, select **Apps** in the left sidebar.
- Search for **Republic** and select it from the results.
- Select **Add**. Republic is free to add and use — there is no in-product purchase step.
- Right-click the Republic icon in the sidebar and choose **Pin** so it stays visible.

OUTLOOK

Deploy the Outlook add-in

The add-in adds a **Report Phishing** button to the message ribbon. It reports Republic phishing simulations as a catch, and forwards genuine suspicious mail to your organisation's security inbox — one button, both jobs.

> **One manifest covers every Outlook client**
> A single XML manifest supports classic Outlook on Windows (2016 / 2019 / 2021 / 2024 and Microsoft 365), new Outlook for Windows, Outlook on the web, and Outlook on Mac. There is nothing else to upload.

Organisation-wide (centralised deployment)

1. **Download the manifest**
   One file, for every client.
   Download republic-outlook-report-phishing.xml ↗
2. **Open Integrated apps**
   Sign in to the Microsoft 365 admin centre at admin.microsoft.com, select **Show all**, then **Settings → Integrated apps**.
3. **Upload the add-in**
   Select **Upload custom apps**, set the app type to **Office Add-in**, choose **Upload manifest file (.xml) from device**, and select the manifest you downloaded.
4. **Choose who gets it**
   Assign it to **Entire organization**, or to specific users and groups if you are piloting. Review the permissions summary, then select **Finish deployment**.
5. **Confirm the deployment**
   The add-in now appears in the Integrated apps list with its assigned users. Allow up to six hours for it to reach every mailbox in scope.

OUTLOOK · SINGLE MAILBOX

Sideload for testing

To try the add-in on one mailbox before deploying it centrally:

- **Outlook on the web / new Outlook:** Settings → **General** → **Manage add-ins** → **My add-ins** → **Custom add-ins** → **Add from file** → choose the manifest.
- **Classic Outlook (Windows / Mac):** ribbon → **Get Add-ins** → **My add-ins** → **Custom add-ins** → **Add from file** → choose the manifest.
- The **Report Phishing** button then appears on the ribbon when reading a message.

WHAT IT DOES

Behaviour once installed

- Adds one **Report Phishing** button to the message ribbon — no dialogs, no forms.
- If the reported message is a Republic simulation, it is recorded as a successful catch and the user's score moves.
- If it is genuinely suspicious, it is logged and forwarded to your organisation's security inbox.
- Either way it feeds Republic's behavioural risk scoring alongside Teams activity.

EMAIL DELIVERABILITY · ADMIN

Allowlist Recyber in Microsoft 365

Republic sends phishing simulations and training email from **mail.recyber.com**. Microsoft 365 filters inbound mail hard — and a convincing simulation looks exactly like real phishing — so allowlist Recyber before you launch, or your people never see the test.

> **Use the advanced delivery policy — not a spam allow list**
>
> To keep tenants safe, Microsoft deliberately ignores ordinary allow lists, connection-filter IP allow lists and `SCL:-1` mail flow rules for anything it scores as high-confidence phishing or malware — which is exactly what a good simulation looks like. The **advanced delivery policy** is the only method Microsoft supports for phishing simulations: it tells Microsoft Defender these messages are an authorised test, not a real attack.

STEP 1

Find Recyber's current sending IP

The policy needs at least one sending IP. We send through a shared pool with no fixed, published IP list — so you read the live one straight off a test message. No dedicated IP is required.

1. **Send yourself a test simulation**
   Trigger a test send to a mailbox you control — an admin can do this from the Republic dashboard. It need not be allowlisted yet; you only need its headers.

2. **Find the message**
   Until Recyber is allowlisted the test may land in Junk or be held in Quarantine (Defender portal → **Review → Quarantine**). Either is fine — the headers are intact wherever it lands.

3. **Read the sending IP**
   Quickest: **Exchange admin centre → Mail flow → Message trace** shows the sender IP directly. Or open the headers and find `Authentication-Results: spf=pass (sender IP is 12.34.56.78) smtp.mailfrom=mail.recyber.com` — that IP is what you enter.

4. **Grab a couple more**
   Send two or three tests and note each distinct sending IP — a shared pool can use more than one. The policy accepts up to 10, so add them all.

STEP 2 · MICROSOFT DEFENDER PORTAL

Add Recyber to the advanced delivery policy

You need the **Security Administrator** role (Email & collaboration) plus **Organization Management** (Exchange Online), or a Global Administrator account.

1. **Open the advanced delivery policy**
   In the Microsoft Defender portal, go to **Email & collaboration → Policies & rules → Threat policies → Advanced delivery** (under Rules), or open security.microsoft.com/advanceddelivery directly.

2. **Open the Phishing simulation tab**
   Select the **Phishing simulation** tab, then **Add** — or **Edit**, if Recyber already has entries there.

3. **Add the sending domain**
   Under **Domain**, enter **mail.recyber.com**. This is the MAIL FROM (envelope) and DKIM domain our simulations use, and the value that carries the trust. Up to 50 domains.

4. **Add the sending IP(s) you found**
   Under **Sending IP**, enter each IP you read from your test messages. A single IP, a range or a CIDR block are all accepted, up to 10 entries. A message must match at least one domain *and* one sending IP.

5. **Add simulation link domains (only if needed)**
   Under **Simulation URLs to allow**, add the phishing-link root domains from your Republic console. This is only for links in Teams messages or Office documents — links inside simulation emails are allowed automatically. Up to 30 entries.

6. **Save and confirm**
   Select **Add**, then **Close**. Send one more test to confirm it now lands in the inbox. Defender leaves our simulations unfiltered, and Safe Links won't block or detonate our links (it still wraps them, which is expected).

EMAIL DELIVERABILITY

What to allow, and checking it worked

These are the exact values Microsoft matches on. The domain is fixed; read the IPs off a test message as in Step 1.

Sending domain	`mail.recyber.com`
Sending IP address	**Read from a test message header (no dedicated IP needed)**
Simulation link domains	**From your Republic console — non-email links only**

If your mail routes through a gateway

If your domain's MX record points somewhere other than Microsoft 365 — a secure email gateway such as Mimecast or Proofpoint — allow **mail.recyber.com** there too, and enable **Enhanced Filtering for Connectors** so Defender still sees our true sending IP rather than the gateway's.

IF SOMETHING LOOKS WRONG

Deliverability troubleshooting

SYMPTOM	WHAT TO DO
Simulations land in Junk or are quarantined	Confirm mail.recyber.com *and* a current sending IP are both on the **Phishing simulation** tab, and that the test matched one of each. A domain alone isn't enough — Microsoft needs an IP match too.
It worked, then simulations get filtered again	Our shared pool can rotate onto an IP you haven't listed. Re-read the header, add the new IP alongside the others (up to 10), and save. If it recurs, a dedicated sending IP makes this a one-time setup — ask us.
Links are stripped, rewritten to a warning, or blocked	That is Safe Links or a gateway. With mail.recyber.com on the policy, Safe Links wraps but won't block our links. Don't add them to **Do not rewrite the following URLs** — that can raise spurious click alerts. Allow Recyber on any gateway too.
Everything is allowlisted but mail still doesn't arrive	If mail routes through on-premises Exchange or a gateway first, Defender may see that hop's IP, not ours. Enable Enhanced Filtering for Connectors, or deliver simulations straight to your Microsoft 365 MX record.
Reported simulations aren't scoring	Reporting is the Outlook add-in's job, not this policy. Confirm the add-in is deployed and that users report with the **${OUTLOOK.appName}** button.

ROLLOUT

Telling your people

Deployment is only half of it. Republic lands best when people know it is coming, so here is the announcement to send — copy it as it is, or make it sound like you.

> **Send it once the rollout has propagated**
> Setup policies can take up to 24 hours to reach every Teams client and a centrally deployed add-in up to six hours to reach every mailbox. Announce Republic after that window, not before — a message about an app people cannot yet see creates support tickets rather than momentum.

SUBJECT **Introducing Republic — your new security coach**

Our organisation has partnered with **Recyber** to bring you **Republic**, a new behavioural security solution designed to help reduce human cyber risk. Accessible through Microsoft Teams and your browser, Republic acts as your personal security coach, offering support only when you need it and making security a positive, rewarding experience. By combining the latest behavioural science with storytelling and gamification, we help you build strong security habits naturally. This isn't just another training tool; it's security reimagined.

Republic also includes a phishing game called **Interception**. It helps you practise secure email reporting while unlocking levels with increasingly deceptive emails. Emails are delivered at a consistent pace across all levels, but you'll earn more Virtucoin for completing the harder ones. Interception is played directly from your email inbox using the Recyber add-in for Outlook — the **Report Phishing** button on your message ribbon — and your progress is managed through the **Map** section of the main Republic app in your browser, where you can view and select from available levels at any time.

You'll soon get a message from the **Republic Teams bot**, which will give you a quick tour and get you up and running.

If you require help or assistance you can access the Recyber Support Hub at https://recyber.atlassian.net/servicedesk.

Two things worth adding

- Say who to contact internally. People who hit a problem should know whether to raise it with IT or go straight to the Recyber Support Hub.
- Say plainly that Republic is not a monitoring tool. It coaches individuals and reports risk to the organisation in aggregate — stating that up front prevents the question being asked in the wrong tone later.

FILES YOU NEED

Manifest downloads

Both files are served over HTTPS and are always the current version. Download them on the machine you are running the admin centre from — the links below are live.

ZIP

Teams app package

Version 2.1.0. Contains the manifest and app icons. Upload the zip as-is — do not unzip it first. Only needed for custom-app deployment.

`republic-teams-app.zip`

Download ↓

XML

Outlook add-in manifest

One file for classic Outlook on Windows, new Outlook for Windows, Outlook on the web and Outlook on Mac. Required to deploy the add-in.

`republic-outlook-report-phishing.xml`

Download ↓

The Outlook manifest is also served live by the API at https://republic-v2-api.vercel.app/api/interceptions/extension/manifest.xml — useful where your admin centre accepts a URL rather than a file upload.

Identifiers

Teams app ID	`1f518d36-07de-4ce5-860c-cc774c7bf327`
Teams app name	**Republic V2 by Recyber**
Outlook add-in ID	`ee7dee35-d48b-4221-904c-115af0017096`
Outlook add-in name	**Report Phishing**

Keep these to hand — they are how you identify Republic in the admin centre, and how you tell the store version apart from a manually uploaded one.

IF SOMETHING LOOKS WRONG

Troubleshooting

SYMPTOM	WHAT TO DO
Republic does not appear in Manage apps	Newly published store apps can take up to an hour to surface in a tenant's catalogue. Clear your search filters and confirm you are searching the Microsoft apps catalogue rather than Custom apps.
Users cannot see the app after a policy change	App setup policy assignments can take up to 24 hours to reach every client. Ask an affected user to sign out of Teams and back in, and confirm they are assigned the policy you edited.
Users are blocked at sign-in	This usually means your tenant requires admin consent for new applications. A Global Administrator can approve Republic in Microsoft Entra ID → Enterprise applications.
The Outlook button is missing from the ribbon	Outlook hides overflow actions behind **More actions (...)**. Users can promote it in Settings → Mail → Customise actions. Centralised deployment can also take up to six hours.
The manifest upload is rejected	Confirm you selected **Office Add-in** as the app type and are uploading the XML manifest — not the Teams app zip. The two are not interchangeable.

SUPPORT

Need a hand?

Your onboarding contact can walk your administrators through deployment and provide staff communication templates.

> Email info@recyber.com · Call +44 (0) 203 443 9153 · recyber.com/contact