

Deploying Desktop Connect with Microsoft Intune

For IT teams deploying to Windows and macOS endpoints through the Intune admin center. Covers silent installation, configuration profiles, pre-install scripts, and verification.

How this works

Windows and macOS are separate deployments with different installers and different steps. If you manage both, plan for two. For macOS, plan for three, since Intel and Apple Silicon Macs need their own packages and their own scripts.

Each platform is covered in its own section below. Work through the one that applies, then use the verification section at the end, which applies to both.

The one rule that matters most: never rename the installer. The filename contains your organization's license key. Renaming it, shortening it, or letting a duplicate download append something like (1) will cause the agent to install, run, and register nothing, with no error anywhere. Use the file exactly as downloaded.

BEFORE YOU START

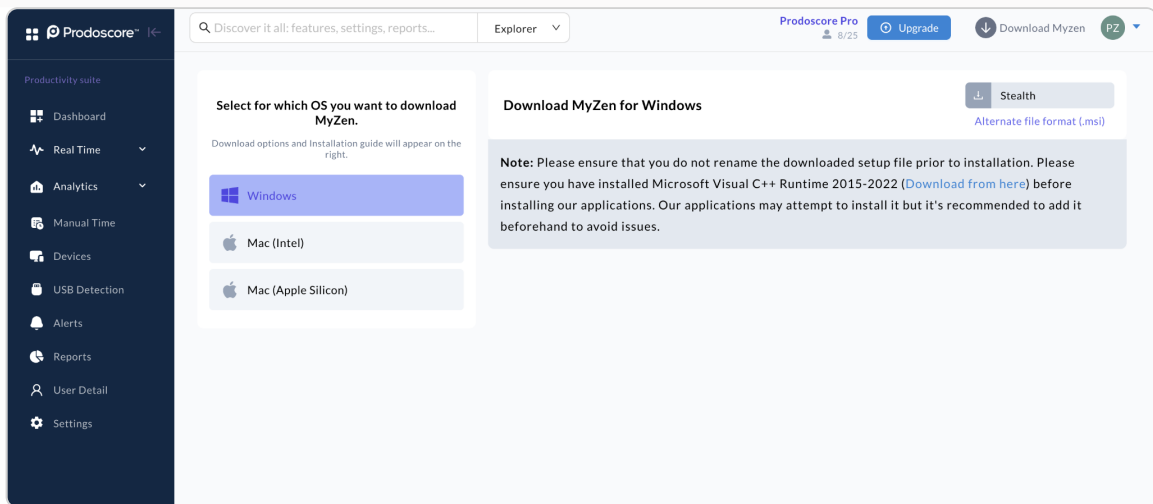
WHAT YOU NEED	DETAIL
Intune access	Administrator privileges in the Intune admin center.
Installer files	One per platform and architecture, downloaded from the Desktop Connect Admin Portal. The filename arrives already encoded with your license key.
Configuration profiles	macOS only. Two .mobileconfig files supplied by Prodoscore.
Pre-install script	macOS only. A short shell script you create using the token from your PKG filename. Covered in Phase 2.
Windows versions	Windows 10 or later.
macOS versions	macOS 13 Ventura or later. Earlier versions are not supported and the install will fail.
Endpoint protection	Add the exclusions listed near the end of this guide before deploying, not after the first failure.

1

Download the installers

One per platform and architecture

Sign in to the Desktop Connect Admin Portal, open the Download option in the top bar, and select the platform you need. Windows, Mac Intel, and Mac Apple Silicon are separate downloads.



Select your platform, then download. Do not rename the file afterwards.

If you download the same file twice, your browser may append (1) to the second copy. That breaks the license key exactly as a rename would, so delete any duplicates before uploading.

WINDOWS DEPLOYMENT

2

Add the app to Intune

Two packaging options

Upload the installer to Intune as a Line-of-business app and enter the command line below, substituting your actual filename:

```
msiexec /i "<your-installer-filename>.msi" /qn
```

- `/qn` is what makes the installation silent. Without it the installer waits for an interface that never appears.
- Set **Install behavior** to **System**.
- Your filename will be a long encoded string. That is expected.

An EXE installer is also available and is more reliable. The MSI has known issues with installations and updates, particularly if any previous installation is still registered on the machine, in which case it will run in maintenance mode, copy no files, and report success anyway. The EXE handles these cases better. It installs with `/exenoui /qn` and needs to be packaged as a Win32 app rather than a Line-of-business app. Contact your Prodoscore representative if you would like to use it.

3 Suppress installation notifications

Otherwise Windows shows a banner to the employee

- Open the **Assignments** tab for the app.
- Assign it to your target group as **Required**.
- In the **End user notifications** column, select **Hide all toast notifications**.
- Save.

4 Add a detection rule

Recommended. Intune's own status is not reliable here.

Intune can report an installation as complete when it has not finished. A detection rule based on a file the agent actually writes gives you a truthful answer.

Use a file-exists rule for:

```
C:\Program Files\zs\zs\version.txt
```

MACOS DEPLOYMENT, PHASE 1: CONFIGURATION PROFILES

Both profiles must reach the Mac before the PKG installs. They deploy immediately over the Apple MDM channel, so create and assign them first. A profile created after the PKG may arrive too late to take effect.

PROFILE	WHAT IT DOES
Permissions (PPPC)	Grants the Accessibility permission the agent needs in order to record activity. Without it the agent installs and registers but captures nothing.
Notifications	Silences the macOS "Background Items Added" alert that would otherwise appear when the agent installs its background service. Note that this suppresses that alert for all applications, not only Desktop Connect.

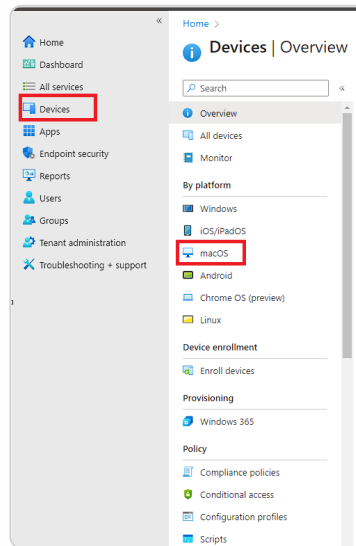
Users may still see a permission prompt even with the profiles deployed. The Permissions profile grants Accessibility centrally, which is what the agent needs in order to record activity. Depending on the agent version in use, a separate prompt can still appear on first run. If your rollout needs to be entirely invisible to employees, raise it with your Prodoscore representative before you begin so we can confirm what to expect on your current version.

5

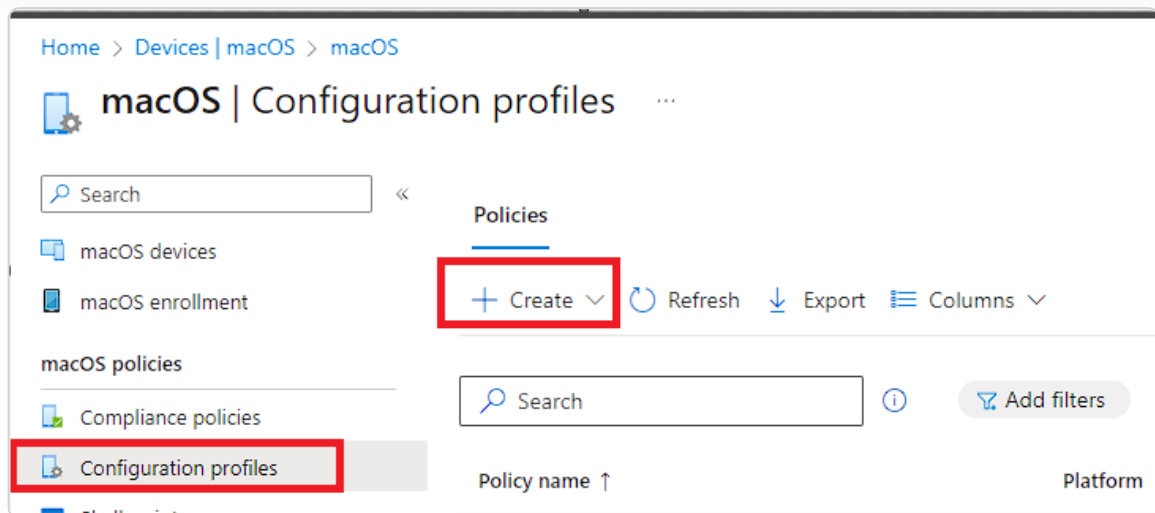
Upload each profile

Repeat the whole process for both

In the Intune admin center, go to **Devices**, then select **macOS** under By platform.



Select **Configuration profiles**, then **Create**.



Choose **macOS** as the platform, **Templates** as the profile type, then **Custom**.

- Give the profile a clear name, for example Prodoscore Permissions or Prodoscore Notifications.
- Set **Deployment channel** to **Device** and upload the .mobileconfig file.
- Assign it to your target device group.

Create profile ...

macOS - Settings catalog

✓ Basics ✓ Configuration settings ✓ Scope tags **1 Assignments** 3 Review + create

Included groups

+ Add groups + Add all users **+ Add all devices**

Groups	Group Members ⓘ	Filter	Filter mode
No groups selected			

Excluded groups

ⓘ When excluding groups, you cannot mix user and device groups across include and exclude. [Click here to learn more about excluding groups.](#)

+ Add groups

Groups	Group Members ⓘ	Remove
No groups selected		

Add your target devices or groups on the Assignments tab, then review and save.

MACOS DEPLOYMENT, PHASE 2: SCRIPT AND PACKAGE

Intel and Apple Silicon need separate deployments. Two packages, two different tokens, two scripts, two device groups. A token from one architecture will not work with the other.

6 Create the pre-install script

One per architecture

Intune renames files during deployment, so on macOS the installer cannot read the license key from its own filename. The pre-install script writes that key to the Mac before the package installs.

Your downloaded PKG has a long encoded filename. The token is that filename with `.pkg` removed. Paste it into the script in place of the placeholder:

```
#!/bin/sh

echo '<YOUR_TOKEN>' | base64 --decode > /Library/Preferences/zs.json

exit 0
```

If you download a fresh package later, the token changes and the script must be updated to match. A script carrying an old token will run without error and the agent will never register.

7

Upload the PKG

Apps, macOS, Add, then macOS app (PKG)

- Upload the .pkg file with its full original filename.
- Paste your script into the **Pre-install script** field.
- Leave **Post-install script** empty.
- Set **Ignore app version** to **Yes**.
- Assign the app as **Required** to the matching device group.

Remove the Qt entries from the detection rules. Intune auto-detects several included apps beginning with `org.qt-project`. These are internal framework libraries that Intune cannot detect on the device, and leaving them in causes Intune to sit on "Waiting for install status" indefinitely. Keep only `ai.zs.zs`.

VERIFICATION

8

When devices should appear

Both platforms

The macOS installer takes 4 to 10 minutes, because it waits for the agent to start before reporting back. During that window Intune shows "Waiting for install status," which looks like a hang but is not. Do not cancel or re-push during it.

Once installed, a device registers within roughly 30 minutes, provided a user has logged into the desktop. On macOS the agent does not start until a login or a lock and unlock cycle, so a Mac that is installed and left untouched will not report.

If a device has had someone logged in and still has not appeared after 30 minutes, treat it as a failure.

9

Check the files on the device

More reliable than the Intune status

PLATFORM	PATH	WHAT IT CONFIRMS
Windows	C:\Program Files\zs\zs\version.txt	The install completed and wrote its files.
macOS	/usr/local/zs/zs.app/Contents/MacOS/ version.txt	The package installed and wrote its files.
macOS	/Library/Preferences/zs.json	The pre-install script ran and the license key is in place. Should be readable JSON, not empty.

On a Mac, the app present but `zs.json` missing or empty means the token was wrong or the script did not run. The agent will never register in that state.

ENDPOINT PROTECTION EXCLUSIONS

The agent monitors processes and window activity in the background, which is what endpoint protection is built to detect. Without exclusions it is often blocked or quarantined, usually with no visible alert. Add these before deploying.

Folders

- Windows: `C:\Program Files\zscaler\` and `%APPDATA%\ai.zscaler\`
- macOS: `/usr/local/zs/` and `~/Library/Application Support/ai.zs/`

Network endpoints

The agent connects outbound over HTTPS on port 443 only. No inbound connections are needed. Allow the following, and exclude them from SSL inspection, authentication requirements, and any web security suite such as Zscaler.

- **Wildcard, recommended:** `*.ag.prodoscoring.com`
- **Licensing:** `origin.hrsaastech.com`
- **Storage:** `storage.googleapis.com`

If your security policy requires explicit subdomains rather than a wildcard, use `api.ag.prodoscoring.com`, `auth.ag.prodoscoring.com`, `portal.ag.prodoscoring.com`, and your own `<base_domain>.ag.prodoscoring.com`. Your base domain is the text immediately before `.ag.prodoscoring.com` when you sign in to Prodoscore in a browser.

If your firewall filters by IP as well as domain, allow these licensing server addresses:

`104.26.15.125`, `172.67.72.141`, `104.26.14.125`, `104.21.48.128`, `172.67.151.154`. An HTTPS request should be permitted if either the domain or the IP matches.

If Defender is managed through Intune, add these exclusions in the Intune Defender policy rather than locally on a machine. Local exclusions on a managed device can be overwritten the next time policy applies, which produces a failure that appears to fix itself and then returns.

IF SOMETHING GOES WRONG

WHAT YOU SEE	MOST LIKELY CAUSE
Intune reports success, device never appears	Intune can report an install as complete when it is not. Retrigger the installation from the Intune portal first, since that resolves most cases.
Files are present, <code>version.txt</code> is missing	The install did not complete, usually because a previous installation was already on the machine. Ask Prodoscore for the cleanup utility, run it, restart, then deploy again. On Windows, the cleanup utility does not clear the installation registration, so if the reinstall still reports that the software is present, ask your Prodoscore contact for the steps to clear it.
Intune stuck on "Waiting for install status"	If it has been more than 15 minutes, the Qt entries are probably still in the detection rules. See step 7.
Files disappear after a successful install	Endpoint protection has quarantined them. Add the exclusions and reinstall.
Mac registers but no activity is recorded	The Permissions profile did not apply. Confirm it deployed and is assigned to that device.
Mac has the app and config but nothing ever runs	Wrong architecture package. An Intel Mac cannot run Apple Silicon binaries.
Nothing on a particular Mac	Check the macOS version. Anything earlier than macOS 13 Ventura is not supported.
Device appears but no activity is ever recorded, Windows	Check which account the person signs in as. Accounts named Administrator may be excluded from tracking by default, which produces a device that looks healthy and records nothing. Tell your Prodoscore contact if this applies, as it is a setting changed on our side.

QUICK REFERENCE

ITEM	VALUE
Windows install command	<code>msiexec /i "filename.msi" /qn</code>
Windows install behavior	System
Windows install path	<code>C:\Program Files\zs\zs</code>
macOS app type in Intune	macOS app (PKG)
macOS install path	<code>/usr/local/zs/zs.app</code>
macOS tenant config	<code>/Library/Preferences/zs.json</code>
macOS bundle ID	<code>ai.zs.zs</code>
Detection rules, macOS	Keep only <code>ai.zs.zs</code> . Remove all <code>org.qt-project</code> entries.
Ignore app version	Yes
macOS packages	Separate Intel and Apple Silicon, separate tokens, separate deployments
Minimum versions	Windows 10, macOS 13 Ventura
Time to appear	Within 30 minutes of install, after a user logs in

Before a full rollout, deploy to two or three machines, one of each platform and architecture you manage, and confirm they appear in Prodoscore. A whole fleet failing identically is almost always one configuration decision repeated across every device.