

Deploying Desktop Connect with Jamf Pro

For Mac administrators deploying to macOS endpoints through Jamf Pro. Covers configuration profiles, the pre-install script, the deployment policy, and verification.

What this covers

This guide is macOS only. If you also manage Windows endpoints, deploy those through Microsoft Intune or an RMM tool and ask your Prodoscure representative for the matching guide.

The deployment has four parts: two configuration profiles, the installer package, a pre-install script that writes your license configuration, and a policy that ties the script and package together.

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
Jamf Pro access	Administrator privileges.
Configuration profiles	Two .mobileconfig files supplied by Prodoscure.
Installer packages	Downloaded from the Desktop Connect Admin Portal. Intel and Apple Silicon are separate files with separate license tokens.
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.

STEP 1: DEPLOY THE CONFIGURATION PROFILES

Both profiles must reach the Mac before the package installs. They deploy immediately over the Apple MDM channel, so upload and scope them first, or at the same time as the package.

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 at all.
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.

1

Upload each profile

Repeat for both

- Go to **Computers**, then **Configuration Profiles**.
- Click **Upload** and select the .mobileconfig file.
- Set the **Scope** to All Computers or your target group.
- Save, then repeat for the second profile.

STEP 2: UPLOAD THE INSTALLER

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

2 Download and upload the package

One per architecture

Sign in to the Desktop Connect Admin Portal and download the installer for the architecture you need. Apple Silicon covers M1, M2, M3, and M4 machines. Intel covers everything older.

Then in Jamf Pro:

- Go to **Settings, Computer Management**, then **Packages**.
- Click **New** and upload the .pkg file.
- Confirm the filename in Jamf matches the original download exactly, character for character.
- Save.

If your fleet has both architectures, upload both packages and create Smart Groups using the **Architecture Type** criteria so each policy targets the right machines.

STEP 3: CREATE THE PRE-INSTALL SCRIPT

3 Write the license configuration to the Mac

One script per architecture

This script writes your license configuration to the Mac before the installer runs, so the agent registers with your Prodoscore account immediately after installation.

Your downloaded package has a long encoded filename. The token is that filename with `.pkg` removed. Copy it, then:

- Go to **Settings, Computer Management**, then **Scripts**.
- Click **New** and name it something clear, for example Pre-Install, Desktop Connect Config.
- On the Script tab, paste the following, replacing the placeholder with your token.

```
#!/bin/sh

PKG_BASENAME="<YOUR_TOKEN>"

echo "$PKG_BASENAME" | 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.

STEP 4: CREATE THE DEPLOYMENT POLICY

4

Tie the script and package together

One policy per architecture

Go to **Computers**, then **Policies**, and click **New**.

GENERAL PAYLOAD

- **Display Name:** Install Prodoscore Desktop Connect
- **Trigger:** Enrollment Complete and Recurring Check-in
- **Execution Frequency:** Once per computer

SCRIPTS PAYLOAD

- Configure and add your pre-install script.
- Set **Priority** to **Before**. The configuration has to be written before the package installs.

PACKAGES PAYLOAD

- Configure and select your uploaded package.
- Set **Action** to **Install**.

SCOPE

Assign to the Smart Group matching this package's architecture, then save.

AFTER DEPLOYMENT

5

The agent needs a login event to start

This catches people out

After installation the agent waits for a login, or a lock and unlock cycle, before it starts. A Mac that is installed and then left untouched will not report, however long you wait.

In practice this happens on its own the next time the person locks their screen or signs in. If you need it sooner, a restart is the quickest route.

6

Verify the deployment

Check the files, not just the portal

A device should appear in the Desktop Connect Admin Console within roughly 30 minutes of the install completing, once a user has logged in. If it has not, check these on the machine:

PATH	WHAT IT CONFIRMS
<code>/Library/Preferences/zs.json</code>	The script ran and the license key is in place. Should be readable JSON, not empty.
<code>/usr/local/zs/zs.app/Contents/MacOS/version.txt</code>	The package installed and wrote its files.

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 AND NETWORK

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

- `/usr/local/zs/`
- `~/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.prodoscure.com`
- **Licensing:** `origin.hrsaastech.com`
- **Storage:** `storage.googleapis.com`

If your security policy requires explicit subdomains rather than a wildcard, use `api.ag.prodoscure.com`, `auth.ag.prodoscure.com`, `portal.ag.prodoscure.com`, and your own `<base_domain>.ag.prodoscure.com`. Your base domain is the text immediately before `.ag.prodoscure.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 SOMETHING GOES WRONG

WHAT YOU SEE	MOST LIKELY CAUSE
Policy ran, device never appears	Check <code>zs.json</code> first. If it is missing or empty, the script did not run or the token was wrong.
App present, config present, nothing ever runs	Wrong architecture package. An Intel Mac cannot run Apple Silicon binaries, and there is no fallback.
Device registers but no activity is recorded	The Permissions profile did not apply. Confirm it deployed and is scoped to that machine.
Files disappear after a successful install	Endpoint protection has quarantined them. Add the exclusions and reinstall.
Nothing happens on a particular Mac	Check the macOS version. Anything earlier than macOS 13 Ventura is not supported.
Install needs to be redone	Installing over a broken installation rarely works. Ask Prodoscore for the macOS cleanup utility, run it, restart, then deploy again.

QUICK REFERENCE

ITEM	VALUE
Supported MDM	Jamf Pro
Architectures	Apple Silicon and Intel, separate packages and tokens
Configuration profiles	Two, Permissions and Notifications, both before the package
Installer format	.pkg
Pre-install script	Required, priority Before
Install path	<code>/usr/local/zs/zs.app</code>
Tenant config	<code>/Library/Preferences/zs.json</code>
Minimum macOS	13 Ventura
Agent start	After a login or a lock and unlock cycle
Time to appear	Within 30 minutes of install, after a user logs in

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