

DEVICE TRUST PASSPORT

User Installation & Entra ID Registration Guide

Document Info	
Version	3.0
Last Updated	March 2026
Audience	End Users / Contractors
Time Required	10–15 minutes
Platforms	Windows 10/11 & macOS

Table of Contents

Table of Contents	2
Overview	3
How It Works	3
Before You Begin	4
Requirements for All Platforms.....	4
Platform-Specific Requirements	4
Windows: Device Registration.....	5
Register Your Device	5
Install the Device Trust Passport App	6
MacOS: Device Registration	7
Pre-Registration: Remove Old Workplace Certificate (If Applicable).....	7
Register Your Device	7
Install the Device Trust Passport App	8
First-Time Login: Safari Certificate Prompt.....	8
Troubleshooting	9
Frequently Asked Questions	10
Getting Help	11

Overview

The Ensure Device Trust Passport is a lightweight application that verifies your device meets your organization’s security requirements before granting access to corporate resources such as Microsoft 365, internal applications, and sensitive data.

This guide walks you through two simple tasks: registering your device with Microsoft Entra ID (formerly Azure AD) and installing the Device Trust Passport application. The entire process typically takes 10–15 minutes.

How It Works

Once installed, the Device Trust Passport runs a series of automated security checks on your device and reports the results to your organization. Your IT administrator has defined which checks are required. Common checks include:

Security Check	What It Verifies
Anti-Malware	An active, up-to-date antivirus or anti-malware solution is running
Disk Encryption	Your hard drive is encrypted (BitLocker on Windows, FileVault on Mac)
Firewall	The operating system firewall is enabled and active
Lock Screen	A screen lock is configured to activate after inactivity
Passphrase	Your device requires a password or passphrase to unlock
No Remote Access	No unauthorized remote access tools are running
OS Updates	Your operating system is up to date with recent patches

NOTE

The Device Trust Passport does NOT install management software on your personal device. It does NOT give your organization the ability to wipe, monitor, or control your device. It only reports whether specific security settings are enabled.

Before You Begin

Confirm you have the following items ready before starting. If anything is missing, contact your organization’s IT administrator.

Requirements for All Platforms

Requirement	Details
Entra ID Account	Your organization must have provisioned a Microsoft Entra ID (Azure AD) account for you. You will sign in with your organizational email and password.
Internet Connection	A stable internet connection is required throughout the registration process.
Admin Rights	NOT required. The Device Trust Passport installs without local administrator privileges on both Windows and Mac.

Platform-Specific Requirements

Windows 10 / 11	macOS
<ul style="list-style-type: none"> • Microsoft Edge or Google Chrome • Access to Windows Settings 	<ul style="list-style-type: none"> • Apple Safari (required for registration) • Microsoft Intune license (temporary — provided by your org, needed only during registration) • Keychain Access (pre-installed on all Macs)

⚠ IMPORTANT

Mac users: During registration, your organization will temporarily assign a Microsoft Intune license to your account. This license is only needed to complete the device registration step and can be removed afterward. It does NOT install mobile device management on your Mac.

Windows: Device Registration

This section covers registering your Windows PC with Microsoft Entra ID. Registration is a one-time process per device.

Register Your Device

Step 1: Open Windows Settings. Click the Start menu and select the gear icon labeled “Settings.”

On Windows 10, Settings appears in the left sidebar of the Start menu.

On Windows 11, it's pinned to the Start screen or searchable.

Step 2: Navigate to Accounts → Access work or school.

In the Settings app, click “Accounts” in the left panel, then select “Access work or school” from the list.

Step 3: Click the “Connect” button.

This opens the “Add a work or school account” dialog. You may also see a “+” icon next to “Add a work or school account.”

Step 4: Sign in with your organizational credentials.

Enter the Microsoft 365 email address and password provided by your organization.

Complete any multi-factor authentication (MFA) prompts if required.

Step 5: Verify registration.

Once complete, your organizational account will appear listed under “Access work or school.” You should see your organization’s name and email address displayed.

 **TIP**

If your account already appears under “Access work or school,” your device is already registered. You can skip ahead to the app installation section.

Install the Device Trust Passport App

Step 1: Download the application from one of these sources:

- *Ensure website: ensureendpoint.com/download-ensure-clients/*
- *Microsoft Store (search "Ensure Device Trust Passport")*
- *Your organization's internal software portal (if applicable)*

Step 2: Run the installer and follow the on-screen prompts.

No administrator rights are needed. The installer will complete in under a minute.

Step 3: Launch the application and verify your security status.

After installation, open the Device Trust Passport from your Start menu or system tray. The app will display a dashboard showing your security check results with green checkmarks for passing items and red X marks for items that need attention.

Step 4: Resolve any failing checks.

If any security checks show a red X, the app will provide guidance on how to fix the issue (for example, enabling BitLocker encryption or turning on the Windows Firewall). Resolve each issue and click "Recheck" to update your status.

 **TIP**

Click "Recheck" at any time to refresh your security status. The app also runs periodic background checks automatically.

MacOS: Device Registration

Mac registration requires a few additional steps compared to Windows, including using the Microsoft Company Portal app and, in some cases, removing a previous workplace certificate. Follow each step carefully.

Pre-Registration:

Remove Old Workplace Certificate (If Applicable)

If your Mac was previously registered to another organization, the old certificate must be removed before you can register again. This is a safe operation and only removes the workplace connection — it does not affect any of your personal data, applications, or settings.

- Step 1:** Open Keychain Access. Go to Applications → Utilities → Keychain Access.
- Step 2:** Select the “Certificates” tab in the top menu bar.
- Step 3:** Look for a certificate named “Microsoft Workplace Join Key.” It may be nested under a string of characters — click the disclosure arrow to expand entries if needed.
- Step 4:** Right-click the certificate and select “Delete.” Confirm the deletion when prompted.
- Step 5:** Close Keychain Access.

Register Your Device

- Step 1:** Download the Microsoft Company Portal app.
Download from Microsoft: <https://go.microsoft.com/fwlink/?linkid=853070>
- Step 2:** Install the Company Portal app by opening the downloaded .pkg file and following the prompts.
- Step 3:** Open the Company Portal app from your Applications folder and click “Sign In.”
- Step 4:** Sign in with your organizational email and password. Complete any MFA prompts.
- Step 5:** A dialog titled “Set up [Your Organization] access” will appear. Click “Begin” to start the registration process.
- Step 6:** Wait for registration to complete. You will see a progress indicator showing “Registering your Mac.”

 **IMPORTANT**

Once registration completes, CLOSE the Company Portal app. Do NOT proceed with installing a Management Profile — this is not required for the Device Trust Passport and should be skipped.

Install the Device Trust Passport App

Step 1: Download the application from one of these sources:

- *Ensure website: ensureendpoint.com/download-ensure-clients/*
- *Your organization's internal software portal*

Step 2: Install the app by opening the downloaded file and dragging it to Applications.

Step 3: Launch the Ensure app from Applications to view your security status.

Step 4: Click "Refresh" to run an immediate security assessment.

First-Time Login: Safari Certificate Prompt

The first time you access organizational resources through Safari after registration, you will see a dialog asking Safari to use the "Microsoft Workplace Join Key" from your keychain.

Step 1: Enter your Mac's local login password (the password you use to unlock your Mac).

Step 2: Click "Always Allow" to avoid being prompted at every future login. If you choose "Allow" instead, you will need to authorize access each time you sign in.

TIP

Choosing "Always Allow" is recommended for convenience. It simply permits Safari to use the workplace certificate without asking for your password each time. It does not change any security settings on your device.

Troubleshooting

If you encounter issues during registration or installation, review the common scenarios below before contacting support.

Issue	Resolution
“Connect” button is grayed out (Windows)	Ensure you are connected to the internet and that no other work or school account is already connected. Try restarting the Settings app.
Registration fails with an error (Windows)	Verify your credentials are correct. If MFA is required, ensure your authenticator app is set up. Contact your IT administrator if the error persists.
Mac won’t register — “Device already registered”	You likely have a previous Workplace Join certificate. Follow the certificate removal steps in Section 4 above, then retry registration.
Company Portal asks to install a Management Profile	Do NOT install the Management Profile. Close the Company Portal app immediately after registration completes. The Device Trust Passport does not require a management profile.
Security check shows a red X after installation	The app provides specific guidance for each failing check. Common fixes include: enabling BitLocker/FileVault, turning on the firewall, installing OS updates, or configuring a lock screen.
App won’t open or crashes on launch	Ensure your OS meets minimum requirements (Windows 10+ or macOS 10.15+). Try re-downloading and reinstalling the application.
Safari certificate prompt keeps appearing (Mac)	You may have selected “Allow” instead of “Always Allow.” Open Keychain Access, find the “Microsoft Workplace Join Key,” double-click it, expand “Access Control,” and add Safari to the allowed applications list.

Frequently Asked Questions

Does the Device Trust Passport give my organization control over my personal device?

No. The app only checks whether certain security settings are enabled. It does not install management software, and it cannot remotely wipe, lock, or monitor your device.

Do I need to keep the Company Portal app installed on my Mac after registration?

The Company Portal app is only needed for the initial registration. You may uninstall it after registration is complete, though keeping it installed will not affect your device.

What happens if my device fails a security check?

You may be blocked from accessing certain organizational resources until the issue is resolved. The Device Trust Passport app will tell you exactly which check failed and how to fix it.

Do I need to register my device again if I reinstall Windows or macOS?

Yes. A full OS reinstall removes the device registration. You will need to repeat both the Entra ID registration and the Device Trust Passport installation.

Can I register multiple devices?

Yes. Each device must be registered individually by repeating the steps in this guide on each device you intend to use for work.

Does this work with browsers other than Edge, Chrome, or Safari?

For Windows, Microsoft Edge or Google Chrome are required for the Conditional Access integration. Firefox is not currently supported. For Mac, Safari is required for the initial registration and first login.

Getting Help

If you've reviewed the troubleshooting section and still need assistance, use the following resources:

Resource	Contact
Your IT Administrator	For account access, MFA setup, Intune licensing, and organizational policy questions
Ensure Support	support@ensureendpoint.com — for issues with the Device Trust Passport application itself
Ensure Website	www.ensureendpoint.com — for downloads, documentation, and product updates
