Technical Note

Admin By Request
ZERO TRUST PLATFORM

Product Platform: **Mac**
Product Version: **5.2 +**
Document Date: **2 November 2026**
Document Version: **1.2**
Classification: **Public**

Configuring Platform SSO for macOS

Introduction

Admin By Request (ABR) manages privilege elevation on macOS by applying policies to users based on which group they belong to in the organisation's Identity Provider (IdP) - typically Microsoft Entra ID or Okta. To do that, ABR needs to know who is actually logged in to the Mac in corporate identity terms: not just the local macOS account name, but the user's corporate email address or User Principal Name (UPN) that the IdP recognises.

Platform SSO is Apple's solution for binding macOS login directly to a corporate IdP. When it is configured, the macOS login screen itself authenticates against Entra ID or Okta, and the OS stores the resulting identity in a system location that trusted applications can read. ABR reads that identity at the top of its lookup chain, before any application-based fallback is consulted. As long as the user has completed Platform SSO registration on their device, ABR gets a reliable, fresh UPN on every check - which in turn means Sub-Settings apply correctly and consistently.

This technical note explains what Platform SSO requires, how to configure it end-to-end for both Entra ID and Okta environments, how to verify that it is working, and what to do when it is not.

Applies to: macOS [Entra ID: ABR v5.1+, Okta: ABR v5.2+]

This technical note is available online:

Configuring Platform SSO on macOS

In this technical note

- "Background: What is Platform SSO?" below
- "How ABR uses Platform SSO - the identity lookup chain" on the next page
- "Entra ID vs Okta: an important difference" on page 4
- "Prerequisites" on page 5
- "Configuration" on page 6
  - "Step 1 - Deploy the Full Disk Access (PPPC) profile" on page 6
  - "Step 2 - Deploy the Extensible SSO (ESSP) profile" on page 9
  - "Step 3 - Verify the IdP selection" on page 12
  - "Step 4 - Deploy the ABR agent" on page 13
  - "Step 5 - Have users complete Platform SSO registration" on page 13
- "Verifying the configuration" on page 14
- "Common issues" on page 15
- "Diagnostic logs" on page 19

Background: What is Platform SSO?

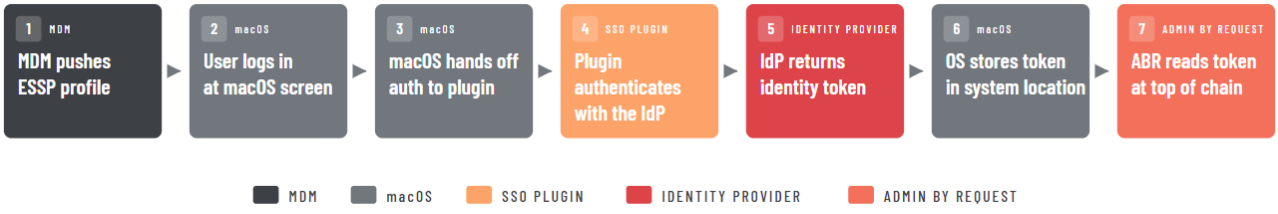
Platform SSO is an Apple capability introduced in macOS 13 Ventura that allows the macOS login screen to authenticate against a corporate IdP rather than against a local password. Instead of the user typing in a password stored only on their Mac, the macOS login dialog hands the authentication challenge off to an SSO plugin - provided by Microsoft (for Entra ID) or Okta - which authenticates the user with the IdP and receives back an identity token. macOS stores that token in a system location and makes it available to applications that are registered as trusted consumers.

The mechanism that delivers the SSO plugin to a Mac is a configuration profile called an Extensible Single Sign-On Profile (ESSP). This profile is pushed to devices via Mobile Device Management (MDM) - Intune or Jamf in most ABR environments. Once the profile is installed and the user has completed the initial registration flow (which typically happens at their next macOS login), Platform SSO is active and the OS-level identity token is available.

ABR does not configure Platform SSO itself. There is no toggle for it in the ABR portal. ABR's role is to read the Platform SSO identity attributes exposed by macOS on the local user record. Whether a token exists depends entirely on the MDM configuration and on whether the user has completed registration.

How the identity token reaches ABR

Step 1 is setup, once per device and steps 2-7 run at every user login. By design, ABR never participates in authentication - it's a *consumer* at the end of the pipeline, not a participant.



How ABR uses Platform SSO - the identity lookup chain

When ABR needs to identify the currently logged-in user, it works through a fixed priority list of identity sources - called the identity lookup chain - and stops at the first source that returns a usable UPN. The chain, from highest to lowest priority, is:

1. **Platform SSO** - The OS-level identity token from the SSO plugin. Used when an ESSP profile is deployed and the user has authenticated through it. This is the most reliable source, because the OS holds the identity rather than any specific application.
2. **Microsoft Intune Company Portal** - The plist file written to disk when the user signs in to Company Portal.
3. **Microsoft Outlook** - The preferences file that Outlook writes when the user is signed in to their Microsoft account.
4. **Microsoft Teams** - The Teams settings file. Requires Full Disk Access because Teams stores its data in a sandboxed container.
5. **Jamf Connect** - Jamf's credential provider plugin, used in Jamf-only environments that do not have Microsoft applications installed.

ABR checks these in order and uses the first source that returns a non-empty UPN. This order is fixed - it cannot be changed by configuration.

Identity lookup is not the same as trust for MFA. Every source in the chain can supply a UPN that Admin By Request uses to look the user up. That does not make the UPN trusted for MFA *Email match*. In particular, signing in to Outlook or Teams lets those apps supply a UPN for lookup, but it does not make that UPN trusted for *Email match*.

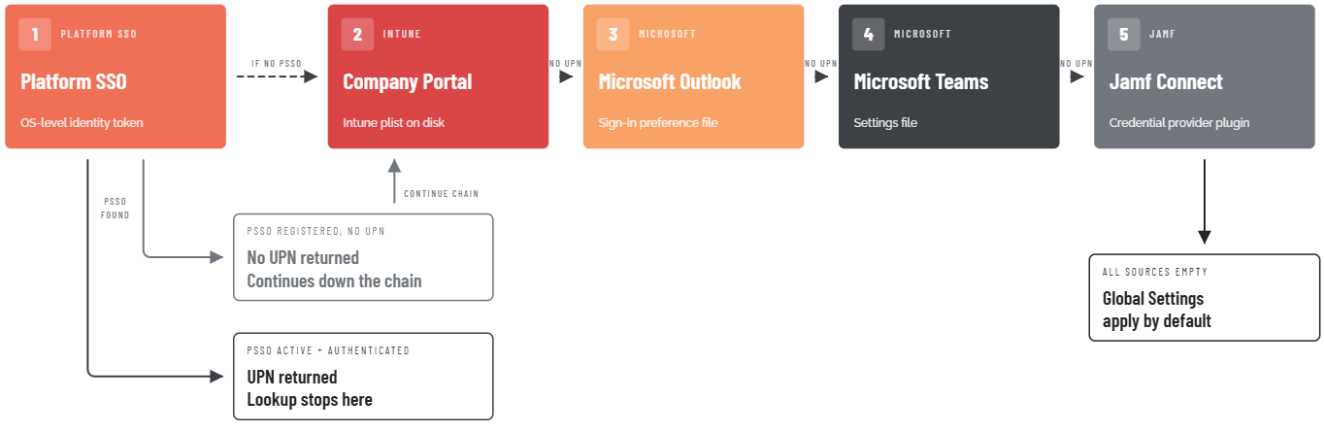
From macOS client version 6.0, *Email match* needs a trusted identity tied to the local Mac user: either a registered Platform SSO identity, or a UPN verified through the Entra ID Connector. Platform SSO needs configuration and user registration, but no Entra ID Connector, for this purpose. See Platform SSO as an identity source for Email match.

Platform SSO being registered on the device is not enough on its own to end the lookup. **If Platform SSO is registered but returns no UPN** - for example because the user has not yet completed Platform SSO authentication - **Admin By Request continues down the chain** to Company Portal and the other sources, exactly as if Platform SSO were not registered. Only a returned UPN ends the lookup at step 1.

In practice, on Entra ID a user who has not completed registration can still be identified from Company Portal, Outlook or Teams, provided they are signed in to one of them. On Okta none of the later sources carries Okta identity, so the user gets Global Settings until registration is complete.

Five sources, in fixed priority order

ABR stops at the first source returning a UPN. Platform SSO is checked first - a returned UPN ends the lookup, but a registration with no UPN falls through to the next source.



Entra ID vs Okta: an important difference

Both Entra ID and Okta environments use the same Platform SSO mechanism described above. The configuration steps are nearly identical. However, there is a fundamental difference in what happens when Platform SSO is not working:

- **Entra ID environments:** Platform SSO is the preferred identity source, but it is not strictly required. If Platform SSO is not configured on a device at all, ABR falls through to Company Portal, Outlook, and Teams - all of which can supply an Entra ID identity. ABR can identify most Entra ID users without Platform SSO. Platform SSO makes this identification more reliable and consistent, but it is not mandatory.

  There is one exception, from macOS client version 6.0. MFA *Email match* does not trust a UPN supplied by Outlook or Teams. If you use *Email match* without the Entra ID Connector, Platform SSO is the only trusted identity source, so it becomes a requirement for those users.
- **Okta environments:** Platform SSO is an essential requirement. The entire fallback chain below Platform SSO (Company Portal, Outlook, Teams, Jamf Connect) consists of Microsoft and Jamf applications. None of them carry Okta identity data. If Platform SSO is not configured, or is registered but unauthenticated, ABR has no way to discover the user's Okta identity and cannot match any Okta-group-based Sub-Setting. The official product documentation states this explicitly: "It is a requirement for using the Okta Connector with Macs that users login to their Mac devices using Platform SSO."

This means that for Okta deployments, any gap in Platform SSO coverage - an ESSP profile not deployed to a device, a user who has not completed registration, an ESSP profile misconfigured without the ABR allow-list entry - results directly in users getting Global Settings with no fallback. The operational risk of a misconfigured or partially deployed Platform SSO is higher in Okta environments than in Entra ID environments.

The following table illustrates the differences:

	Entra ID	Okta
Introduced	Mac agent v5.1	Mac agent v5.2
Platform SSO required?	No - fallbacks exist via Microsoft apps	Yes - no Okta-capable fallbacks
If PSSO registered but returns no UPN	Falls through to Company Portal, Outlook, Teams	Falls back to Global Settings
If PSSO not configured at all	Falls through to Company Portal, Outlook, Teams	Falls back to Global Settings
MFA Email match (macOS client 6.0+)	Needs Platform SSO or the Entra ID Connector - an Outlook or Teams UPN is not trusted	Needs Platform SSO
Group query mechanism	Entra ID Connector (Microsoft Graph API)	Okta Connector (Okta REST API)

Prerequisites

Before starting configuration, confirm that all of the following are in place:

	Requirement	Detail
Mac and MDM requirements	macOS version	Platform SSO itself needs macOS 13 Ventura or later (Microsoft's Smart Card authentication method needs macOS 14 or later, and Okta's Desktop Password Sync needs macOS 14 Sonoma or later). The Admin By Request macOS client version 6.0 supports macOS 15 Sequoia, macOS 26 Tahoe and macOS 27. Check the client's system requirements for the version you deploy.
	Microsoft Company Portal (Entra ID)	Version 5.2404.0 or later, deployed to the Mac. Company Portal installs the Microsoft Enterprise SSO plug-in that Platform SSO uses, and Microsoft states that Platform SSO fails with older versions.
	Okta Verify (Okta)	Okta Verify, deployed to the Mac. It provides Okta's Platform SSO extension (Desktop Password Sync).
	MDM platform	Microsoft Intune or Jamf Pro. The device must be MDM-managed because configuration profiles can only be deployed via MDM - users cannot install them manually.
	ABR agent version	v5.1 or later for Entra ID environments; v5.2 or later for Okta environments. Version 6.0 or later to use Platform SSO as the trusted identity for MFA *Email match*.

	Requirement	Detail
ABR portal requirements	Entra ID Connector	Required for Entra ID environments. ABR uses this connector to call the Microsoft Graph API and retrieve the user's Entra ID group memberships once it has their UPN from Platform SSO. If the connector is already configured for Windows endpoints in the same portal, it is shared across platforms - no additional configuration is needed for macOS.
	Okta Connector	Required for Okta environments. ABR uses this connector, with an Okta API token, to call the Okta REST API and retrieve the user's Okta group memberships. Also shared across platforms if already configured for Windows.
User requirements	Platform SSO registration	The user must complete the Platform SSO registration flow on their device before ABR can read their identity. This typically happens automatically at the next macOS login after the ESSP profile is deployed, but may require the user to open Company Portal (Entra ID) or respond to an on-screen prompt (Okta) to complete registration. Until registration is complete, no identity token exists for ABR to read.

With ABR portal requirements, neither connector needs a separate macOS-specific configuration. Platform SSO is auto-detected by ABR at the device level - there is no toggle to enable it in the portal.

Configuration

The configuration has five steps:

1. "Step 1 - Deploy the Full Disk Access (PPPC) profile" below
2. "Step 2 - Deploy the Extensible SSO (ESSP) profile" on page 9
3. "Step 3 - Verify the IdP selection" on page 12
4. "Step 4 - Deploy the ABR agent" on page 13
5. "Step 5 - Have users complete Platform SSO registration" on page 13

Step 1 - Deploy the Full Disk Access (PPPC) profile

ABR requires Full Disk Access (FDA) for macOS identity-related reads and application fallback sources. Platform SSO identity is resolved from local identity attributes and App SSO status metadata.

Recommended: use the ABR-supplied EPM mobileconfig

ABR ships a ready-made `Admin By Request - EPM.mobileconfig` profile that grants Full Disk Access to the ABR app and System Extension, pre-approves the System Extension, and grants Accessibility - all in one profile. It also grants the `SystemPolicySysAdminFiles` privacy service and manages the Admin By Request login items, so it gives the agent everything it needs in one place.

Download it (with the SRA companion file) from https://docs.adminbyrequest.com/resources/ConfigFiles/AdminByRequest-MDM-Config.zip, then deploy the EPM profile via your MDM to the target Mac group. Most customers will use this bundle rather than build the PPPC profile by hand. See Multiple endpoint installation in the install docs for the full MDM walkthrough.

Alternative: build the PPPC profile by hand

If your environment requires you to manage the profile directly rather than deploy the Admin By Request-supplied profile, build a PPPC profile with the values below. MDM consoles change where they show these settings more often than the values themselves change, so this section gives the values and the Apple payload keys they belong to, followed by short pointers for Intune and Jamf Pro.

Note that **both** the main Admin By Request executable and the System Extension need an entry, and that they are identified differently: the main executable by its **path**, and the System Extension by its **bundle ID**. This matches the shipped `Admin By Request - EPM.mobileconfig` profile. Each entry also needs its **code requirement**, which macOS uses to check that the binary really is signed by Admin By Request.

Entry	Identifier	Identifier type	Code requirement
Admin By Request (main executable)	`/Library/adminbyrequest/adminbyrequest`	Path	`identifier "com.fasttracksoftware.adminbyrequest" and anchor apple generic and certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = AU2ALARPUP`
Admin By Request System Extension	`com.fasttracksoftware.adminbyrequest.extension`	Bundle ID	`anchor apple generic and identifier "com.fasttracksoftware.adminbyrequest.extension" and (certificate leaf [field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1 [field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf [field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf [subject.OU] = AU2ALARPUP)`

In each entry, allow **Full Disk Access**. In the Apple payload (`com.apple.TCC.configuration-profile-policy`) this is the `SystemPolicyAllFiles` service.

NOTE
The shipped profile does more than grant Full Disk Access. It also grants the `SystemPolicySysAdminFiles` and `Accessibility` services, approves the System Extension, and manages the Admin By Request login items. A hand-built profile that grants only Full Disk Access is not equivalent to it, which is another reason to use the shipped profile where you can.

Intune steps

For Intune, do the following:

1. In the Intune admin centre, go to **Devices > Manage devices > Configuration > Create > New policy**.
2. Select **macOS** as the platform and **Settings catalog** as the profile type.
3. In **Configuration settings**, select **Add settings** and search for **Privacy Preferences Policy Control**.
4. Add the two entries from the table above, each with its identifier, identifier type and code requirement, and allow Full Disk Access (System Policy All Files) for both.
5. Assign the profile to the device group containing your Mac devices.
6. Save and deploy. In the portal, verify that the profile status shows as **Succeeded** for target devices before proceeding to Step 2.

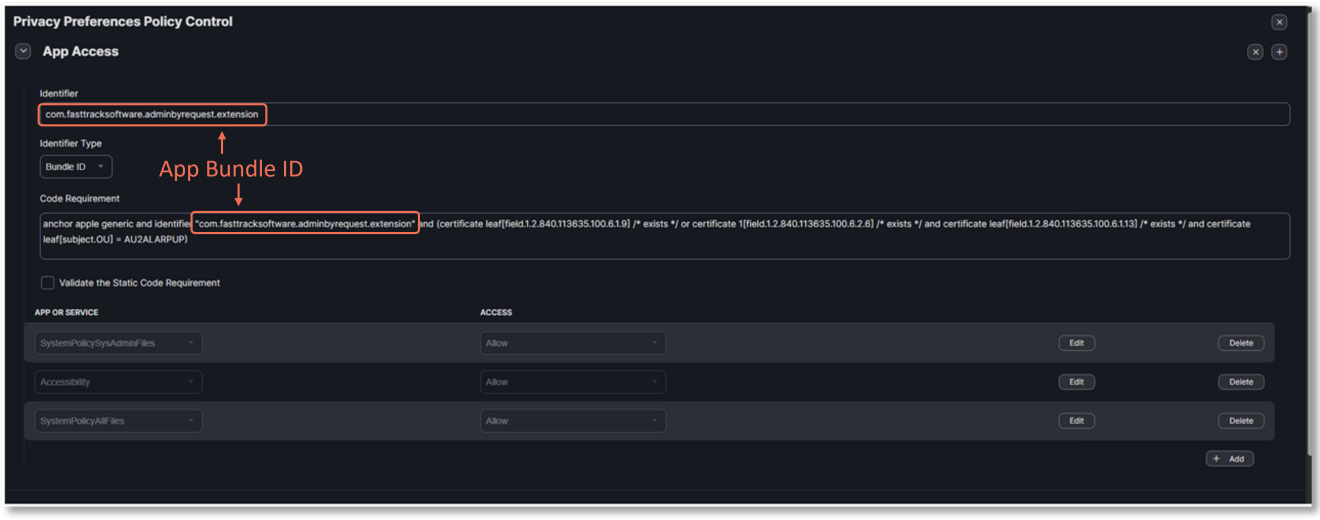
> **NOTE**
> Older guides build this profile from the **Device restrictions** template (**Privacy preferences** section). Microsoft no longer updates that template and recommends the settings catalog for all new policies. Existing template-based profiles continue to work.

Jamf Pro steps

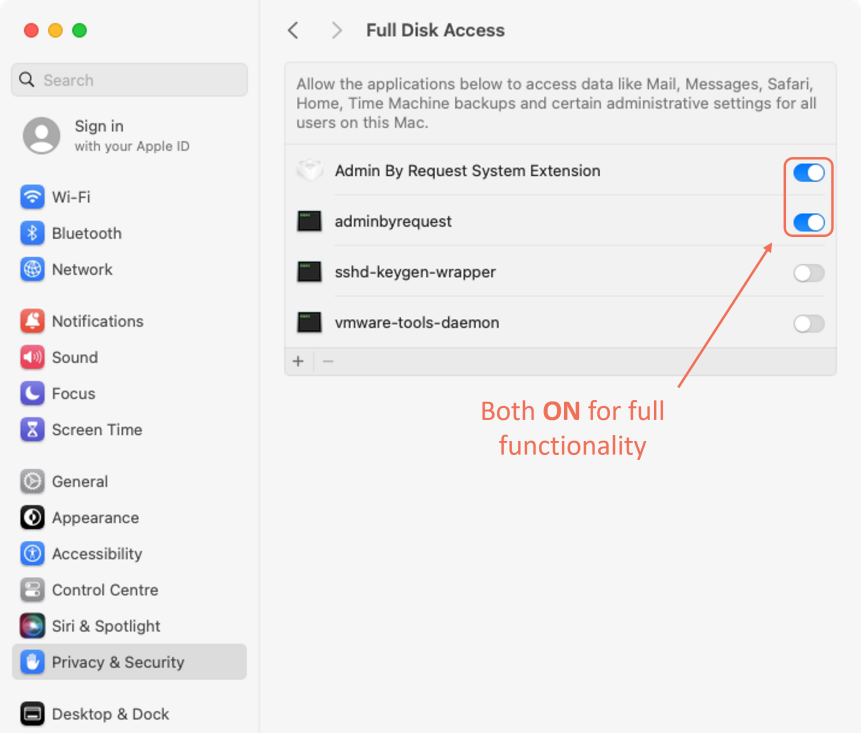
For Jamf, do the following:

1. In Jamf Pro, go to **Computers > Configuration Profiles > New**.
2. Add a **Privacy Preferences Policy Control** payload.
3. Click **+** to add an application entry for the main executable:
   - Identifier: `/Library/adminbyrequest/adminbyrequest`
   - Identifier Type: **Path**
   - Code Requirement: the main executable value from the table above
   - Full Disk Access: tick **Allow**
4. Click **+** again to add a **second** application entry for the System Extension:
   - Identifier: `com.fasttracksoftware.adminbyrequest.extension`
   - Identifier Type: **Bundle ID**
   - Code Requirement: the System Extension value from the table above
   - Full Disk Access: tick **Allow**
5. Set the scope to the relevant computer group and save.

This example shows the App Bundle ID for the ABR System Extension in Jamf:



To verify that FDA has been granted on a device, go to **System Settings > Privacy and Security > Full Disk Access** on the Mac and confirm that **both** `adminbyrequest` and `Admin By Request System Extension` are listed with their toggles on:



macOS 26.1 / 26.2

On macOS 26.1 and 26.2, the privacy settings picker can fail to list binaries even when they are present. This problem is fixed in macOS 26.3 and later. If you are configuring or verifying FDA on macOS 26.1 or 26.2, drag-and-drop the binary from Finder into the Full Disk Access list as a temporary workaround.

Step 2 - Deploy the Extensible SSO (ESSP) profile

This profile is what tells macOS to use Platform SSO and which SSO plugin to use (Microsoft's for Entra ID, or Okta's). It also controls which applications on the Mac are allowed to access the Platform SSO identity token - and this is where the most commonly missed configuration step lives.

The `AppPrefixAllowList` key in the ESSP profile is a whitelist of application bundle ID prefixes that are allowed to read the Platform SSO token. ABR's bundle IDs start with `com.fasttracksoftware.`, so that prefix must be in the list. If it is missing, the Platform SSO token is available to other applications (including the SSO plugin itself) but not to ABR. ABR will then behave as if Platform SSO is not configured - falling through to application-based sources on Entra ID, or returning Global Settings on Okta.

For Entra ID via Intune

Intune configures Platform SSO with a **settings catalog** policy. Microsoft's guide, Configure Platform SSO for macOS devices, is the reference for the full set of Platform SSO settings and for choosing an authentication method. The steps below summarise it and add what Admin By Request needs.

Already using Platform SSO? Edit your existing policy

Microsoft supports only one SSO policy per device. A second extensible SSO profile conflicts with the first (Microsoft error `10002: multiple SSOe payloads configured`). If Platform SSO is already deployed, add the `AppPrefixAllowList` key in step 3 to that policy rather than creating a new one.

Do the following:

1. In the Intune admin centre, go to **Devices > Manage devices > Configuration > Create > New policy**. Select **macOS** as the platform and **Settings catalog** as the profile type.
2. In **Configuration settings**, select **Add settings**, expand **Authentication**, select **Extensible Single Sign On (SSO)**, and configure the settings Microsoft lists as required. The values that identify Microsoft's SSO extension are:
   - Extension Identifier: `com.microsoft.CompanyPortalMac.ssoextension`
   - Team Identifier: `UBF8T346G9`
   - Type: **Redirect**, with the URLs listed in Microsoft's guide
   - Registration Token: `{{DEVICEREGISTRATION}}` (including the curly braces)

   Microsoft's guide also covers the Platform SSO authentication method (Microsoft recommends Secure Enclave), Use Shared Device Keys, Token To User Mapping and Screen Locked Behavior.
3. In the same **Extensible Single Sign On (SSO)** category, add the **Extension Data** setting and add the following key:
   - Key: `AppPrefixAllowList`
   - Type: String
   - Value: `com.apple.,com.microsoft.,com.fasttracksoftware.`

   Setting this key **replaces** the Microsoft SSO plug-in's default list rather than adding to it. Microsoft documents the macOS default as `com.apple.` and `com.microsoft.`, so keep both in the value alongside the Admin By Request prefix. If the key already exists in your policy, append `com.fasttracksoftware.` to its comma-separated value instead of adding a second key. Keep the trailing period on every prefix.

   The ESSP profile is also where you enable **YubiKey** and **smartcard authentication** for ABR's MFA prompt on macOS.

   This works out of the box on Windows but requires two additional Extension Data keys on Mac - `browser_sso_interaction_enabled=1` and `disable_explicit_app_prompt_and_autologin=1`, both Integer - alongside the `AppPrefixAllowList` entry described above. The same two keys also enable Entra Conditional Access policies that restrict login by operating system to recognise macOS MFA logins.

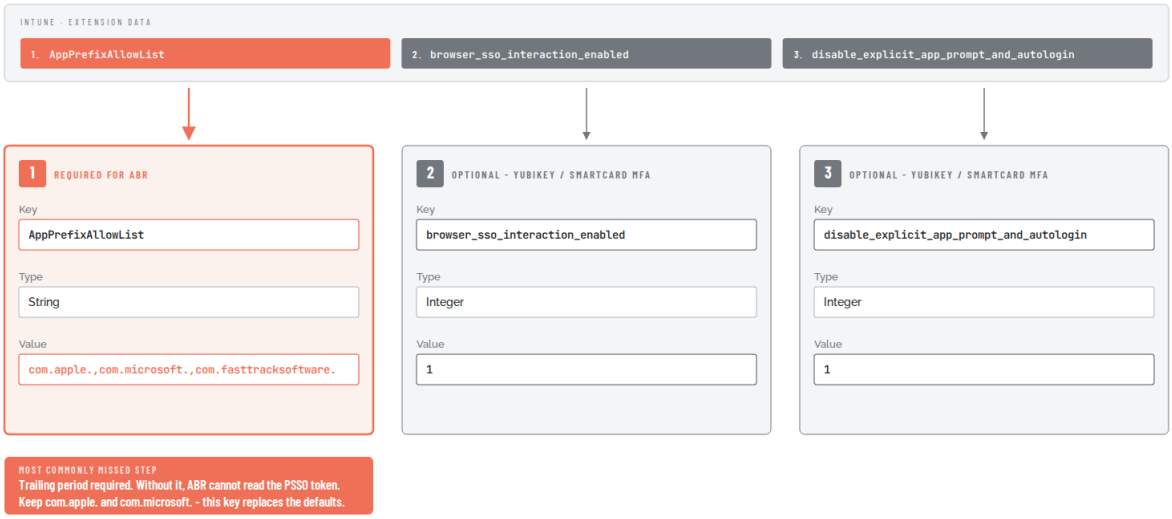
   Refer to YubiKey / Smartcard Authentication in macOS for more information.
4. Assign the policy. For Macs that have a primary user (user affinity), assign it to **users or user groups**: Microsoft does not support device group assignment of Platform SSO on those devices. Use device groups only for shared Macs enrolled without user affinity. This can be a different group from the one used in Step 1.

5. Once the new policy is working, unassign any older SSO app extension profile created with the Intune **Device features** template, so that the two do not conflict.

> **NOTE**
> Earlier versions of this technical note pointed to the Intune **Templates > Extensions** profile type. That template is deprecated, and it configures kernel and system extensions rather than SSO. Use the settings catalog as described above.

Three Extension Data keys, one critical value

In the Intune settings catalog policy, add these three keys under Extension Data. Key 1, the `AppPrefixAllowList` entry is the one customers most often miss - this is the key that lets ABR in (and don't forget the trailing period). Keys 2 and 3 are needed only for YubiKey and smartcard authentication and for Conditional Access policies that restrict login by operating system, as described above. Microsoft's own defaults are `browser_sso_interaction_enabled` = 1 and `disable_explicit_app_prompt_and_autologin` = 0.



For Okta via Intune

Okta's Platform SSO extension is **Desktop Password Sync**, delivered by **Okta Verify**, and it needs macOS 14 Sonoma or later. Okta configures it in Intune with a settings catalog policy, plus associated domains and preference file profiles. Follow Okta's guide, Configure device configuration profiles for PSSO using Microsoft Intune, for the full procedure. The values that identify Okta's extension are:

- Extension Identifier: `com.okta.mobile.auth-service-extension`
- Team Identifier: `B7F62B65BN`
- Type: **Redirect**

The `AppPrefixAllowList` requirement is the same as for Entra ID: the value must include `com.fasttracksoftware.`, added to the extension data of the same SSO policy.

For Jamf Pro (Entra ID or Okta)

Do the following:

1. In Jamf Pro, go to **Computers > Configuration Profiles > New**.
2. Add a **Single Sign-On Extensions** payload.

3. Add a new extension entry for the relevant IdP (Microsoft or Okta), using the Extension Identifier, Team Identifier and Type given above. Configure the remaining Platform SSO settings as described in Microsoft's or Okta's Jamf Pro guidance.
4. In the extension data / additional configuration section, add the key `AppPrefixAllowList` with string value `com.apple.,com.microsoft.,com.fasttracksoftware.` for Microsoft, or a value that includes `com.fasttracksoftware.` for Okta. If the key already exists, append to it.
5. Scope the profile to the target computer group and save.

NOTE
The Jamf Pro navigation for SSO Extensions profiles may vary by Jamf Pro version. Consult current Jamf documentation if the path above does not match your interface.

Step 3 - Verify the IdP selection

Once ABR has the user's UPN from Platform SSO, it needs to use that UPN to look up the user's group memberships in the IdP. That lookup happens through (1) the Authentication tab and (2) the identity connector configured in the ABR portal.

In the portal, the Mac-side configuration that affects this is on the EPM macOS Authentication tab (under Mac Settings); the connector itself is managed in Tenant Settings and is shared across platforms.

There is no Platform SSO-specific toggle in the portal - ABR auto-detects Platform SSO from the device state.

Prerequisite: Authentication Mode must be "Multi-factor Authentication"

On the EPM macOS Authentication tab, the Authentication Mode panel offers three mutually-exclusive options: Confirm, Multi-factor Authentication, and Authenticate. The Sign-on method and Email match settings that select the IdP for Platform SSO are only visible when **Multi-factor Authentication** is selected. If the tenant currently has Confirm or Authenticate selected, switch to Multi-factor Authentication first.

On the Authentication tab itself:

1. Log in to the ABR portal.
2. Navigate to **EPM > Settings > Mac Settings > Endpoint > Authentication**.
3. In the **Authentication Mode** panel, confirm **Multi-factor Authentication** is selected.
4. In the **Multi-factor Configuration** panel, confirm:
   - **Sign-on method** is set to the IdP you want ABR to use. The combo lists the SSO methods configured for this tenant (typically Microsoft 365 / Entra ID, plus any ADFS / Okta / SAML methods that have been added). A trailing "-- ADD NEW METHOD --" option opens a separate form for registering a new SSO method.
   - **Email match** is set per your matching policy (No matching / Email match / Account separation). See the on-tab About text for the semantic difference.

The Mac Authentication tab itself does **not** contain the Entra ID Connector or Okta Connector credentials (Client ID, Tenant ID, Client Secret, Okta URL, API token). Those are managed at a different portal location and shared across platforms.

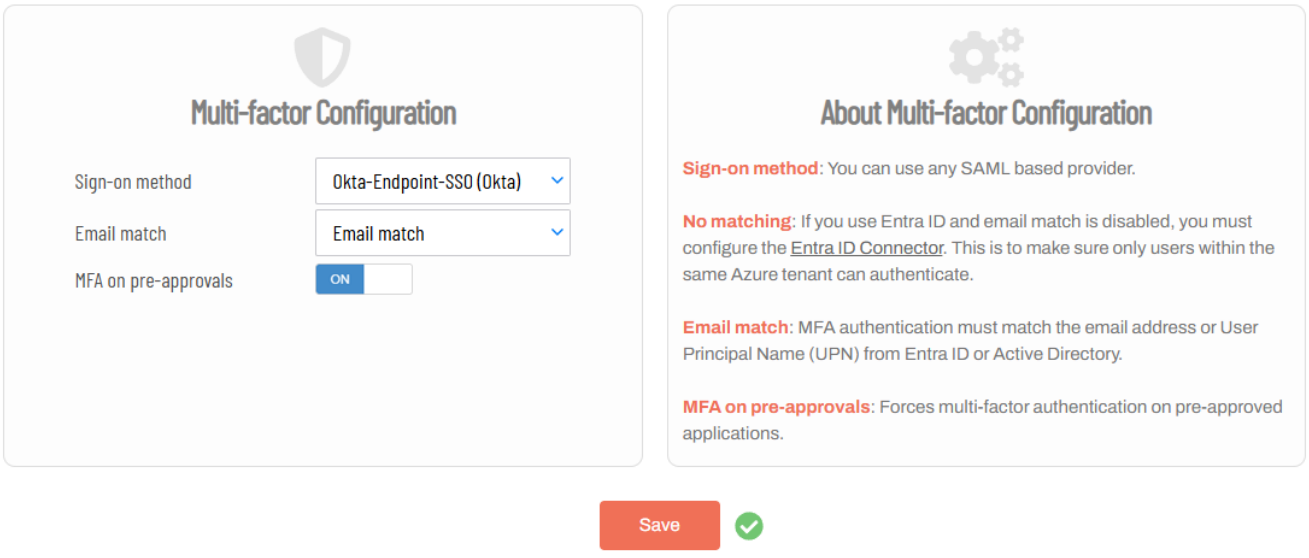
Confirm with your portal administrator that the relevant connector is already configured and connected before proceeding to Step 4. If the connector is not yet configured, follow the standard ABR portal procedure for the relevant IdP:

- **Entra ID:** create an App Registration in Entra ID with `Directory.Read.All` Application permissions, then enter the resulting Client ID, Tenant ID, and Client Secret in the ABR Entra ID Connector page.
- **Okta:** create a token in the Okta Admin Console (Security > API > Tokens > Create token; copy the value at creation time as it is only displayed once), then enter your Okta tenant URL and the token in the ABR Okta Connector page.

Refer to Tenant Settings > Identity for more information on configuring IdP Connectors.

Setting MFA in the portal to your IdP sign-on method

For your *Sign-on method* to appear in the dropdown list, configure it at Entra ID Single-Sign-on or Okta Single-Sign-on, depending on your environment. This example shows **Okta-Endpoint-SSO (Okta)** - a name that was created during the configuration procedure:



Step 4 - Deploy the ABR agent

Deploy the ABR Mac PKG file to devices via MDM only after Steps 1 and 2 are confirmed as complete on target devices. The PKG is available for download from the ABR portal under the macOS installation section. It is tenant-specific: signed with your tenant's licence key - and should not be shared with other organisations.

Confirm that the PPPC profile (Step 1) and ESSP profile (Step 2) show as successfully installed in your MDM before pushing the agent. If the agent arrives before the PPPC profile, Full Disk Access will not be in place when the agent first starts and ABR will log an FDA error. Although the PPPC profile will eventually be installed later, FDA may not be recognised until the device is rebooted.

For the broader MDM deployment picture - including the SRA companion mobileconfig, package signing notes, and Jamf-side policy construction - see Multiple endpoint installation in the install docs.

Step 5 - Have users complete Platform SSO registration

Deploying the ESSP profile is not the same as completing Platform SSO registration. The profile tells macOS how to use Platform SSO, but the user's identity token does not exist until the user has actually authenticated through the Platform SSO flow at least once on that device.

On newly enrolled Macs, registration typically happens the first time the user logs in at the macOS login screen after the ESSP profile is deployed. The macOS login screen may present a different prompt than usual - asking the user to sign in with their corporate credentials rather than their local password.

For Entra ID environments

The most reliable way to trigger and confirm registration is via Company Portal:

1. Open **Microsoft Company Portal** on the Mac and sign in with Entra ID credentials if not already signed in.
2. Watch for a **"Registration required"** notification in macOS Notification Centre. Click it if it appears and follow the sign-in and MFA prompts.
3. After completing registration, click **"About Admin By Request"** in the ABR menu bar icon to trigger an immediate identity sync.

For Okta environments

1. Log out of macOS and log back in. If the ESSP profile is correctly installed, the macOS login dialog should be backed by Okta. Log in with Okta credentials and complete any MFA required by your Okta policy.
2. After logging in, click **"About Admin By Request"** in the ABR menu bar icon to trigger an immediate identity sync.

Include Platform SSO registration in Mac onboarding checklists

Until a user completes registration, Admin By Request cannot identify them through Platform SSO. On Entra ID it falls back to Company Portal, Outlook or Teams, which works only if the user is signed in to one of them, and from macOS client 6.0 a UPN from Outlook or Teams is not trusted for MFA *Email match*. On Okta there is no fallback, so the user gets Global Settings rather than their intended Sub-Setting policy until registration is done.

Verifying the configuration

After completing all five configuration steps, confirm that everything is working before rolling out to additional devices.

1. **Check the Groups tab in portal Inventory.** In the ABR portal, go to Inventory and open the record for a target device. If Platform SSO is active and the identity connector is working, a **Groups** tab will appear in the device record, listing the IdP group memberships that ABR has collected for that device. If the Groups tab is absent entirely, ABR has not been able to collect any group data - something in the configuration chain is broken.
2. **Check the Sub-Settings match view.** Navigate to the Sub-Setting that should apply to your test user and open the **"Who matches this sub-setting?"** view. Confirm that the expected device or user appears in the list.
3. **Trigger a manual sync if needed.** ABR caches group membership data and refreshes it on a four-hour automatic cycle. To verify immediately without waiting, click **"About Admin By Request"** in the ABR menu bar icon on the test device. This triggers an immediate identity check and group lookup.
4. **Test an elevation.** Request an elevation on the test device (for example, try to run an installer that requires admin rights). Confirm that the elevation request is handled according to the Sub-Setting that should apply to that user, not according to Global Settings.

Common issues

The following issues are recorded here:

- "AppPrefixAllowList missing from the ESSP profile" below
- "Platform SSO registered but user not yet authenticated" below
- "Full Disk Access not granted" on the next page
- "ESSP profile configuration errors" on page 17
- "Platform SSO artifacts persist after profile removal" on page 17
- "New combined EPM mobileconfig deployed over old separate profiles" on page 18
- "[Okta only] v5.2.0 and v5.2.1 - device groups fail when HostName and NetBIOS name differ" on page 18

The log messages shown below are examples for reference only. Because we are continuously improving our system diagnostics alongside our support team, the format and text of these logs may change in future client updates.

AppPrefixAllowList missing from the ESSP profile

Symptom:

Platform SSO appears to be working for other applications (for example, the user can sign in to macOS with their corporate credentials), but Sub-Settings are not applying correctly in ABR. The Groups tab in portal Inventory is absent or incorrect. There is no ABR log entry that specifically identifies this as the cause.

Cause:

The ESSP profile does not include `com.fasttracksoftware.` in the `AppPrefixAllowList`. macOS restricts access to the Platform SSO identity token to applications whose bundle ID prefix appears in this list. Without the entry, the token is inaccessible to ABR. On Entra ID environments, ABR will fall through to the application-based sources (Company Portal, Outlook, Teams). On Okta environments, identity resolution fails entirely.

Fix:

1. Open the ESSP configuration profile in your MDM.
2. Locate the Additional configuration or Extension Data section.
3. Add the key `AppPrefixAllowList` with string value `com.fasttracksoftware.` (including the trailing period). With Microsoft's SSO extension, use `com.apple.,com.microsoft.,com.fasttracksoftware.` so the plug-in's default prefixes are kept. If the key already exists, append to its value rather than adding a second key, and add it to the existing SSO profile rather than a new one. See "Step 2 - Deploy the Extensible SSO (ESSP) profile" on page 9.
4. Save the updated profile and push it to devices. The change takes effect on the next MDM sync.

Platform SSO registered but user not yet authenticated

Symptom:

Users are getting "Admin Session denied by policy" or landing on Global Settings despite being in the correct Entra ID or Okta group. The ABR diagnostic log contains a message like:

`Entra ID UPN - macOS Platform SSO enabled, but user has not authenticated`

Cause:

ABR can see that Platform SSO is registered on the device (the ESSP profile has been deployed and macOS has processed it) but the user has not yet completed the authentication flow that creates the identity token. Platform SSO therefore returns no UPN, and Admin By Request continues down the identity lookup chain. The user ends up on Global Settings when none of the later sources supplies a UPN either: always on Okta, and on Entra ID when the user is not signed in to Company Portal, Outlook or Teams. This is the most common issue seen immediately after deploying Platform SSO to a Mac fleet.

Fix:

For Entra ID:

1. Open **Microsoft Company Portal** and sign in.
2. Look for a "Registration required" notification in macOS Notification Centre and follow any prompts.
3. After completing registration, click **"About Admin By Request"** in the menu bar icon to sync immediately.

For Okta:

1. Log out of macOS and log back in using the Okta-backed login screen.
2. Complete any MFA prompted by Okta.
3. Click **"About Admin By Request"** to sync.

Full Disk Access not granted

Symptom:

Sub-Settings are not applying and the ABR diagnostic log contains a message like:

`Entra ID UPN - macOS Platform SSO enabled, but Full Disk Access not enabled`

Cause:

The PPPC profile granting Full Disk Access to ABR was not deployed before the ABR agent, or was deployed but not recognised by macOS until after a reboot. ABR cannot read identity data without FDA.

Fix:

1. On the affected Mac, go to **System Settings > Privacy and Security > Full Disk Access**.
2. Check whether **both** `adminbyrequest` and `Admin By Request System Extension` appear in the list. If either is missing, the PPPC profile is incomplete - FDA is required on both the main executable (path `/Library/adminbyrequest/adminbyrequest`) and the System Extension (bundle ID `com.fasttracksoftware.adminbyrequest.extension`), as in the shipped profile. If either appears but its toggle is off, the profile may be present but not correctly enforced.
3. Verify in MDM that the PPPC profile is assigned to and installed on this device.
4. If the profile is present but FDA is still not applied, reboot the device. macOS sometimes requires a reboot to pick up FDA grants from MDM profiles.
5. On macOS 26.1 or 26.2, if you need to add FDA entries manually as a workaround, drag-and-drop the binary from Finder rather than using the privacy-settings picker (the picker can fail to list binaries on those OS versions; fixed in 26.3).

ESSP profile configuration errors

Symptom:

The ABR diagnostic log contains one or more messages such as:

- `[AppSSO] JSON parsing error for Device Configuration: The data couldn't be read because it isn't in the correct format.`
- `[AppSSO] JSON parsing error for Login Configuration: The data couldn't be read because it isn't in the correct format.`
- `[AppSSO] No extensionIdentifier/accountDisplayName found. Exiting early.`

Cause:

ABR cannot read the ESSP profile configuration at all. This is distinct from the "user has not authenticated" error - it means the configuration profile itself is broken or absent, not just that the user has not registered. Common causes include:

- The ESSP profile was not assigned to this device in MDM (check the assignment scope).
- The profile extension data contains a syntax error.
- For Okta: Okta Verify, which provides Okta's Platform SSO extension, is not installed on the Mac.
- A conflict with another ESSP or SSO configuration profile on the device. For example, an older Intune Device features SSO app extension profile still assigned alongside a settings catalog Platform SSO policy (Microsoft error `10002: multiple SSOe payloads configured`).

Fix:

1. In your MDM, confirm that the ESSP profile is assigned to this specific device and that its status is successful (not pending or failed).
2. Review the profile's extension data configuration for syntax errors.
3. For Okta: confirm that the Okta device management app components are installed and running on the Mac.
4. Check whether any other SSO-related profile is deployed to this device that might conflict.

Platform SSO artifacts persist after profile removal

Symptom:

A device was removed from the Platform SSO ESSP profile (for example, a device was taken out of an Intune group during or after a pilot). Even after removal, ABR still behaves as if Platform SSO is registered - it looks for a token, cannot find one (because the user has not re-authenticated since PSSO was removed), and continues down the identity lookup chain. The user gets Global Settings when no later source supplies a UPN: always on Okta, and on Entra ID when the user is not signed in to Company Portal, Outlook or Teams.

Cause:

Platform SSO registration data is written into the device's keychain and OS configuration state when it is first set up. Removing the ESSP profile from MDM does not automatically clean up this data. ABR still detects the device as having Platform SSO registered, but no token is available, so Platform SSO returns no UPN.

Fix:

Per Microsoft's guidance, the intended resolution is to reset the Company Portal app state and clean the relevant keychain entries. However, in practice, support teams have found this cleanup unreliable - the Platform SSO configuration is often too deeply embedded in the device state to fully remove without a wipe. The most dependable resolution is to wipe and re-enroll the device.

> Before rolling out Platform SSO to a pilot group, decide in advance how you will handle devices that need to exit the pilot. If a clean exit without a wipe is important, plan carefully and test the cleanup procedure on a small number of devices before committing to the pilot. Exiting a Platform SSO deployment is significantly harder than entering one.

New combined EPM mobileconfig deployed over old separate profiles

Symptom:

After switching from the older pair of mobileconfigs (`AdminByRequest - FDA PPPC_v2.mobileconfig` and `AdminByRequest - System Extension.mobileconfig`) to the new combined `Admin By Request - EPM.mobileconfig`, devices show unpredictable behaviour: Full Disk Access may not register, the System Extension may show as not approved, or both states may flap. ABR cannot reliably read the Platform SSO token, and Sub-Settings stop applying.

Cause:

The new combined `Admin By Request - EPM.mobileconfig` consolidates what the two older profiles did. When it is pushed to a device that still has the old profiles installed, macOS sees overlapping PPPC and System Extension payloads from different profiles and the resulting state is not deterministic.

Fix:

1. In your MDM, remove the assignments for `AdminByRequest - FDA PPPC_v2.mobileconfig` and `AdminByRequest - System Extension.mobileconfig` from the target Mac group and confirm both have been uninstalled from devices.
2. Once the old profiles are gone, push `Admin By Request - EPM.mobileconfig` to the group.
3. Verify FDA in **System Settings > Privacy and Security > Full Disk Access** and the System Extension approval in **Login Items and Extensions** on a sample device.

Do not deploy the new combined profile on top of the old ones - delete the old ones first.

[Okta only] v5.2.0 and v5.2.1 - device groups fail when HostName and NetBIOS name differ

Symptom:

After upgrading Mac agents from v5.1.x to v5.2.0 or v5.2.1 in an Okta environment with Platform SSO active, device-group-based policies stop applying. The Groups tab in Inventory shows "No data to display" on upgraded devices. The same devices showed groups correctly on v5.1.x. Windows devices on the same tenant are not affected.

Cause:

A bug in ABR Mac v5.2.0 and v5.2.1 caused device group resolution to fail when the device's HostName and NetBIOS name did not match exactly. This affected environments that used computer groups in Global Scope or Sub-Settings with Platform SSO active.

Fix:

Upgrade the Mac ABR agent to v5.2.2 or later. The fix checks both HostName and NetBIOS name formats when resolving device group membership.

If you cannot update immediately, a temporary workaround is available: change the scope condition in the affected Global Scope or Sub-Setting from computer groups to user groups. This restores correct policy application without requiring a client update.

Diagnostic logs

When investigating Platform SSO issues, ABR's diagnostic logs are the fastest way to identify which part of the configuration chain has failed. Log entries from the AppSSO layer will tell you whether the ESSP profile is absent, misconfigured, or present-but-unauthenticated.

Two ways to access the logs:

1. **macOS Console app:** Open the Console app on the affected Mac and navigate to **Log Reports > adminbyrequest.log**.
2. **In-app diagnostics submission:** Click **"About Admin By Request"** in the ABR menu bar icon and select **Diagnostics > Submit**. This sends the logs directly to the ABR support team, which is useful when a customer is submitting a support ticket.

Key log patterns:

Log entry (text might not be exact)	What it means
`Entra ID UPN - macOS Platform SSO enabled, but user has not authenticated`	ESSP profile is deployed and macOS recognises Platform SSO, but the user has not completed the registration flow.
`Entra ID UPN - macOS Platform SSO enabled, but Full Disk Access not enabled`	Platform SSO is registered but ABR cannot read the token because FDA has not been granted.
`[AppSSO] JSON parsing error for Device Configuration`	The ESSP profile is absent from the device or contains a syntax error.
`[AppSSO] No extensionIdentifier/accountDisplayName found. Exiting early.`	The ESSP profile is absent, incomplete, or conflicted with another profile.

Acronyms and Abbreviations

Abbreviation	Full form	Notes
ESSP	Extensible Single Sign-On Profile	A macOS MDM configuration profile that installs and configures an SSO extension at the OS level, allowing the macOS login dialog to authenticate against a corporate IdP (Entra ID or Okta) via Apple's Platform SSO mechanism. Deployed via Intune or Jamf. ABR requires the `com.fasttracksoftware.` prefix in the profile's AppPrefixAllowList to access the Platform SSO identity token.

Abbreviation	Full form	Notes
FDA	Full Disk Access	macOS permission required by the ABR agent to function.
IdP	Identity Provider	The external system that authenticates users via SSO/MFA (e.g., Entra ID, Okta, ADFS, Google, JumpCloud).
MDM	Mobile Device Management	Platforms (Intune, Jamf, Kandji, SCCM) used to deploy and manage the ABR agent (among other things).
UPN	User Principal Name	The user's identity in Active Directory or Entra ID, typically in `user@domain.com` format. Used by ABR's Email match setting for SSO identity verification.

Technical Terms

AppPrefixAllowList - A configuration key in an Extensible Single Sign-On Profile (ESSP) that whitelists application bundle ID prefixes allowed to read the Platform SSO identity token. ABR's bundle IDs begin with `com.fasttracksoftware.`, so the value `com.fasttracksoftware.` must be present in this list for ABR to access the Platform SSO identity token. If this key is absent or does not include the ABR prefix, the token is readable by the SSO extension but not by ABR, and identity resolution fails silently.

PPPC profile - Privacy Preferences Policy Control profile. A macOS MDM configuration profile that grants specific applications specific privacy/accessibility permissions at the system level, bypassing the macOS user consent dialogs. ABR requires a PPPC profile to grant it Full Disk Access (FDA) so it can resolve user group membership via Entra ID or Platform SSO. This profile must be deployed to devices via MDM (Intune, Jamf, Kandji) before or at the same time as the ABR agent package.