Temporary Administrator Access with SAP Privileges (macOS)

Overview

SAP Privileges lets a standard macOS user request administrator rights for a limited period. This article explains how to deploy Privileges 2.5.3, configure administrator rights to expire after five minutes, require users to authenticate and provide a reason, and optionally report the most recent change in privilege status through a FileWave Custom Field.

> ⚠ Administrator access cannot be made risk-free. While elevated, a user or process can change security settings, install persistent software, unload management components, or interfere with later revocation. Privileges cannot undo those changes or guarantee that administrator rights will be removed on schedule. Keep a separate recovery or management account, test the workflow on representative devices, and treat the timer as a policy control rather than a security boundary.

Requirements and compatibility

- FileWave Central and enrolled macOS devices with FileWave Client installed.
- A user account that normally runs as a standard user.
- A protected administrator account or another recovery method that does not depend on Privileges.
- Privileges 2.5.3 supports macOS 11 through macOS 26. Tamper protection requires macOS 13 or later.

On affected macOS 13 devices, macOS may report a false launch constraint violation and terminate the standard build. SAP provides a `noLC` package for those devices but recommends the standard package whenever it works.

Downloads

Item	Purpose
Privileges 2.5.3 installer package	Official signed and notarized SAP installer. The SHA-256 digest is `5948b4b809d05796f-f09d4f064a72f049a3f895af194c146d3937f005d34401d`.
Profile - Privileges Config.fileset.zip	Example FileWave Profile Fileset with the five-minute policy, authentication, reason prompts, menu bar access, and notification approval.
Privileges - Last Change.customfields	Optional client-script Custom Field named Privileges - Last Change.
SAP approval profile	

Item	Purpose
	Official reference profile for notifications, Service Management, the system extension, and the system extension's Full Disk Access grant.

Deploy Privileges

1. Download and verify the installer

Download the official 2.5.3 package. Before importing it, confirm the digest and Apple signature:

```
shasum -a 256 Privileges_2.5.3.pkg
pkgutil --check-signature Privileges_2.5.3.pkg
```

The `shasum` output should match the digest listed above. `pkgutil` should report a Developer ID Installer signature from `SAP SE (7R5ZEU67FQ)` and a notarization status trusted by the Apple notary service.

2. Create the PKG Fileset

1. In FileWave Central, open Filesets.
2. Drag `Privileges_2.5.3.pkg` into the Filesets view, or choose New Fileset and select the PKG Fileset type.
3. Name the Fileset clearly, such as PKG - Privileges, and put 2.5.3 in the revision name.

See Create and Update PKG and MSI Filesets for the standard package workflow.

3. Import and review the Profile Fileset

1. Download and extract Profile - Privileges Config.fileset.zip.
2. Drag the extracted `Profile - Privileges Config.fileset` into FileWave Central.
3. Open the imported Profile Fileset and review every setting before assigning it.

Setting	Example value and effect
`ExpirationInterval`	`5`. Administrator rights are scheduled to expire after five minutes. Do not also configure `ExpirationIntervalMax`; a fixed interval takes precedence.
`RequireAuthentication`	`true`. Requires the current user to authenticate with a password or Touch ID before requesting administrator rights. This verifies user presence; it is not manager approval and does not require separate administrator credentials.
`ReasonRequired` and `ReasonPresetList`	Requires a stated reason. The example includes Installing an App and Deleting Files; Privileges adds its own Other... entry for free text. A reason records intent but does not restrict what the user can do.
`RevokePrivilegesAtLogin`	`true`. Revokes administrator rights at login. Before deployment, add the short names of all permanent local administrator accounts to `RevokeAtLoginExcludedUsers`. If login-

Setting	Example value and effect
	time revocation does not fit your account design, remove this setting.
`LimitToUser` and `LimitToGroup`	Not included in the example. Add one or both settings if only approved account short names or groups should be able to request administrator rights. Use arrays of strings rather than the legacy single-string format.
Notification bundle identifier	`corp.sap.privileges.agent`. The notification payload must target the agent, not the main application bundle.
`EnableSystemExtension`	Not included in the example. Configure the approval payloads described below before enabling tamper protection.

> ⚠ The downloadable Profile Fileset enables `RevokePrivilegesAtLogin` and does not contain excluded usernames. Before deployment, add every protected or permanent local administrator account to `RevokeAtLoginExcludedUsers`, or remove `RevokePrivilegesAtLogin` from the policy. Otherwise, those accounts become standard users at their next login.

The example intentionally omits the deprecated `DockToggleTimeout` key, broad Full Disk Access and Post Events grants for the main application, and a post-change executable. If you add `PostChangeExecutablePath`, deploy the executable at that exact path and use `PostChangeExecutableChecksum` to verify it.

4. Deploy the Filesets

1. Create a Deployment that includes both the PKG Fileset and Profile Fileset, and target a small test group. If your environment still uses legacy Fileset Associations, associate both Filesets with the same group.
2. Select Update Model.
3. Confirm that both Filesets install successfully on the test devices before widening the deployment.

Optional tamper protection

Privileges 2.5 introduced an Endpoint Security system extension that helps prevent attempts to remove Privileges or unload its launch services. To use it, build a separate Profile Fileset from SAP's 2.5.3 approval profile. It contains:

- Service Management approval for Team Identifier `7R5ZEU67FQ`.
- Endpoint Security system extension approval for the same team.
- A removable system extension entry for `corp.sap.privileges.extension`, which allows managed removal later.
- Full Disk Access for `corp.sap.privileges.extension`.

Deploy and confirm those approvals before setting `EnableSystemExtension` to `true`. Do not substitute Full Disk Access for `corp.sap.privileges`; SAP's profile grants it to the extension bundle.

Optional inventory reporting

The attached Custom Field reports the most recent change to administrator or standard-user status that remains in the local unified log.

1. Download Privileges - Last Change.customfields.
2. In FileWave Central, open Assistants > Custom Fields > Edit Custom Fields.
3. Click Import, select the downloaded file, and review the macOS script.
4. Associate Privileges - Last Change with the required macOS devices.
5. After the next FileWave Client verification and inventory update, add the field to the Clients view or an Inventory Query.

Example values:

```
jsmith: privilege=administrator reason="Installing an App"
jsmith: privilege=standard reason="privileges expired"
```

The script searches up to seven days of the local unified log using the dedicated Privileges 2.5.2 or later subsystem and category:

```
log show --predicate 'subsystem == "corp.sap.privileges.daemon" AND category ==
"privchange"' --last 7d
```

> This Custom Field is a reporting aid, not an audit log. macOS decides when unified log entries are removed, so the field can be blank even when Privileges was used. For durable records, configure Privileges remote logging to a managed syslog or webhook destination.

Verify the deployment

1. Confirm the receipt and installed version:

   ```
   pkgutil --pkg-info corp.sap.privileges.pkg
   ```

2. Launch Privileges as a standard user, authenticate, and select or enter a reason.
3. Confirm the account enters the local `admin` group, then returns to standard-user status after the configured interval:

   ```
   CONSOLE_USER=$(stat -f '%Su' /dev/console)
   id -Gn "$CONSOLE_USER"
   ```

4. Confirm the local event is present:

   ```
   log show --predicate 'subsystem == "corp.sap.privileges.daemon" AND category
   == "privchange"' --last 30m
   ```

5. If tamper protection is enabled, confirm the system extension is active:

   ```
   systemextensionsctl list | grep -F 'corp.sap.privileges.extension'
   ```

6. If you assigned the optional Custom Field, run another FileWave Client verification and confirm Privileges - Last Change is populated.

Troubleshooting

Symptom	Check
Privileges immediately exits on macOS 13	Test SAP's `Privileges_2.5.3_noLC.pkg`. Before importing it, verify that its SHA-256 digest is `f88fe902a5850704900cb0b6e365f-f9b5979354c801ee8452a349459e7f823f9` and check its Apple signature as described above. Use the standard package on other systems unless you reproduce the launch constraint problem.
Notifications do not appear	Confirm the profile targets `corp.sap.privileges.agent` and that the profile installed successfully.
A permanent administrator becomes a standard user at login	Add the account's short name to `RevokeAtLoginExcludedUsers`, or remove `RevokePrivilegesAtLogin` from the policy.
The Custom Field is blank	Run the log command above locally. The device needs Privileges 2.5.2 or later for the dedicated subsystem, and macOS may already have removed the event.
The system extension prompts for approval or remains inactive	Deploy SAP's Service Management, system extension, removable extension, and Full Disk Access payloads before enabling `EnableSystemExtension`.

Remove Privileges

Do not assume that removing the PKG Fileset from a Deployment, or breaking a legacy Fileset Association, removes every Privileges component. If tamper protection is enabled, first remove or disable the managed `EnableSystemExtension` setting, select Update Model, and confirm the extension is disabled before continuing. Then deploy SAP's current Privileges 2 uninstall script as root.

Related information

- SAP Privileges 2.5.3 release
- Managing Privileges
- SAP uninstallation guidance
- Importing and Exporting Custom Field Files
- Custom Fields

Revision #6
★Created 2026-07-24 19:42:15 UTC by Andrew Kloosterhuis
Updated 2026-08-06 20:13:24 UTC by Josh Levitsky