Troubleshooting Intune for macOS management

This guide outlines key troubleshooting methods for managing macOS devices with Microsoft Intune. It covers common issues related to local group management, configuration profiles, compliance, and app deployment. Use these steps to identify, diagnose, and resolve problems efficiently during macOS device management.

Visit the following page for a summary of awesome community tools that support you in managing macOS on a greater scale:

Shell Commands

This section provides essential shell commands used in macOS Intune troubleshooting. These commands help verify system status, logs, profiles, and connectivity during device diagnostics.

Add User as Admin

In some troubleshooting or configuration scenarios, it's necessary to ensure that the local user account has administrative rights. This can be done manually or through scripting in a managed deployment.

```
dseditgroup -o edit -a "<username>" -t user admin
```

Remove User as Admin

For security or compliance reasons, you may need to revoke administrative privileges from a user account on a managed macOS device. This can be done manually or via command line.

```
dseditgroup -o edit -d "<username>" -t user admin
```

Review Group Membership

Use these commands to check if a user has admin rights and view current members of the admin group. Helpful for verifying permissions before making changes.

```
dscacheutil -q group -a name admin
```

Get Current Active User

Use these commands to identify the currently logged-in user, useful for scripts and remote troubleshooting.

```
dscl . -list /Users | grep -v -e '_' -e root -e nobody -e daemon
```

Search Filelocation of Bundle ID

This command uses **macOS Spotlight search** (via `mdfind`) to locate the path of an app or bundle on the system by its **bundle identifier**.

In this case, it searches for the **Microsoft Teams 2.0** app, whose bundle identifier is `com.microsoft.teams2`.

```
mdfind "kMDItemCFBundleIdentifier = 'com.microsoft.teams2'"
```

Update Privacy Settings

macOS requires explicit user consent for apps to access sensitive system resources like Full Disk Access, Camera, Microphone, and automation controls. For managed devices, these permissions can be pre-approved using a configuration profile with the **Privacy Preferences Policy Control (PPPC)** payload.

PPPC settings are defined in a configuration profile (`.mobileconfig`) using the `com.apple.TCC.configuration-profile-policy` payload. This allows IT administrators to grant or deny specific permissions to apps without user interaction.

Jamf PPPC Utility is a free macOS tool that lets you build and export PPPC payloads through a user-friendly interface. It helps you:

- Select an app and automatically extract its code signing information
- Define specific services and permissions (e.g., Files and Folders, Automation, System Access)
- Export the result as a `.mobileconfig` file ready for deployment via Intune or another MDM

This tool is especially useful when configuring permissions for third-party or custom apps.

Change Primary Kerberos TGT

On macOS the kswitch command is a Kerberos utility command that interactively shows all cached Kerberos identities (from your credential cache) and allows you to choose which identity should be set as the active one for authentication, such as when accessing network services or enterprise resources that use Kerberos.

```
kswitch -i
```

Troubleshooting

Explore key diagnostic steps and resolution paths for frequent macOS management issues in Intune, helping you isolate causes and apply targeted fixes.

View live logs of Intune MDM Daemon

To monitor real-time activity from the Intune MDM agent, use the following command in Terminal:

```
tail -f /Library/Logs/Microsoft/Intune/*IntuneMDMDaemon*.log
```

Revision #5
Created 2025-07-29 15:30:02 UTC by Luca Noah Caprez
Updated 2026-01-13 18:28:37 UTC by Luca Noah Caprez