

OS Patching

Document Number	Effective Date	Review Date	Version	Author	Approved By
[ITEP.1.x]	03/04/25	[Date]	1.0	Andrew Barnett	[Approver Name]

IT Admin Procedure

1. Purpose

Describe the purpose of the SOP. Explain why this procedure is necessary and what it aims to achieve.

The purpose of this Standard Operating Procedure (SOP) is to provide a basic guideline for operating system patching in Jamf Pro. This SOP is especially important for operating system patching that will be deployed to every applicable Apple device, including both computers and mobile devices. Given the different settings for each type of device, it is crucial to follow a recommended approach to ensure effective deployment.

2. Scope

Define the scope of the SOP. Specify the departments, teams, or processes that this procedure applies to.

This SOP applies to the UEM Apple Team responsible for updating operating systems via **Jamf** for **macOS or mobile devices**.

3. Definitions

Provide definitions for any terms, acronyms, or jargon used in the SOP.

- **Self-Service Hub** – A portal within Jamf where users can manually install approved applications.
- **System Settings** - (known as **System Preferences** prior to macOS Ventura), Is an application included with macOS. It allows users to modify various system settings, which are divided into separate Preference Panes.
- **Settings App** - Is an application included with iPadOS and iOS. It allows users to modify various system settings.
- **SOP:** Standard Operating Procedure. It typically is a set of written instructions that outlines how to perform a routine task

- **Apple UEM Team:** Refers to the Apple Unified Endpoint team. It is the team that manages the overall Jamf Pro server health on campus
- **Jamf Pro Server:** Texas A&M tool of choice to manage Apple devices on campus
- **Team Dynamix:** The current official ticketing system used by Texas A&M
- **S.U.P.E.R.M.A.N.** - (or just Super) is an open-source script that provides administrators with a comprehensive solution to encourage and enforce macOS minor updates, macOS major upgrades, Jamf Pro Policies, or enforced system restarts.
- **Managed Software Updates** - Managed software updates in Jamf Pro provides a simple, unified interface that enables you to easily deploy software updates to the computers and mobile devices in your environment.
- **Jamf Pro API** - Jamf Pro has two APIs that can be used to programmatically interface with your data.

4. Responsibilities

Outline the roles and responsibilities of individuals or teams involved in the procedure.

- **UEM Apple Team**
 - Review, test, and deploy necessary Configuration Profiles, Policies, and scope of devices.
 - Assists in troubleshooting failed deployments.
 - If a device needs to not be updated, the Apple UEM team will work with the department or college to un-scope the device to meet their requirements after the necessary security exceptions have been submitted.

5. Procedure

Detail the step-by-step process to be followed. Include any necessary sub-steps, decision points, and contingencies.

5.1. Preparation

- **Description:** Ensure all deployment details are accurate, including the Configuration Profiles, Policies, deployment scope, and whether the Policies should be available in the Self-Service Hub or Support Hub.
- **Responsible Party:** Apple UEM Team
- **Tools/Resources Needed:**
 - **Necessary:** Jamf Pro Server
 - **Optional:** S.U.P.E.R.M.A.N. (for macOS), Microsoft Teams, Team Dynamix, Jamf Pro API

5.2. Execution

- **Description:**
 - **macOS:**
 - Configure and test the necessary Configuration Profiles, Policies, and Smart Groups.
 - Verify an end user has a Bootstrap Token (must be escrowed to Jamf to use API or Jamf Managed Software Updates) and Volume Ownership.
 - Create a Jamf Pro API Client account with the necessary account permissions.
 - Verify the S.U.P.E.R.M.A.N. Configuration Profile and Policy have deployed properly to the necessary scoped groups.
 - Optional: Jamf Managed Software Updates to push operating system updates to devices enrolled via a Prestage enrollment and macOS 11 or higher.
 - Optional: Update macOS via System Settings or System Preferences. Apple Silicon requires the end user to have a Bootstrap Token.
 - iPadOS/iOS
 - Configure and test the necessary Smart Device Group.
 - Deploy Jamf Managed Software Updates to Smart Device Group.
 - Optional: Update the operating system via the Settings App.
 - **Requirements:** Target devices with iOS 14 or later, iPadOS 14 or later, or tvOS 14 or later, supervised or enrolled via a PreStage enrollment in Jamf Pro.
- **Responsible Party:** UEM Apple Team
- **Tools/Resources Needed:**
 - **Necessary:** Jamf Pro Server
 - **Optional:** Jamf Pro API, S.U.P.E.R.M.A.N.

5.3. Troubleshooting

- **Description:**
 - If deployment fails, or OS updates fail to complete, review the **Console – Log Reports** to diagnose errors and escalate issues to the **Apple UEM Team** if needed.
 - Local Support can submit a ticket with Team Dynamix with reported issues.
- **macOS:**
 - Jamf Managed Software Updates:
 - Target computers with macOS 11 or later, supervised or enrolled via a PreStage enrollment in Jamf Pro.
 - To have the update for computers with Apple silicon (i.e., M1 chip) installed automatically without user interaction, a Bootstrap Token for target computers must be escrowed with Jamf Pro. macOS will automatically request the Bootstrap Token from Jamf Pro to authorize updates that were scheduled to install.



- **Responsible Party:** Local Support, Apple UEM Team
- **Tools/Resources Needed:** macOS Device, iPadOS device, iOS device, Jamf Pro Server, Team Dynamix

5.4. Completion

- **Description:**
 - Verify that all scoped devices successfully received and executed the deployment.
 - Confirm with device inventory records are reporting a successful update of the operating system.
 - Notify the **Apple UEM Team** that the deployment is complete, and if any issues arise, troubleshoot and resolve them if possible.
- **Responsible Party:** Local Support, Apple UEM Team
- **Tools/Resources Needed:** Jamf Pro Server

5.5. Review and Approval

- **Description:** After verifying the deployment, the Apple UEM Team will monitor all targeted devices to have successfully received the required updates.
- **Responsible Party:** Apple UEM Team
- **Tools/Resources Needed:** Jamf Pro Server

6. Documentation

List any forms, logs, or records that need to be maintained as part of this procedure.

- Any Team Dynamix ticket created while going through this operating system update process.

7. References

Include any related documents, policies, or regulations that support this SOP.

- **Team Dynamix:** <https://service.tamu.edu/>
- **Jamf Pro:** https://learn.jamf.com/en-US/bundle/jamf-pro-documentation-current/page/Jamf_Pro_Documentation.html
- **Jamf Managed Software Updates:** https://learn.jamf.com/en-US/bundle/jamf-pro-documentation-current/page/Managed_Software_Updates.html
- **S.U.P.E.R.M.A.N.:** <https://github.com/Macjutsu/super>
- **Jamf Pro API:** <https://developer.jamf.com/jamf-pro/>



8. Revision History

Track changes made to the SOP over time.

Version	Date	Description of Change	Author
1.0	03/04/2025	Initial release	Andrew Barnett
1.1	[Date]	[Description]	[Author Name]

Appendices

Include any additional information, diagrams, or charts that support the procedure.

1. [University Rules and SAPs - Texas A&M University](#)
2. [University-Wide IT Governance Framework](#)
3. [SOPs – Division of Research - Texas A&M University](#)