

Application Patching

Document Number	Effective Date	Review Date	Version	Author	Approved By
[ITEP.1.x]	02/27/2025	02/27/2025	1	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 third party application patching in Jamf Pro. This SOP is especially important for application 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.

This SOP aims to:

- Ensure a consistent and effective method for creating application patching policies, configuration profiles or mobile device apps.
- Highlight the importance of understanding the various settings within a policy, configuration profile or mobile device app.
- Emphasize the need for experience or assistance when creating policies, configuration profiles or mobile device apps to avoid potential issues.

By following this SOP, users can achieve a more efficient and reliable deployment of policies, configuration profiles or mobile device apps across all applicable Apple devices.

2. Scope

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

This Standard Operating Procedure (SOP) is intended for anyone involved in deploying policies, configuration profiles or mobile device apps for application patching using Jamf Pro. It is applicable to all individuals, regardless of their department or role, who are responsible for creating and managing policies, configuration profiles or mobile device apps for application patching for Apple devices. This includes both computers and mobile devices.

There are no specific limitations or boundaries for this SOP; it covers the creation and management of all types of configuration profiles within Jamf Pro.

3. Definitions

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

4. Responsibilities

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

The primary responsibility for monitoring and managing application patching lies with the Apple UEM Team. This team is also tasked with deploying policies, configuration profiles or mobile device apps that are intended for all computers or mobile devices within the organization. Specific responsibilities include:

- Creating Policies, Configuration Profiles or Mobile Devices Apps: Team members will create policies configuration profiles in Jamf Pro, ensuring they meet the organization's requirements.
- Testing Policies, Configuration Profiles or Mobile Devices Apps: Before deployment, team members will thoroughly test the policies and configuration profiles to ensure they function as intended and do not cause any issues.
- Deploying Policies, Configuration Profiles or Mobile Devices Apps: The Apple UEM Team will deploy the tested policies and configuration profiles to all applicable devices.
- Monitoring and Troubleshooting: The team will continuously monitor the deployed policies, configuration profiles or mobile device apps and address any issues that arise.

5. Procedure

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

5.1. Execution

Configuration Profiles

1. Sign in to Jamf Pro: Begin by signing in to your Jamf Pro account.
2. Select Device Type: On the left sidebar, decide whether you need a configuration profile for a computer or a mobile device. Select the appropriate option.
3. Access Configuration Profiles: In the menu that appears, click on "Configuration Profiles."
4. Create or Upload Profile:
 - a. To create a new configuration profile, click "New."

- b. To use an existing configuration profile, click "Upload" and select the profile you want to use.
5. Configure the Payload: If you are creating a new profile, ensure you configure the payload settings properly according to your requirements.
6. Add Scope Group: Once your configuration profile is ready, add the scope group for the profile.
7. Deploy the Profile: Finally, deploy the configuration profile to the selected devices.

Policies & Mobile Device Apps

8. Sign in to Jamf Pro: Begin by signing in to your Jamf Pro account.
9. Select Device Type: On the left sidebar, decide whether you need a policy for a computer or a mobile device app for a mobile device. Select the appropriate option.
10. Access Computer Policies: In the menu that appears, click on "Policies."
11. Create Computer Policy:
 - a. To create a new policy, click "New."
 - b. To use an existing policy, open an existing policy and click "Clone" and select the policy you want to use.
12. Access Mobile Device Apps: In the menu that appears, click on "Mobile Device Apps."
13. Create Mobile Device App:
 - a. To create a new mobile device app, click "New."
14. Configure the Payload: If you are creating a new profile, ensure you configure the payload settings properly according to your requirements.
15. Configure the Policy or Mobile Device App: If you are creating a policy or mobile device app, ensure you configure the policy or mobile device app settings properly according to your requirements.
16. Add Scope Group: Once your configuration profile, policy or mobile device app is ready, add the scope group for the profile, policy or mobile device app.
17. Deploy: Finally, deploy the configuration profile, policy or mobile device app to the selected devices.

5.2. Troubleshooting

The type of troubleshooting required will depend on the specific configuration, policy or mobile device app being deployed. Here are some general guidelines to help resolve common issues:

- Scoping Issues: Ensure that the configuration profile, policy or mobile device app is scoped to the correct scope group. Incorrect scoping can prevent the profile from being applied to the intended devices.
- Site Configuration: Verify that the configuration profile, policy or mobile device app is placed in the correct site on the server. For configuration profiles, policies or mobile device apps that are meant to go to all devices, the site should typically be set to "None."

- Application: If configuration profiles, policies or mobile device apps are not applying correctly, check the logs in Jamf Pro for any errors. This can provide insights into what might be going wrong.
- Device Enrollment: Ensure that the devices are properly enrolled in Jamf Pro. Devices that are not enrolled correctly may not receive the configuration profiles, policies or mobile device apps.
- Configuration Settings: Review the configuration profiles, policies or mobile device apps settings to ensure they are correct. Incorrect settings can lead to configuration profiles, policies or mobile device apps not functioning as expected.

By following these troubleshooting steps, you can address common issues and ensure that configuration profiles are deployed successfully.

5.3. Completion

Once the configuration profiles, policies or mobile device apps is deployed, it is essential to verify that it has been applied correctly to the devices. This can be done by checking the status of the policies, configuration profiles or mobile device apps in Jamf Pro and ensuring that the devices have received the configuration profiles, policies or mobile device apps as intended. Additionally, you should document the configuration profiles, policies or mobile device apps settings and any changes made to the configuration profiles, policies or mobile device apps for future reference.

After deployment, it is crucial to monitor the deployment to ensure that no issues arise that were not identified during testing. Keeping an eye on the deployment helps to promptly address any unexpected problems and ensures the smooth functioning of the configuration profiles, policies or mobile device apps.

5.4. Review and Approval

The Apple UEM Team will review the configuration profiles, policies or mobile device apps to ensure they meet the necessary standards and requirements. The review process involves testing the profiles in a controlled environment and gathering feedback from relevant stakeholders. Once the profiles have been reviewed and any necessary adjustments have been made, the change request will be submitted for approval to the Apple UEM Manager and Director. Following this, the profiles will need to be approved in the Change Advisory Board (CAB) before they can be deployed.

6. Documentation

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



[Jamf Pro Configuration Profile Documentation](#)

[Jamf Pro Policies Documentation](#)

[Jamf Pro Managed Content Documentation](#)

Tools that Can Help with Configuration Profiles, Policies or Mobile Device Apps:

<https://imazing.com/profile-editor>

<https://github.com/jamf/PPPC-Utility>

<https://www.jamf.com/products/jamf-composer/>

https://learn.jamf.com/en-US/bundle/jamf-pro-documentation-current/page/Apps_Purchased_in_Volume.html

https://learn.jamf.com/en-US/bundle/jamf-pro-documentation-current/page/Package_Deployment.html

7. References

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

8. Revision History

Track changes made to the SOP over time.

Version	Date	Description of Change	Author
1.0	02/27/2025	Initial release	Andrew Barnett
1.1		[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](#)