



Requesting and Managing Roles and Permissions – Apple School Manager

Commented [FN1]: Peer Review: 🍌

Document Number	Effective Date	Review Date	Version	Author	Approved By
[ITEP.1.x]	3/4/24	[Date]	[Version Number]	Danielle Narita	[Approver Name]

IT Enterprise 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 SOP is to provide a standardized process for requesting access for local support users to Jamf Pro, ensuring they are granted standard user roles and group access as appropriate. This will help maintain a controlled and efficient process for local support to handle device management tasks within the limits of their permissions.

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, specifically for managing and integrating MAIDs and FAIDs with Jamf Pro for device management. The scope includes:

- Creation and management of MAIDs and FAIDs
- User roles and permissions for Jamf Pro and Apple services
- Troubleshooting any issues related to MAID/FAID integration with Jamf Pro.

3. Definitions

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

- **Apple School Manager (ASM)** is a web-based service that allows educational institutions to manage Apple devices, apps, and accounts.
- **Managed Apple IDs (MAIDs)** are Apple IDs created and controlled by an institution (such as a school or organization) using Apple School Manager or Apple Business Manager. These accounts are used to provide access to Apple services such as iCloud, App Store, and Apple



Schoolwork. Managed Apple IDs have restrictions and permissions set by the institution, and they are primarily used by students, teachers, and staff for educational purposes.

- **Federated Apple IDs (FAIDs)** are Apple IDs that are linked to an existing directory service (such as Microsoft Azure Active Directory or a school's LDAP system). When a federated identity is set up, users can log into Apple services using their existing credentials (e.g., school email or other enterprise login). This process helps schools and organizations simplify user management by integrating Apple services with their existing authentication systems.
- **Jamf Pro Pro:** A comprehensive Apple device management solution that helps IT departments manage and secure Apple devices.
- **UEM - Apple Team:** Unified Endpoint Management team responsible for managing Apple devices in the organization.
- **Alert:** A notification generated in Jamf Pro that indicates a specific condition or status requiring attention.

4. Responsibilities

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

- **UEM - Apple Team Members:**
 - Ensure that roles and permissions are correctly configured in Jamf Pro
 - Ensure that Apple ID integration is done correctly in Jamf Pro and troubleshoot any integration issues.
 - Assist end-users with access issues and provide support for any device management concerns
- **Local Support Users:**
 - Utilize assigned MAIDs or FAIDs for moving MDM sites
 - Confirms successful completion

5. Procedure

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

5.1. Preparation

- **Description:** Local support users will complete the access request form or click on the designated link to initiate their request for ASM access. With the following information:
 1. **Name** of the local support user



2. **Department/Team** they belong to.
3. **Justification** for the request (e.g., need to access something specific in Jamf Pro).
4. **Requested access level** (should default to Standard User with specified group access).
5. **Manager or Supervisor approval** (if necessary for higher-level access).

- **Responsible Party:** Local Support User
- **Tools/Resources Needed:** Ability to create tickets in Team Dynamix

5.2. Execution

- **Description:**
 1. The completed form is submitted to the UEM - Apple Team for review and confirm details. If the request is approved the UEM - Apple Team member will create the requested account in ASM with the correct permission and will send confirmation to requestor
 2. Navigate to Apple School Manager or Apple Business Manager.
 - Select "Accounts" and choose "Add Managed Apple ID."
 - Enter the user information (name, email, and role) and assign appropriate permissions.
 - Sync the MAID with Jamf Pro via the Jamf Pro integration section.
 - Ensure that the MAID is linked to the relevant user profile in Jamf Pro.
 3. Creating Federated Apple IDs (FAIDs):
 - In Apple Business Manager, link FAIDs via the Federated Authentication settings.
 - Ensure the organization's Identity Provider (IdP) supports Single Sign-On (SSO) for seamless FAID creation.
 - Sync FAIDs to Jamf Pro using the Federated Authentication feature.
 - Set the role for each FAID within Jamf Pro and Apple services, ensuring the user can access only necessary resources.
 4. Assigning Roles and Permissions:
 - Assign roles such as Admin, Device Manager, or Standard User based on user needs.
 - Adjust the permissions based on the level of access required for apps, devices, and services.
- **Responsible Party:** UEM - Apple Team Members
- **Tools/Resources Needed:** Apple School Manager

5.3. Troubleshooting

- **Description:**
 1. Sync Issues: If users report that their MAID or FAID isn't syncing with Jamf Pro:



- Check the integration status between Apple School Manager/Business Manager and Jamf Pro.
- Ensure that the Apple IDs are correctly linked in both systems.
- Confirm that the user's role and permissions are set correctly in Jamf Pro.
- If the issue persists, check Apple's system status and verify connectivity with Apple's servers.

2. Access Denied Issues: If users are unable to access specific apps or services:

- Verify the role assigned to the user in Jamf Pro and Apple services.
- Check if the app is provisioned correctly for that user.
- Ensure that the app or resource is available in the user's region or system configuration.

3. Federated Apple ID Login Failures:

- Verify that the IdP settings are correct for SSO authentication.
- Ensure that the user's FAID is synced and properly mapped in Jamf Pro.
- Check the user's login credentials against the corporate directory to ensure they are correctly authenticated.

▪ **Responsible Party:** UEM - Apple Team Members

▪ **Tools/Resources Needed:** Jamf Pro, ASM.

5.4. Complete Request

- **Description:** The UEM - Apple Team member will send confirmation to requestor that the account is created
- **Responsible Party:** UEM - Apple Team Members
- **Tools/Resources Needed:** TDx

6. Documentation

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

N/A

7. References

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

- [Apple School Manager Account Setup Guide](#)
- <https://it.tamu.edu/policy/it-policy/controls-catalog/controls/AC/AC-2/>
- <https://it.tamu.edu/policy/it-policy/controls-catalog/controls/AC/AC-3/>
- <https://it.tamu.edu/policy/it-policy/controls-catalog/controls/AC/AC-6/>



- <https://it.tamu.edu/policy/it-policy/controls-catalog/controls/AU/AU-2/>
- <https://it.tamu.edu/policy/it-policy/controls-catalog/controls/CM/CM-5/>
- [ITEP - Requesting and Managing Toles and Permissions - Process Diagram](#)

8. Revision History

Track changes made to the SOP over time.

Version	Date	Description of Change	Author
1.0	2/27/25	Initial release	Danielle Narita
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](#)