Managing Enterprise Device Configurations

SOP Number	Effective Date	Review Date	Version	Author	Approved By
ITEP-1.0.WIN	04/01/2025	07/21/2025	1.3	Jon Griffey	Jon Griffey

IT Enterprise Procedure

1. Purpose

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

The purpose of the SOP is to establish a standardized approach for defining, implementing, and maintaining device configurations across all Unified Devices within the organization. It ensures consistency, security, and compliance with the Texas A&M Controls Catalog, specifically addressing:

- Baseline Configuration (CM-2) – Ensuring all devices adhere to a standardized and approved configuration baseline.
- Configuration Change Control (CM-3) – Implementing a structured process for modifying and approving configuration changes.
- Configuration Settings (CM-6) – Defining and enforcing security and operational settings to maintain compliance.

By following this SOP, UEM personnel can efficiently manage configurations for desktops, laptops, tablets, and mobile devices while ensuring alignment with organizational standards and security policies.

2. Scope

Define the scope of the SOP. Specify departments, teams, or processes that apply.

This SOP applies to IT Administrators who are responsible for designing, testing, deploying, and managing enterprise device configurations in Microsoft Intune, MECM, PatchMyPC, and Admin By Request. It includes the following groups:

- UEM System Administrators
- Unit System Administrators
- Security Administrators

3. Definitions

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

- **Microsoft Endpoint Configuration Manager (MECM):** The on-premises device management platform for Texas A&M to administer Windows workstations and servers. It is part of the co-managed ecosystem, along with Microsoft Intune, and supports Technology Services modern device management strategy.

- **Intune:** The cloud-only device management platform for Texas A&M to administer Windows workstations and Android devices. It is part of the co-managed ecosystem, along with MECM, and supports Technology Services modern device management strategy.
- **Configuration Items (MECM)** – Defines rules and settings that must be met for a device to be considered compliant (like Intune's configuration policies).
- **Configuration Baselines (MECM)** – A collection of configuration items that can be applied to devices to ensure they meet security and operational requirements.
- **Configuration Policy (Intune):** A set of predefined settings and policies applied to devices to ensure compliance and security. These profiles help streamline device management by enforcing standard settings without requiring manual adjustments on each device.
- **Admin By Request (ABR)** – A privileged access management solution that provides just-in-time administrator rights for end users, ensuring elevated privileges are granted securely and temporarily to reduce security risks.
- **ABR Sub Setting** – A security feature within Admin by Request that allows granular control over administrative access on Windows devices. It enables IT administrators to define specific applications, processes, or system settings that users can modify without granting full administrator privileges, enhancing security while maintaining operational flexibility.
- **Technology Services Change Advisory Board (TS-CAB):** The department-wide advisory board for all significant IT enterprise changes that occur at Texas A&M University.
- **Device Management Focused Change Advisory Board (DM-FCAB)**: An advisory board focused on reviewing and approving the implementation of endpoint management-related changes. This includes all Enterprise-level changes and any unit-level changes that may have significance or impact on other University Academic or Business Units.

4. Responsibilities

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

- **A&E System Administrator**: Responsible for designing and building configuration policies for Intune, setting compliance parameters for MECM, creating configuration baselines for MECM, and developing group policy objects for MECM. This role ensures configurations meet security, compliance, and operational requirements, in collaboration with the Security Administrator to align policies.

- **UEM System Administrator**: Manages deployment, monitors compliance, and provides ongoing support for configurations, ensuring security and operational integrity.
- **Security Administrator:** Oversees security policies, ensures device configurations meet security standards, and creates and manages configurations for Admin By Request settings, collaborating with A&E and UEM teams for enforcement, deployment and testing.
- **Unit System Administrator:** The Unit System Administrator collaborates with the UEM System Administrator to deploy configurations, monitor security controls, troubleshoot issues, and support end users while aligning unit-specific needs with broader IT governance and security standards.

- **End User**: Utilizes devices in accordance with organizational policies, providing feedback on issues and ensuring compliance with security and operational guidelines.

5. Procedure

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

5.1 Preparation

- **Description:** Does the Policy Already Exist or Does Another Unit Have a Similar Policy?
  - If so, consult with the UEM System Administrator for Intune or MECM and the Security Administrator for ABR or the admin of the other unit to assess whether the existing policy can be adapted to meet the need.
  - If not, proceed assessing technical capabilities and management capacity.
  - Prepare Technical Capabilities Capacity Assessment Recommendation Matrix (TCCARX) found in ITEP Enterprise Testing and Validation Procedures
- **Responsible Party:** UEM System Administrator, A&E System Administrator, Security Administrator
- **Tools/Resources Needed:** Access and Roles needed to create and modify Configuration Policies in Intune, MECM or ABR. Setup Testing Environment if needed (Physical or VM).

5.2. Execution

- **Description:** Create a new configuration or duplicate the existing configuration for modification testing. Performing the tests, validate the defined criteria. Performing deployment testing in production environment.
  - **Keep Configurations Focused**: Ensure that configurations focus on a single action. Avoid creating large, multi-functional configurations.

    Example:
    Create separate configurations for setting up Chrome and Windows wallpaper.
  - **Collaboration:** Consult with the **Endpoint Security Team** to ensure the configuration meets security and compliance standards. Validate with Unit Admins to ensure testing encompasses unit-specific use cases.

5.2.1 Perform Dev Tests

- Reference and follow UEM's established Enterprise testing procedures.

5.2.2 Perform Deployment Tests

- Notify stakeholders that a test is being conducted.
- Follow the same procedure as Dev for testing.
- Collaborate with **Unit System Admins** to verify unit-specific requirements.
- Test configurations to ensure they operate as expected without conflicts.
- **Contingency Plans:** Test and validate an appropriate backout plan and be ready to initiate it if the change fails.

- **Responsible Party:** UEM System Administrator, Unit System Administrator, and Endpoint Security Team.
- **Tools/Resources Needed:** Access and Roles to publish, modify and delete configurations in the testing environment and production environment. This includes Intune, MECM, and PatchMyPC.

5.3. Documentation

- **Description:** Record the results of dev testing, deployment testing, including any issues that were identified and how they were resolved. Include any user feedback forms.
- **Responsible Party:** UEM System Administrator, Endpoint Security Team, End User (Acceptance Testing), Unit Administrator (Acceptance Testing)
- **Tools/Resources Needed:** Enterprise Testing Logs

5.4. Review, Approval and Deployment

- **Description:** Upon successful testing and validation by Unit administrators, prepare Change Request for approval, coordinate scheduling, and prepare for implementation.
    - Submit change request for review by **Device Management Focus Change Advisory Board (FCAB)**; upon approval,
    - Ensure that Unit System Administrators are available to address any issues specific to their units during the implementation and for post implementation testing and validation.
    - Implement change according to defined Implementation Plan
    - Document change result appropriately, Include any applicable user feedback forms.
- **Responsible Party:** UEM System Administrator, Endpoint Security Team, FCAB members, and Unit System Administrators.
- **Tools/Resources Needed:** Access and Roles to publish, modify and delete configurations in the production environment. Access to TeamDynamix to create change request.

5.5 Configuration Change Methodology & Versioning

Methodology
All configuration changes are evaluated for the most appropriate method of implementation, consisting of one of the following 'method-types':

1. ***ITERATIVE*** *(most MINOR changes)*: Results in the current configuration being modified at a scheduled time for all scoped devices and users.

   Criteria for determining an '*iterative*' configuration change:
   - No change in user experience or functionality
     (e.g. Updating the University Privacy Statement in the logon banner)
   - Replacing expiring certificates that require no user interaction
     (e.g. Silently replacing existing TAMU-CA Root certificate before its expiration date)
   - Change in duration of an existing configuration
     (e.g. Increasing the timeout period of display sleep settings)

Disclaimer: If an iterative change is necessary, a copy of the existing configuration that includes the new version modification ***will be*** *created for testing and validation purposes.*

2. ***COMPREHENSIVE*** *(most MAJOR changes)*: Results in the new version created alongside the existing configuration. Scoped devices/users migrate to the new version over a defined period.

   Criteria for determining a '*comprehensive*' configuration change:
   - Results in a fundamental change in behavior on the target device(s) for user(s)
     (e.g. Admin by Request replaces CyberArk and users must elevate for Admin rights)
   - Requires user interaction to complete the change successfully.
     (e.g. Users prompted with a migration workflow to migrate to Jamf or Intune)
   - Introducing a new or replacement enterprise product.
     (e.g. Elastic Defend replaces CrowdStrike Falcon)

3. ***DEPRECATION*** *(configurations that are no longer needed):* Results in a scheduled or phased removal of an existing configuration.

Versioning
All configurations approved for the 'Production' state will receive a version number ***after*** thorough pre-production testing with Unit Administrators and solicitation of feedback and deemed 'Production-Ready' upon approval by the DM-FCAB or TS-CAB.

Minor changes receive a *[.dot]* release number, while major changes receive a *[Full.]* release number. A 'Last Updated' date is included in the description or notes of the configuration.

Version Lifecycle
All minor and major versions will be preserved in an '*N-2*' state as general practice. This means that the current version along with the prior two versions are always preserved. All 'Change Enablement' Backout Plans will include a way to restore to a previous version, if possible.

6. Documentation

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

- **Configuration Design Document**
  - Includes detailed design specifications for the configuration, including actions, settings, and dependencies.
  - Document any security, compliance, and operational requirements considered during the design.
- **Change Request Form**
  - A formal document submitted to initiate the change process, including a description of the configuration, impact analysis, and approval process.
  - Should include links to relevant policies and security standards.
- **Testing Logs**
  - Unit Testing (ITAP) Log: Records of the unit-level testing, including test cases, results, and issues encountered.
  - Enterprise Testing (ITEP) Log: Logs from enterprise-wide testing, documenting performance, issues, and feedback from the broader environment.
- **Deployment Schedule**
  - A detailed schedule for the production deployment, including the timeline, device groups, and milestones.
  - Should include contingency plans for any potential failures or delays.
- **Compliance Monitoring Logs**
  - Logs from the UEM System Administrator that track the compliance of deployed configurations across devices, including any issues detected and resolutions.
- **Security Compliance Report**
  - Document created by the Security Administrator to validate that the configuration meets all security standards and policies.
  - Should include risk assessments, validation results, and any mitigating actions.
- **End User Feedback Form**
  - A record of feedback from End Users regarding device performance, functionality, and compliance with security and operational guidelines.
  - Includes suggestions for improvements or issues that may need addressing in future configurations.

- **Deployment Incident Log**
  - A log of any issues or incidents that arise during deployment, including troubleshooting steps taken and outcomes.
  - Document actions taken by both the UEM and Unit System Administrators.

7. References

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

Related Vendor References

- **Device Configuration Policies**: To create and manage device configuration policies using Intune, you can refer to the official documentation on Device profiles in Microsoft Intune.
- **Microsoft Intune Documentation**: For comprehensive information on using Microsoft Intune for device management, please visit the Microsoft Intune documentation.
- **MECM User Guide**: The official documentation for Microsoft Endpoint Configuration Manager (MECM) is available at Microsoft Configuration Manager documentation.
- **Security Policies**: To manage and secure devices using Microsoft Intune, you can refer to the Endpoint security policies in Microsoft Intune.

Related Texas A&M Controls

To ensure compliance with the following Controls in the Texas A&M Controls Catalog:

- Information System Monitoring (SI-4)
- Security Alerts, Advisories, and Directives (SI-5)

Related Internal Documentation

- ITEP Enterprise Device Management Change Control Process
- ITEP Enterprise Testing Validation

8. Revision History

Track changes made to the SOP over time.

Version	Date	Description of Change	Author
0.1	02/19/2025	Initial Draft	Jon Griffey
1.0	03/28/2025	Finalized SOP	Jon Griffey
1.1	04/09/2025	Formatting	Jon Griffey
1.2	07/16/2025	Updates	Jon Griffey
1.3	07/21/2025	Updates	Jon Griffey

Appendices

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

Additional Rules & Regulations

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

Process Diagram

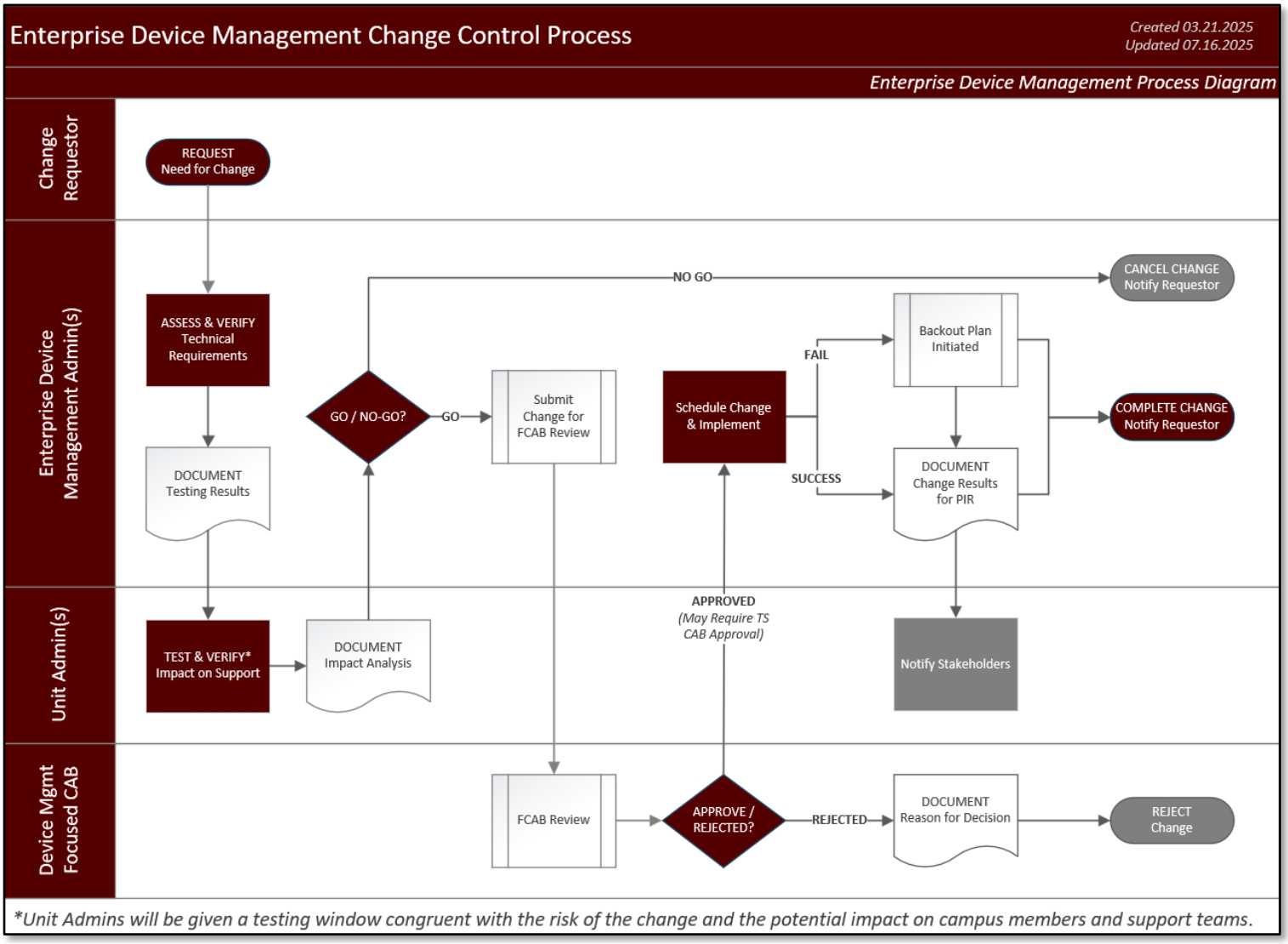

Figure 1: Enterprise Device Management Change Control Process.