MODERN MANAGEMENT

PROOF OF CONCEPT

Q4-2021

Modern Management – Roadmap

The following table illustrates several key next steps on the journey to modern management.

Work Stream	Outcome	Benefits
Modernize enforcement policies	• Migrate Config Manager Baselines and Client Policies • Migrate up to five Group Policy Objects	• Centralized management of endpoint policies • No longer need to maintain .admx files in AD for endpoints
User segmentation / persona	• Define 8 – 10 segments • Capture hardware and software standards • Establish service level and warranty standards • Define policy, access, data, security standards • Optimize M365 licenses	• Elimination of exceptions • Elimination manual configuration steps • Identification of GAPS, preventing modern management
Application rationalization	• Rationalize software estate • Roadmap to address compatibility • Profile standards	• Eliminate redundant applications • Foundational for software asset management • Preparation for future publisher audits • Windows Store for Business
Tool optimization	• Elimination of legacy, non-supported, or difficult to support tools • Reduced infrastructure investment • Improved staff utilization	• Simplified management • Cost savings • Foundational to Unified Endpoint Management
Governance Structure	• Process for implementing policies, profiles and restrictions • Managed of Windows as a Service • Policy for adding/removing applications	• Foundational to Unified Endpoint Management • Persistent endpoint security posture • Improved supportability

Proof of Concept

PHASED APPROACH

01 Prepare

Discuss approach to PoC engagement, what's in-scope, overall Endpoint Management deployment goals, objectives and challenges. Also review what the Intune team's been releasing, roadmap and briefly touch on design and implementation.

02 Use-Case Scenarios

Determine use-case scenarios that support deployment goals and objectives. Also discuss Win10/11 management strategy.

03 External Dependencies

Discuss services and products that are separated from Intune but are either a requirement of Intune or might integrate with Intune.

04 Implement & Validate

Implement Intune and its external dependencies. Also discuss the approach to test and validate use-cases and the design previously discussed in the early stages of the PoC engagement.

Proof of Concept

In Scope

- Discovery/scoping calls to understand current environment, discuss the PoC scope and schedule/approach.
- Review external dependencies to expand use of Intune.
- Define configuration policies, profiles and restrictions per user segment / persona.
- Implementation:
  - Add user groups in Azure AD
  - Assign Intune and Office 365 user licenses
  - Set mobile device management (MDM) authority to Intune
  - Prepare device platforms for enrollment (iOS, Android, Windows)
- Add and deploy the following for each OS:
  - Terms and conditions policies
  - Device configuration policies
  - Resource profiles (Wi-Fi, VPN)
  - 2-3 Apps
  - 2 - 3 Azure AD Conditional Access policies
- Enroll up to 10 devices per OS
- Perform test and validation
- Monitor the success of the PoC
- Create action plan to remediate issues
- Knowledge transfer and deployment support will conclude with skill transfer, and delivery of document

Deliverables

- Intune design that fits organization’s deployment goals and objectives
- New Intune environment implemented

Optional Services

- Comprehensive user segmentation
- Full modernization of device enforcement policies

Work Stream 1: USE CASE SCENARIOS

Activities

Define device ownership scenarios (*examples*)

- Corporate-owned devices
- BYOD devices
- Shared devices
- Shop floor devices

Define primary and sub-use cases (*examples*)

- Corporate
  - Corp Standard Enrollment
  - Kiosk
  - Any other custom use cases
- BYOD
  - Mobile Application Management Policies (MAM)
  - Enrollment vs MAM without Enrollment

Align use case scenario to user segment/persona and device platform (i.e. operating system).

Cross-walk GPOs and other device enforcement policies to configuration profiles.

Define per-app deployment and management scenarios.

Define device compliance and conditional access policies.

Outcomes

- Groups created to organize users or devices by geographic location, department, or hardware characteristics.
- Device ownership scenarios established.
- Initial set of policies and profiles created.

Requirements

- Client security stakeholders to confirm policy definitions and approach for BYOD and Corporate use cases.
- Client Desktop Engineering and Support Team representation
- Client to provide 3 – 5 GPOs to convert
- Client to provide 2 – 3 configuration baselines
- Client to provide 2 – 3 configuration profiles
- Client to identify applications for POC user segments

Work Stream 2: IMPLEMENT & VALIDATE

Activities

Create user and device groups to determine the target of a deployment, including policies, applications, and profiles, adding AAD users or security groups, as needed.

Assign user and device (for shared devices) licenses.

Define per platform enrollment standards.

- Standard enrollment via Company Portal
- Device Enrollment Manager (typically for shared devices)
- Apple Device Enrollment Program
- Android enterprise
- Windows 10 Enrollment (OOBE or Company Portal)

Establish portal branding and user terms and conditions.

Define any enrollment restrictions.

Create configuration profile policies including:

- Hardware settings
- Password length and quality policies
- Application policies

Create device compliance policies.

Create conditional access policies.

Deploy various applications by platform and option.

Enroll devices.

Test and validate.

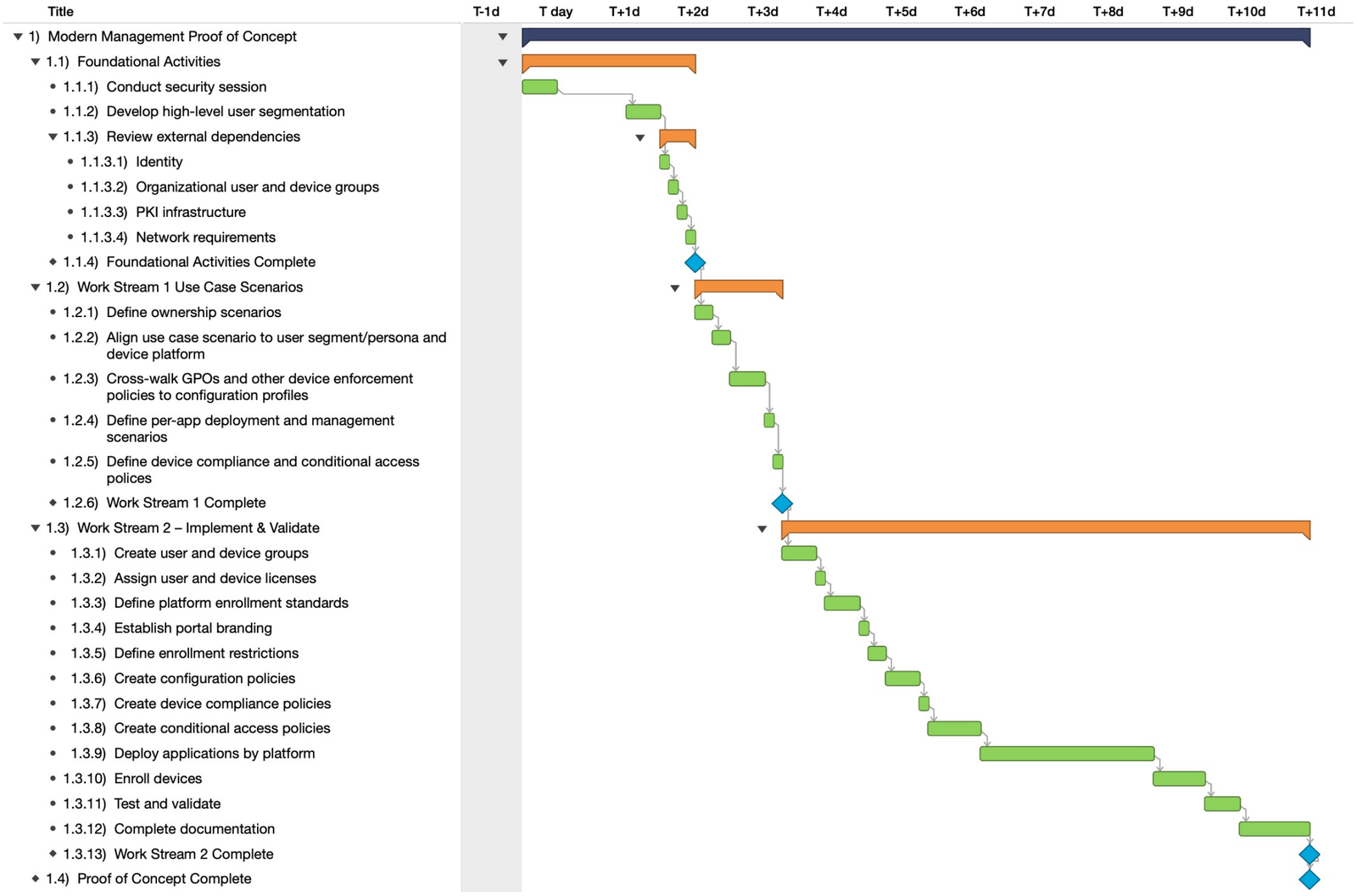
Outcomes

- Implemented device policies, profiles and compliance controls.
- Enrolled devices across use case scenarios.
- Tested and validated use case scenarios.

Requirements

- User personas and use cases defined from work stream 1
- Client to allocation technical test users for appropriate feedback
- Client to allocation users for shadowing MCPc engineers

Estimated Timeline



Proof of Concept

OUT OF SCOPE

- Product licenses (Microsoft or non-Microsoft) will not be provided under this Statement of Work. Customer is responsible for acquiring all necessary product licenses.
- Set up Azure AD identity environment along with the Azure AD connect tool;
- Hardware will not be provided under this Statement of Work. Customer is responsible for acquiring all necessary hardware, including mobile devices;
- MCPc will not be responsible for integration with 3rd Party Software;
- MCPc will not modify existing applications for any reason, including: to add functionality, fix defects, remediate existing issues, or integrate these applications with Intune;
- Enablement of Enterprise Mobility Suite functionality beyond Intune, such as Microsoft Information Protection, Cloud App Security and Microsoft Defender ATP;
- Remediation or upgrade of any existing on-premises upstream dependency for the solution such as existing Active Directory or Azure Directory Sync tool used;
- Implementation of Active Directory Federation Services (ADFS);
- Implementation of updates to Customer's external DNS records;
- Implementation of public key infrastructure (PKI) based infrastructure required to issue or manage certificates;
- Review or development of standard operating procedures for the customer IT organization.
- Drive communication plans for deployment;
- Drive Change or release management for any aspect of the project;
- Required certificate for Apple Push Notification Service for iOS device management;
- Deployment or configuration of an NDES server;
- Troubleshoot Microsoft cloud services or Microsoft on-premises products outside the scope of this Proof of concept engagement.

Functional Validation Testing – Example

Type	Name	Setting	Testing	Actual Result	Pass/Fail	Comments
Configuration policy	*Corp-Restrictions-iOS*	*Required PIN length of 6* *Block sending usage of diagnostic data to apple & ability to change setting* *Hide Apps – Prevent display of unwanted apps such as iTunes*	*Enroll device without a PIN, verify a PIN is requested and it meets quality requirements* *Confirm Diagnostics settings on device* *Confirm hidden apps are hidden.*	*6-digit PIN*	*Fail*	
Configuration Policy	*BYOD-iOS*	*Restrict iCloud backup*	*Attempt to backup iPhone to iCloud*	*Was unable to backup iPhone to iCloud*	*Pass*	
Mobile Application Management Policy *(enrollment not required)*	*IOS&Android-MAM-Unmanaged Devices*	*Force Pin & Encryption on all Office Apps Prevent screen shots and sharing data to unapproved apps*	*Confirm PIN enforcement on Device Confirm screenshots blocked*	*Office Apps force PIN use disallow screenshots and data being transferred to non-MAM protected apps*	*Pass*	*Policy applies w/out enrollment via company portal, policies apply by simply signing into application*

Use-Case Validation Testing – Example

Scenario	Testing	Actual Result	Pass/Fail	Comments
Configuration policy	*Enroll device in Intune*	*Enrollment was successful*	*Pass*	
	Download Outlook app from company portal	*Outlook app downloaded successfully*	*Pass*	*Download Outlook app from company portal*
	Open Outlook app and add work account	*Work account was easy to add*	*Pass*	
	Verify email synchronizes to the device and is able to be read	*Received quarantine email for non-compliance. iPhone did not meet iOS version requirement*	*Pass, once iOS updated*	*Send communication to end users re: iOS version minimum requirements.*
	Open Word attachments	*Open Word attachment*	*Pass*	*Open Word attachments*

Thank you!

Feel free to contact us if you have any questions.

msservices@mcpc.com