



John Marler
Brian Jenkins
Phil Overstreet
Alan Blitstein

Introduction & Agenda

- Who we are
- What we plan to talk to you about
 - *WorkspaceONE (WS1) vs Intune*
 - *The decision to migrate*
 - *Intune console preparation and related technologies*
 - *Redesigning mobile operation processes*
 - *Migrating workforce to Intune (~8,500 iOS/iPadOS devices)*
 - *Challenges and Lessons Learned*
- Q&A!

WorkspaceONE

- On-Prem
- Hub mobile app
- Granular payload capabilities
- Multiple tenants (Dev, QA, Prod)
- Boxer for BYO

Intune

- Cloud
- Company Portal mobile app
- Integrates with Azure AD & O365
- Single production tenant
- App Protection Policies (DLP)
- Conditional Access/Launch
- No enrollment BYO (MAM)



Why Move to Intune?

- Licensing and Cost Savings
- Move from On-Prem to the Cloud
- Interoperability with O365 ecosystem
- Ability to manage outlook client with more functionality like delivering certs

Company Portal vs Hub mobile apps

- New broker app
- CP lower maintenance for MOWs
 - Not needed to open monthly to get device info synced
- App store similarity to Hub, easy on end user

ABM, ADE, iOS Supervision

- Entry in ABM tenant
- ABM/Intune integration
 - *Vendors/resellers setup*
- Hard Supervision vs Soft Supervision desire
 - ADE helping to increase Supervision numbers
 - Allows more controls
- Self-service enrollment

MAM vs MDM

- Mobile Application Management vs Mobile Device Management
- Government Owned vs Personally Owned Devices
- APP – App Protection Policy for managed and unmanaged devices
- Conditional Access Conflicts for “Compliance” with MDM vs MAM
- DLP
- Conditional Launch
- Some application configs reserved for MDM only

Authentication

- Microsoft Authenticator/Azure Auth
- Goal to remove re-usable passwords
- Goal to use MFA – Multi Factor Authentication
- Meet NIST 800-63-3 AAL2
- Use Microsoft Authenticator to replace certificate authentication
- Re-authentication requirements

Microsoft Defender

- Proactively scans all links to see if they are malicious
- OS Updates
- Threat Score
- Security Center integration
- Conditional Launch Integration

User assignment, dynamic groups, and “optional profiles”

- Intune does not have “optional” profiles like Workspace one
- Intune does not have tags that have similar functionality to WS1
- Microsoft recommends user assignments for configurations and device assignment is limited
- Dynamic device groups showed to be slow to populate in our testing
- Solution: Accept user based assignments and create niche azure groups

Compliance

- No Compliance 'consequences' available
- Rethink Compliance for MDM
- Conditional Access
- Enhance with APP Conditional Launch
- Enhance with APIs/Scripting

Automation

- Evaluate existing Automation for WorkspaceONE (WS1) and compare
 - Do they make sense for Intune
 - Can they be replicated
- New APIs and API access method – Microsoft Graph API
- Azure Automation – Logic apps/Runbooks

Support changes

- Weekly training sessions
- Wiki knowledge repository
 - Mobile Support sections
 - Tier Zero sections
- Teams channel for Engineering/Support confluence
 - *Support can ask questions for quick wins/low hanging fruit*
 - *Alerts quickly distributed vs email overload*
- Built more self-service options to alleviate ticket count

Migration Strategy

- Manual Migration – around 8,500 iOS/iPadOS devices
- Heavy time investment in self-service instructions (critical to success)
- Pilot with IT partners
- Preparing support teams
- Automatic communications via ‘fake’ WS1 compliance policies
- Broke out migrations into 18 phases over 6 months
- PowerBI dashboard for tracking progress

Critical Success Factors

- Introducing Apple Business Manager
- Taking the time to understand Intune as comprehensively as WorkspaceONE
- Test, test, and test more
- Self-service instructions with screenshots
- Automating communications via WorkspaceONE

Challenges and Lessons Learned

- Challenges:
 - *New methods needed for automation/APIs compared to WorkspaceONE*
 - *Chasing down employees who ignored our messages to migrate*
 - *Intune console nuances (delays and slowness)*
 - *Microsoft changing things along the way*
- Lessons Learned:
 - *User assignment and filters significantly improved overall "speed" when compared to device groups*
 - *Exclusion groups and duplicate policies to effectively test in production*
 - *Intune ended up having the core functionality the team needed to succeed, even without all the bells and whistles of WorkspaceONE*

Questions?
Comments?

Thanks for listening!