

All-in with Azure AD, Intune, and Office 365

 Notes and Slides: billdeitrick.com/citn2019

Your Environments

Our Environment

Church

- PCs, Macs, Chromebooks, and iPads
- ~65 employees
- PC-dominated, moving to mix of above
- Traditional AD environment (with AADConnect); moving to Azure AD/Intune only

School

- PCs, Chromebooks, and iPads
- ~65 employees, ~400 students
- Employees all use PCs, students use Chromebooks (one-to-one for high school) and iPads
- Fully transitioned into an Azure AD-driven environment

Why Azure AD and Intune?

- Best fit for ministry needs within licensing and cost constraints
- Better Windows device management: NO MORE IMAGING!! 🚀
- Identity Consolidation
- Device-agnostic, user-driven, available-from-anywhere experience
- Forward-looking solution

M365: Two Minute Overview

- Office 365 ProPlus
- Office 365 - E1, E3, E5
- Enterprise Mobility Plus Security (EMS) - E3, E5
- Windows Enterprise - E3, E5
- Microsoft 365 (M365) - E3, E5
- Our Licensing Strategy
 - Users with org-owned Windows devices: M365 E3
 - Users without org-owned Windows devices: ProPlus, O365 E1, and EM+S
 - Users with no org-owned devices: O365 E1 and EM+S

"Azure AD is not Cloud AD"

- Goodbye NTLM, LDAP, Group Policy, and RADIUS; hello web services
- Azure AD manages applications
- Flat user structure; no more OUs or forests
- Can't customize the directory schema

Groups

- Two types of groups: Security and O365
- Three membership types: Assigned, Dynamic User, Dynamic Device
- Group-based licensing
 - Sec-[GROUP TYPE]-[GROUP NAME]

Connecting devices

- Azure AD Registered
- Azure AD Joined
 - Down-Level Logon Name: AzureAD\FirstLast
- Hybrid Azure AD Joined

Enterprise applications

- Administrative control of SSO with third-party apps
 - Hundreds of applications in the gallery
 - SaaS vendors and/or Microsoft will typically have documentation
- Azure AD as IDP for G Suite
 - Google "Cloud Identity Free" licenses
 - Web App Login: "Sign in with Google"
 - Chrome Sync with Azure AD logins
 - Azure AD logins on Chromebooks 🧐

Conditional Access

- Configure security controls to apply in specific scenarios
- Based on a variety of "signals", such as:
 - Group membership
 - IP Geolocation
 - Device (managed or not)
 - Application being accessed
 - Risk detection (depending on license)

Our Pain Points

- Security group nesting is...unpredictable
- Password changes on AAD-joined devices are...jarring

Intune

- Device configuration profiles
 - Assigned to devices or groups of devices (not OUs), not hierarchical like GPO
 - Administrative Templates
 - Custom Profiles/OMA-URI
 - Specify custom OMA-URI and values
 - Ingest Custom ADMX



Refresh

All products



 Search to filter items...



Setting Name



State



Setting ty...



Path

Prevent users from redirecting their Windows known folders to their PC

Enabled

Device

\OneDrive

Prevent users from syncing personal OneDrive accounts

Enabled

User

\OneDrive

Patching: No WSUS? No problem!

- Delivery Optimization
- Software Update Policy: Update Rings

 Create  Columns  Filter  Refresh  Export

 Search by name

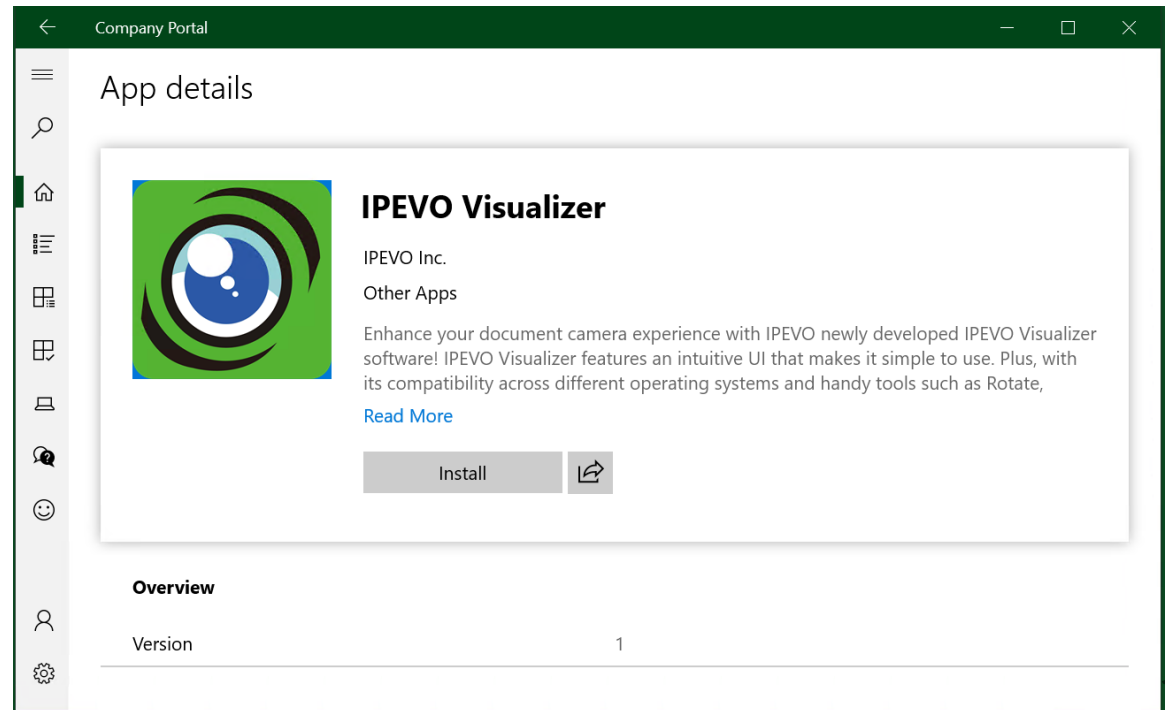
Name	↑↓	Feature Deferr... ↑↓	Quality Deferral ↑↓	Feature	↑↓	Quality	↑↓	Servicing chan... ↑↓	Assigned	↑↓
Fast Ring		60	7	Running		Running		SAC (Targeted)	Yes	...
Standard Ring		120	28	Running		Running		SAC (Targeted)	Yes	...

PowerShell Scripts

- Intune Management Extension deploys scripts and installs Win32 apps
- PowerShell Scripts can be run user or machine-scoped
- DO NOT put sensitive data into PowerShell scripts you push with Intune

App Deployment

- Types of apps that can be deployed on Windows:
 - Microsoft Store apps
 - Line of business apps (well-behaved MSI)
 - Windows app (Win32)
- Company Portal app



Our Pain Points






- App install error codes for Win32, MSI are often...unhelpful
- Built-in cloud-based printer deployment solution is...nonexistent
 - Needed third party product (Printix)
- Wi-Fi policies will report an error if pushed to a device without a Wi-Fi adapter, which we find...annoying
- Reporting intervals are...really slow 🐢

Getting Devices "Business Ready"


- Azure AD/Intune Integration
- Primary choice: User or IT-driven?
 - Self-enrollment methods
 - BYOD
 - Azure AD Join
 - Autopilot
 - Administrator-based enrollment methods
 - Hybrid Azure AD Join
 - Bulk enrollment
- Our process: Bulk enrollment, Fresh Start reset



Random Tasty Tidbits

-  BitLocker: Key escrow to Azure AD, Intune policy for automatic encryption
-  Azure AD Sign-in logs
-  Azure Cloud Shell
-  Intune: Compliance policies
-  Mobile App Management

Conclusion: Is this the right fit?

- What are your dependencies on traditional AD? Can they be eliminated?
 - LDAP, RADIUS, traditional Windows Auth
- Our goals:
 - Best fit for ministry needs within licensing and cost constraints
 - Better Windows device management: NO MORE IMAGING!!

 - SSO for SaaS apps
 - Mobile Application Management (MAM)
 - Device-agnostic, user-driven, available-from-anywhere experience
 - Most future proof solution

 billdeitrick.com/citn2019

 bill.deitrick@cwc.life

 @billdeitrick (CITN Slack)