Intune Mac Management
What’s new

September 2024

Arnab Biswas

Senior Product Manager

Microsoft Intune for Mac

Key takeaways

Security above all else

Establishing new standards across our products, operations, and culture to better protect ourselves and our customers.

Best managed Mac experience for M365 customers

Cloud-native management delivering scalable, reliable, and secure macOS experiences.

Simplify and consolidate endpoint management

Cut cost and complexity while unifying endpoint management and security tools – All you need is Microsoft 365.

Generative AI and automation simplify IT

Unlock better outcomes for IT and end-users through data, end-to-end context and automation.

How Intune manages Macs

“Create the best managed Mac experience for Microsoft 365 customers.”

Platform-first

Native apps

Day zero support for new macOS versions

Supports next-gen declarative management

MDM+

Intune agent enhances native macOS MDM

Extends admin control

Secure productivity

Microsoft 365

Conditional Access

Phish-resistant auth

Comprehensive security, compliance and data governance tooling with Defender, Sentinel, Purview

Intune macOS capabilities

Endpoint Security

- Firewall
- FileVault (Disk Encryption)
- Gatekeeper
- Activation Lock
- Rapid Security Response

Conditional Access

- Device Compliance

Enrollment

- ADE with Modern Authentication
- Local Account Management
- Await final configuration
- Platform SSO and passkeys
- Hardware-bound Entra registration

Scripting

- User / Root scripts with schedules
- Can use any interpreter (Bash, ZSH, Python, etc.)
- Custom attribute collection using scripts
- Log collection

Configuration

- Entra ID Single Sign-on Extension
- LDAP (AD)
- Restrictions policies
- Custom Policy support (iMazing)
- Passcode policies
- Software Update
- Enterprise Certificates / PKI
- Network configuration / Proxy server
- Login Window
- Managed Login Items
- Content Caching
- Settings picker
- Device Actions (Erase, Restart, etc.)
- DDM Software Update
- FileVault during Setup Assistant

Intune Suite

- Remote Help with full control
- Cloud PKI

Apps

- DMG, PKG support with available assignment
- Custom PKG pre-install and post-install scripts
- Volume-purchased apps
- Native integrations for Edge, Office and Defender
- Config for Edge, Office, Defender and OneDrive
- Custom Preference

3rd Party Integration

- Munki integration (App Lifecycle)
- Privileges (Elevation control)
- Santa (Binary Access control)
- Octory (Onboarding splash screen)
- Nudge (OS Update Controls)

Coming soon

- Managed device attestation with ACME
- macOS Recovery lock management
- User channel support for resource access profiles
- JIT compliance remediation
- Custom app detection
- Script size increase to 1 MB

Intune Mac Onboarding

Demo

Coming soon

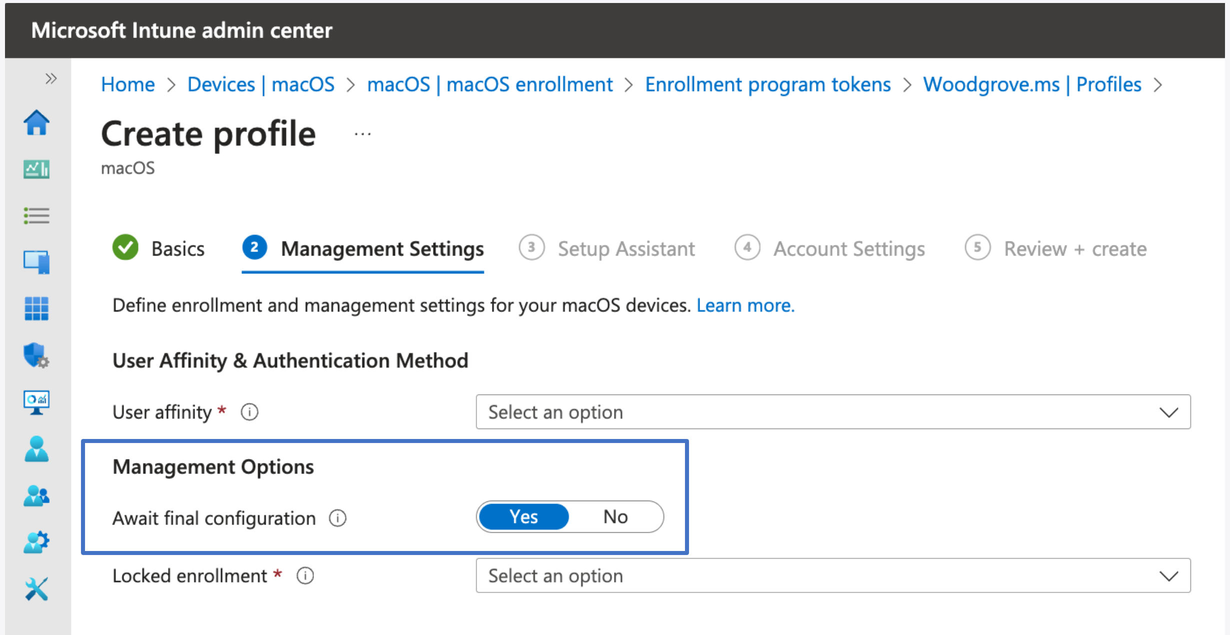
Managed device attestation with ACME

- ACME: Automated Certificate Management Environment (macOS 13.1+).
  - More secure than SCEP.
  - Bound to Secure Enclave.
- Attestation is the strongest proof of hardware-bound device identity that is attested to by Apple (macOS 14+).
  - Managed Macs can provide the trusted attestation to prove device identity to servers.
  - Initiated via MDM, it protects the Intune enrollment cert against spoofing.
  - The security benefits also extend to Resource Access profiles.

Available

Await configuration after Automated Device Enrollment

- Create a more secure onboarding experience by guaranteeing that the Mac is configured before releasing to the user.
- User remains within Setup Assistant experience until first device check-in completes.



Microsoft Intune admin center

Home > Devices | macOS > macOS | macOS enrollment > Enrollment program tokens > Woodgrove.ms | Profiles >

Create profile ...

macOS

✓ Basics   2 Management Settings   3 Setup Assistant   4 Account Settings   5 Review + create

Define enrollment and management settings for your macOS devices. Learn more.

User Affinity & Authentication Method

User affinity * ⓘ Select an option

Management Options

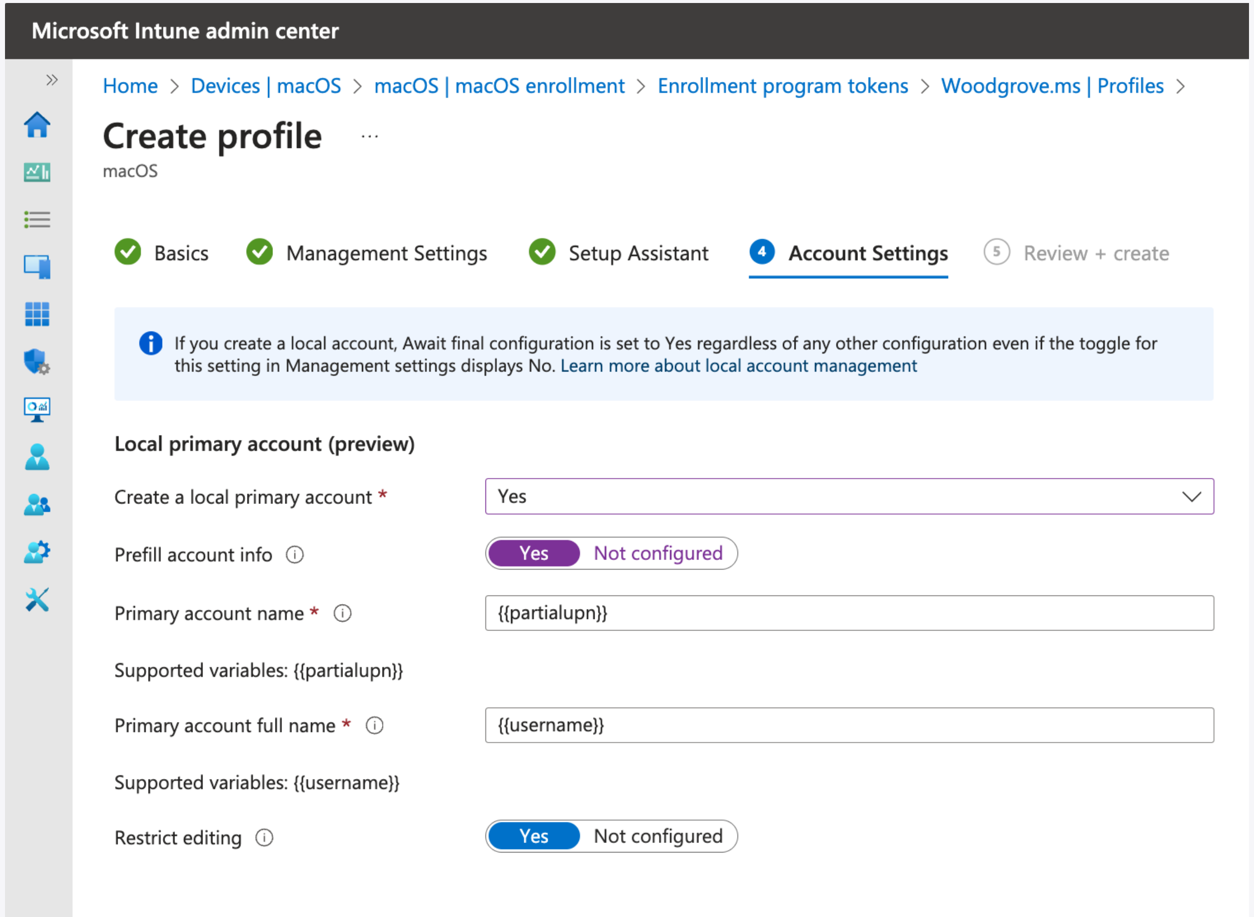
Await final configuration ⓘ [✓ Yes] No

Locked enrollment * ⓘ Select an option

Available

Account management

- Create and configure local admin & primary account on auto-enrolled Macs during enrollment.
- Standardize how local accounts are named.



Microsoft Intune admin center

Home > Devices | macOS > macOS | macOS enrollment > Enrollment program tokens > Woodgrove.ms | Profiles >

Create profile ...

macOS

✓ Basics ✓ Management Settings ✓ Setup Assistant 4 Account Settings 5 Review + create

If you create a local account, Await final configuration is set to Yes regardless of any other configuration even if the toggle for this setting in Management settings displays No. Learn more about local account management

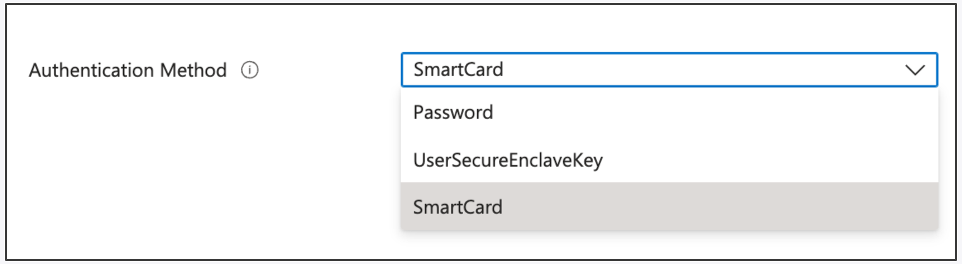
Local primary account (preview)

Create a local primary account *	Yes
Prefill account info ⓘ	[✓ Yes] Not configured
Primary account name * ⓘ	{{partialupn}}
Supported variables: {{partialupn}}	
Primary account full name * ⓘ	{{username}}
Supported variables: {{username}}	
Restrict editing ⓘ	[✓ Yes] Not configured

Public Preview

Platform SSO: Overview

- Entra ID platform’s integration with built-in macOS APIs on macOS 13+.
  - Included with Intune.
- Extends auth with Entra ID to the macOS lock screen, provided WHfB-like sign-in & SSO experiences.
- Leverages the Enterprise SSO Plug-in enabled via SSO extension profile.
- Choose one of the supported authentication methods:
  - **Password synchronization** with Entra ID
  - **Password-less SSO** on device, enabled by hardware-backed credential – analogous to WHfB (Microsoft recommends)
  - **Smart card-based** device sign-in



Authentication Method: SmartCard

- Rights management for Entra users on the Mac.

Public Preview

Platform SSO & Passkeys

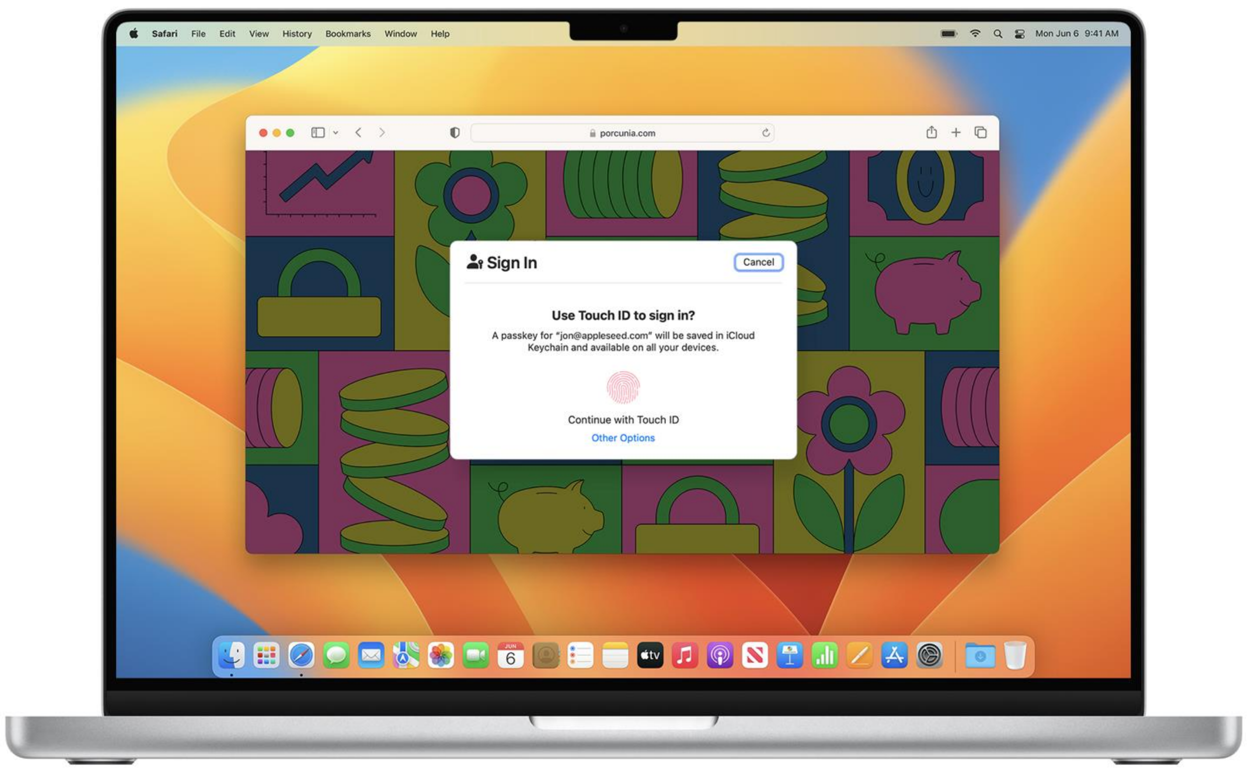
Passkeys can’t be phished and replaces passwords.

Allows using Touch ID or Face ID to sign in to apps and websites.

Passkeys for managed accounts are enabled using Platform SSO, when “Secure Enclave” is chosen as the authentication method.

Managed identities don’t sync to personal iCloud.

Passkeys for enrollment are enabled using Entra Authentication Methods.



Use Touch ID to sign in?

A passkey for “jon@appleseed.com” will be saved in iCloud Keychain and available on all your devices.

Authentication method strengths in PSSO

	Good: Password	Better: SmartCard	Best: Secure Enclave
Local account password sync with Entra ID	☑	☒	☒
Federation support	☑	☑	☑
MFA required for registration	☒	☑	☑
Phishing resistant	☒	☑	☑
Phishing resistant via built-in Apple hardware	☒	☒	☑
Passkey usage	☒	☒	☑

- Microsoft recommends Secure Enclave as the authentication method.
- Better/best options are superior to password-sync solutions even when using MFA.
- US federal govt is mandating phish-resistant auth.

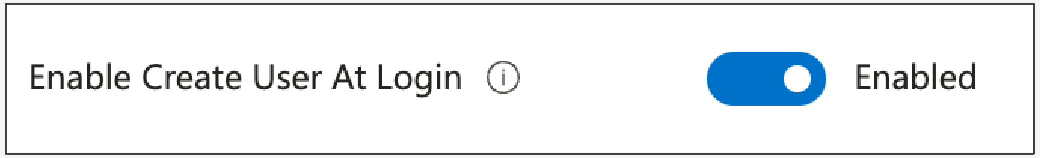
Passkey in Automated Enrollment

Demo

Public Preview

Platform SSO: User creation & privileges

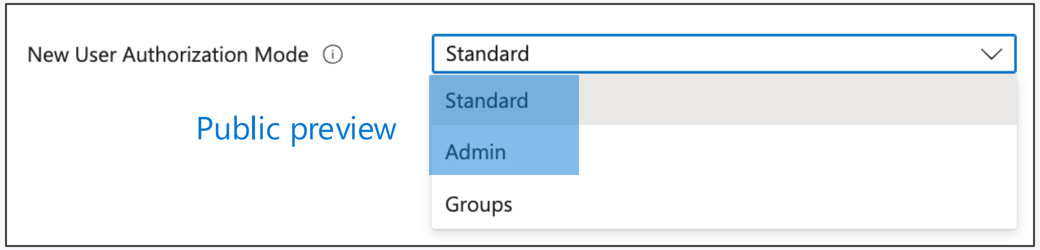
- Enable Entra ID user creation at login window.
  - Requires deploying login items payload to show “other” user option.



Enable Create User At Login

Enabled

- New user authorization mode.
  - User rights for the first session.

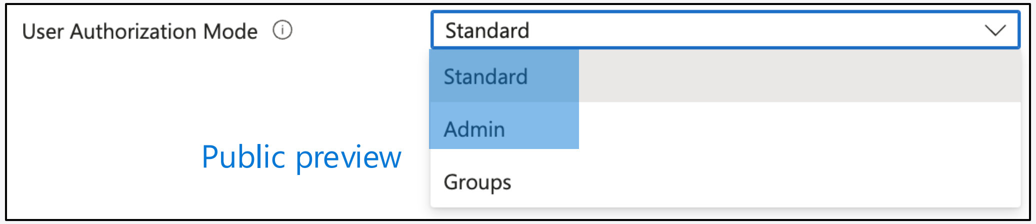


New User Authorization Mode

Standard

Public preview

- User authorization mode.
  - Persistent user rights for second session onwards.
  - Can be manipulated to elevate privileges for a session.



User Authorization Mode

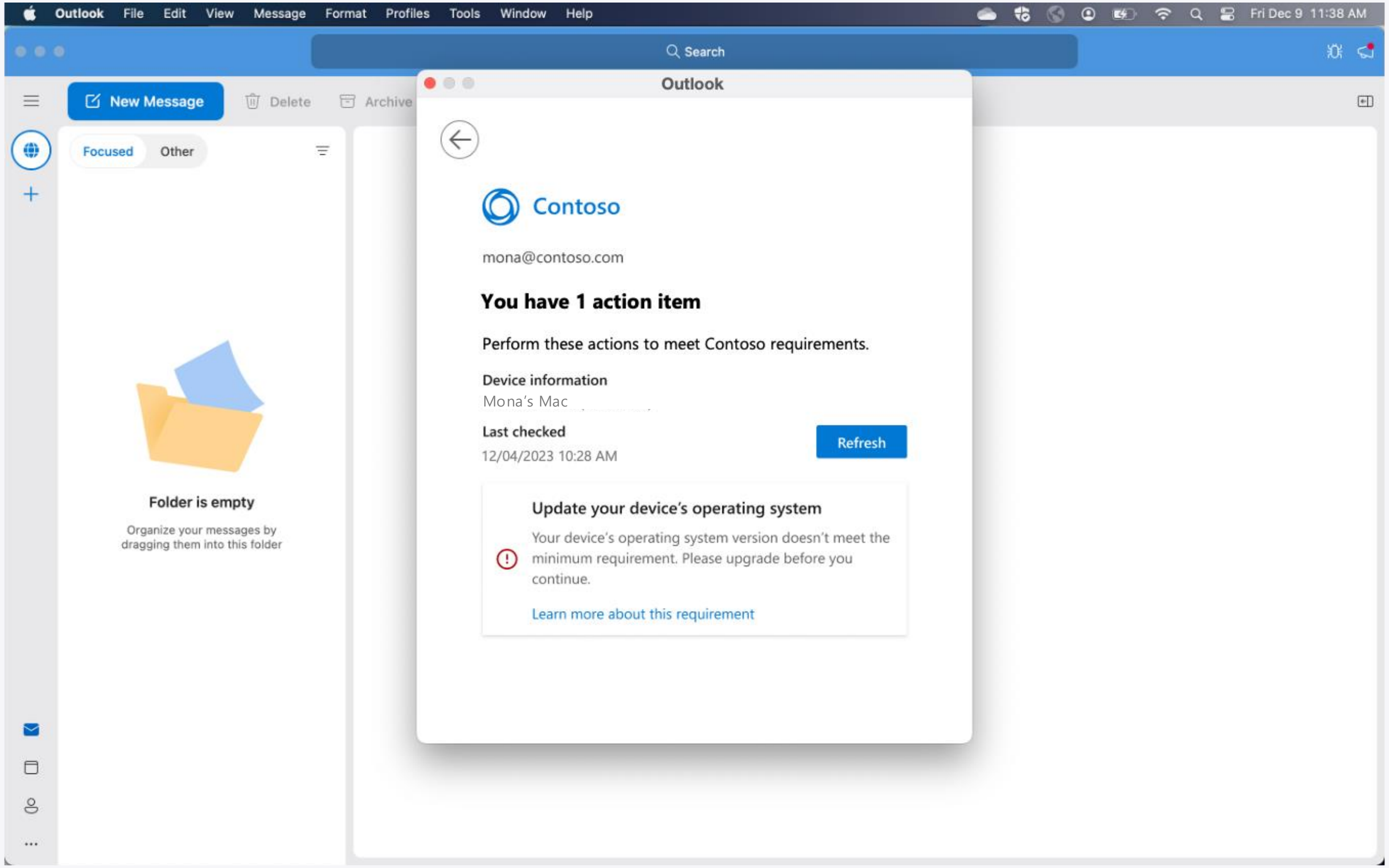
Standard

Public preview

Coming soon

“Just-in-time” Compliance

- Noncompliance detection and remediation experience from within protected apps.
- Company Portal app is not required!



Folder is empty

Organize your messages by dragging them into this folder

Outlook

Contoso

mona@contoso.com

You have 1 action item

Perform these actions to meet Contoso requirements.

Device information
Mona’s Mac

Last checked
12/04/2023 10:28 AM

Refresh

Update your device’s operating system

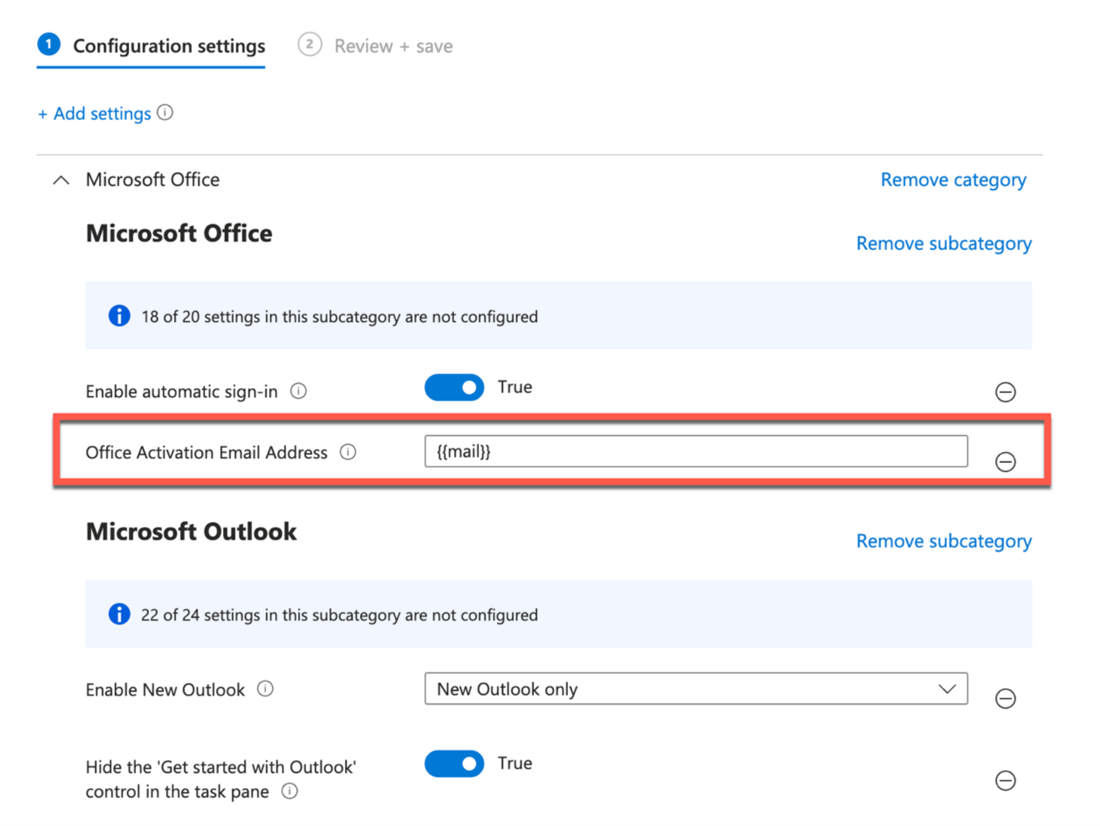
Your device’s operating system version doesn’t meet the minimum requirement. Please upgrade before you continue.

Learn more about this requirement

Available

Settings Catalog

- Automated settings ingestion system.
- **Built for day-zero support:**
  - Minimized time to develop new settings from 8+ weeks to:
    - ~3 days for Sonoma
    - ~24 hours for Sequoia
  - Microsoft app preferences including variables
- Once ingested, new payloads are immediately tested for deployment.
- **Built for the future:**
  - DDM declarations
  - Data reference architecture



Microsoft Office

18 of 20 settings in this subcategory are not configured

Enable automatic sign-in: True

Office Activation Email Address: {{mail}}

Microsoft Outlook

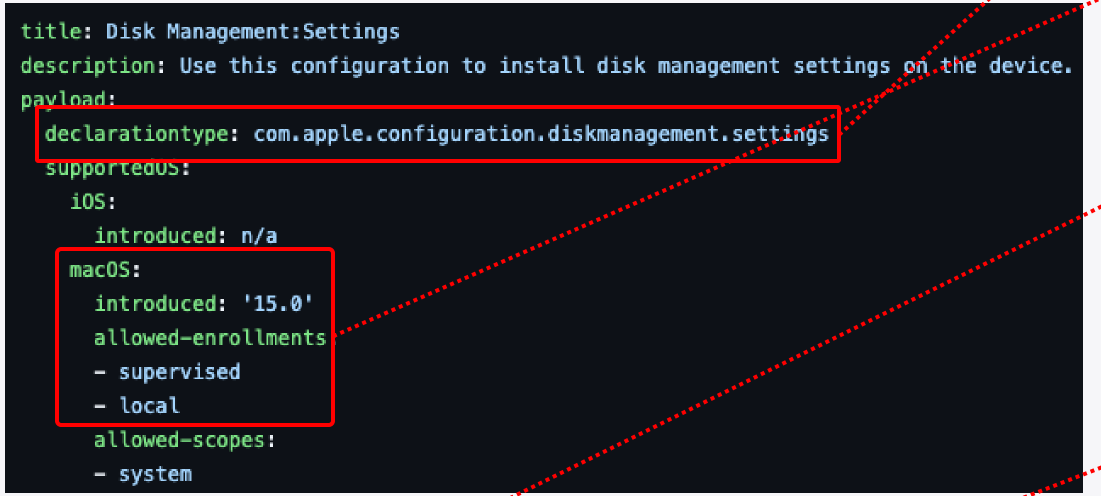
22 of 24 settings in this subcategory are not configured

Enable New Outlook: New Outlook only

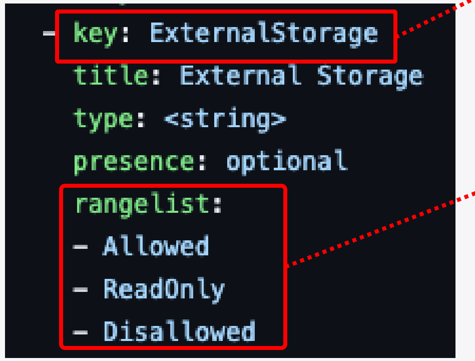
Hide the 'Get started with Outlook' control in the task pane: True

Available

Settings catalog in action

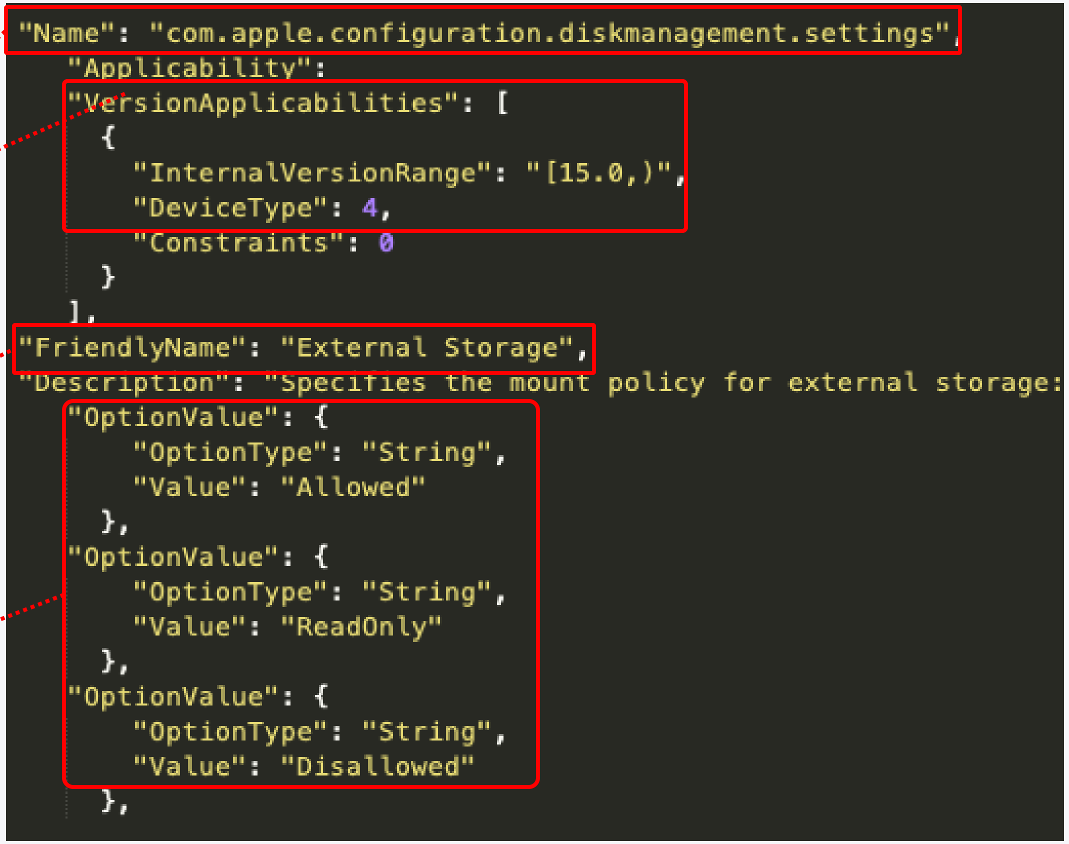


```
title: Disk Management:Settings
description: Use this configuration to install disk management settings on the device.
payload:
  declarationtype: com.apple.configuration.diskmanagement.settings
  supportedOS:
    iOS:
      introduced: n/a
    macOS:
      introduced: '15.0'
      allowed-enrollments:
      - supervised
      - local
      allowed-scopes:
      - system
```



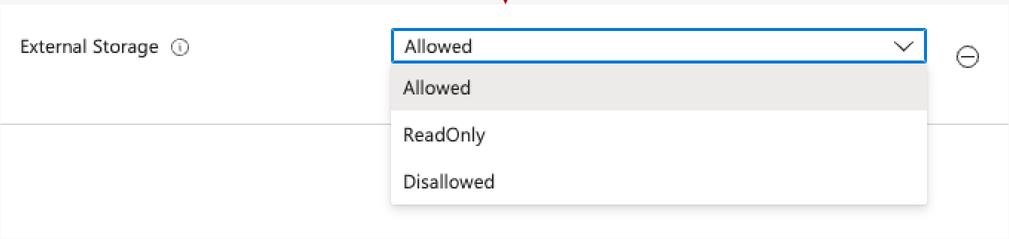
```
  - key: ExternalStorage
    title: External Storage
    type: <string>
    presence: optional
    rangelist:
    - Allowed
    - ReadOnly
    - Disallowed
```

1. Apple YAML



```
"Name": "com.apple.configuration.diskmanagement.settings",
   "Applicability":
   "VersionApplicabilities": [
     {
       "InternalVersionRange": "[15.0,)",
       "DeviceType": 4,
       "Constraints": 0
     }
   ],
"FriendlyName": "External Storage",
"Description": "Specifies the mount policy for external storage:
   "OptionValue": {
       "OptionType": "String",
       "Value": "Allowed"
     },
   "OptionValue": {
       "OptionType": "String",
       "Value": "ReadOnly"
     },
   "OptionValue": {
       "OptionType": "String",
       "Value": "Disallowed"
     },
```

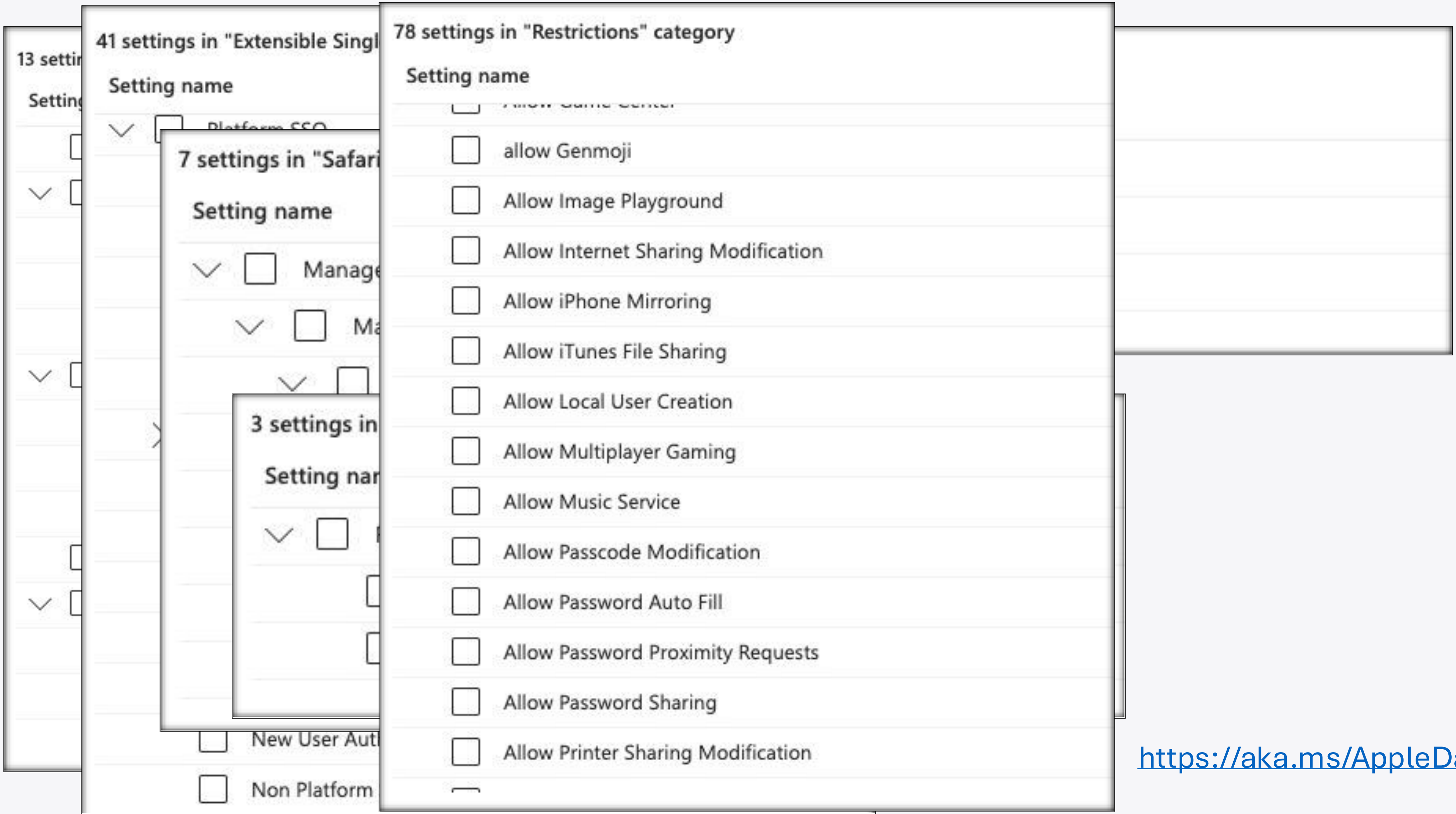
2. Processed JSON understood by Apple Settings Catalog



External Storage ⓘ — Allowed

Available

New in setting catalog



13 settir

Settin

41 settings in "Extensible Singl

Setting name

□ Platform SSO

□ New User Aut

□ Non Platform

7 settings in "Safari

Setting name

□ Manage

□ Ma

3 settings in

Setting nar

78 settings in "Restrictions" category

Setting name

□ Allow Game Center

□ allow Genmoji

□ Allow Image Playground

□ Allow Internet Sharing Modification

□ Allow iPhone Mirroring

□ Allow iTunes File Sharing

□ Allow Local User Creation

□ Allow Multiplayer Gaming

□ Allow Music Service

□ Allow Passcode Modification

□ Allow Password Auto Fill

□ Allow Password Proximity Requests

□ Allow Password Sharing

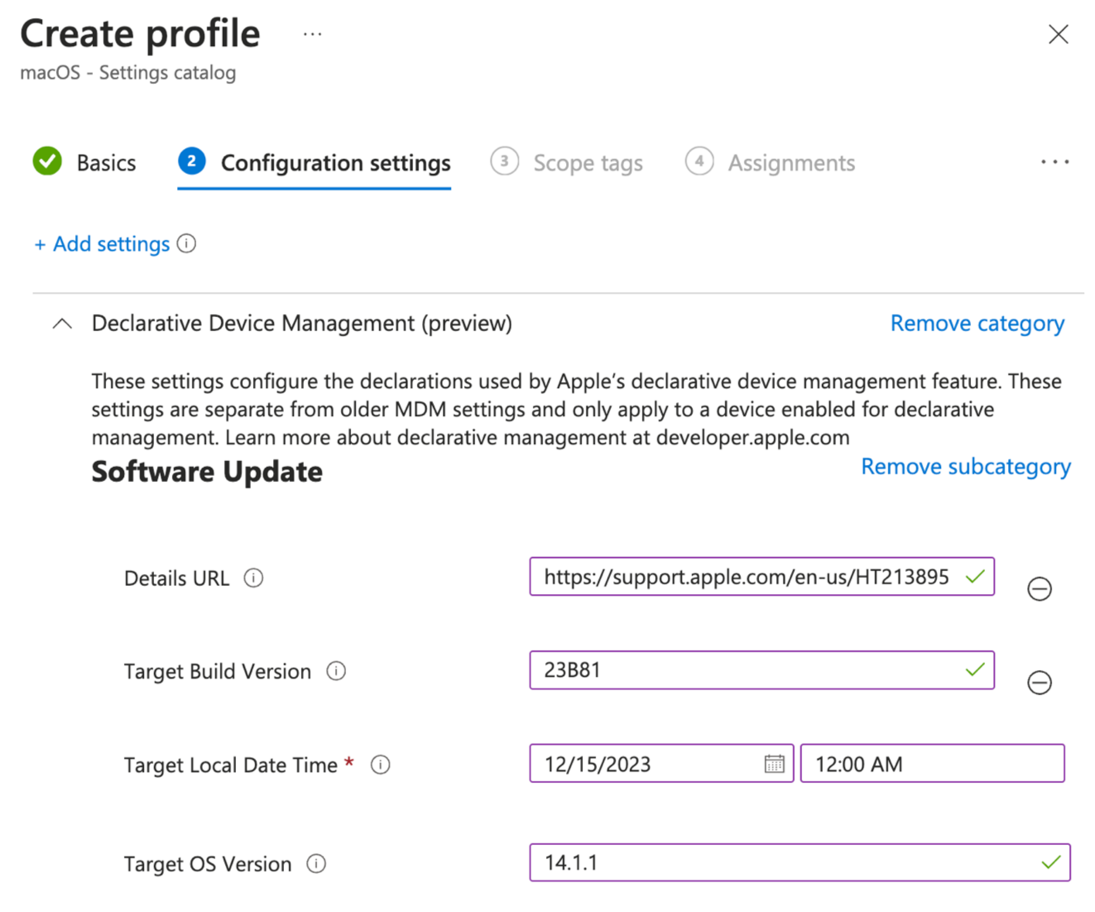
□ Allow Printer Sharing Modification

https://aka.ms/AppleDayZero

Available

Declarative software updates

- DDM configuration for software update enforcement.
- Specify OS version or build to install by an exact time.
- System notifications and deadline are managed by macOS.



Create profile

macOS - Settings catalog

Declarative Device Management (preview)

These settings configure the declarations used by Apple's declarative device management feature. These settings are separate from older MDM settings and only apply to a device enabled for declarative management. Learn more about declarative management at developer.apple.com

Software Update

Details URL	https://support.apple.com/en-us/HT213895
Target Build Version	23B81
Target Local Date Time *	12/15/2023 12:00 AM
Target OS Version	14.1.1

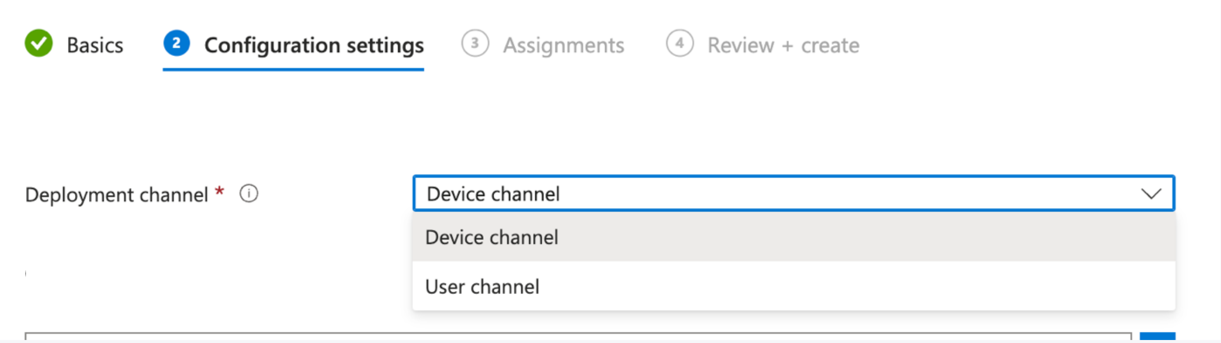
Declarative Software Updates

Demo

Coming soon

Resource access profiles via user channel

- Enable admins to choose in which keychain (device/user) RA profiles or certificates are delivered.
- By default, “device channel” is used, and the profile applies to any user logging in.
- Profiles in scope:
  - SCEP
  - PKCS
  - WiFi
  - VPN
  - Wired network
  - Trusted (root) certificate



Deployment channel * : Device channel

Available

macOS app management

Managed apps

Flat PKGs installed using MDM.

Simplified app upload.

Intune app wrapping tool is no longer needed.

Will take advantage of DDM improvements.

Purchased and custom apps are also supported.

DMG apps

Most common Mac apps.

Easy to create with macOS Disk Utility.

Intune supports DMGs containing one or more apps (not .zip).

Deployed using Intune agent.

Expanded up to 8 GB per app.

Flexible PKG installers

Great for deploying unsigned, component, or custom (non-flat) packages.

Uses built-in installer command.

Pre and post install scripts.

Deployed using Intune agent.

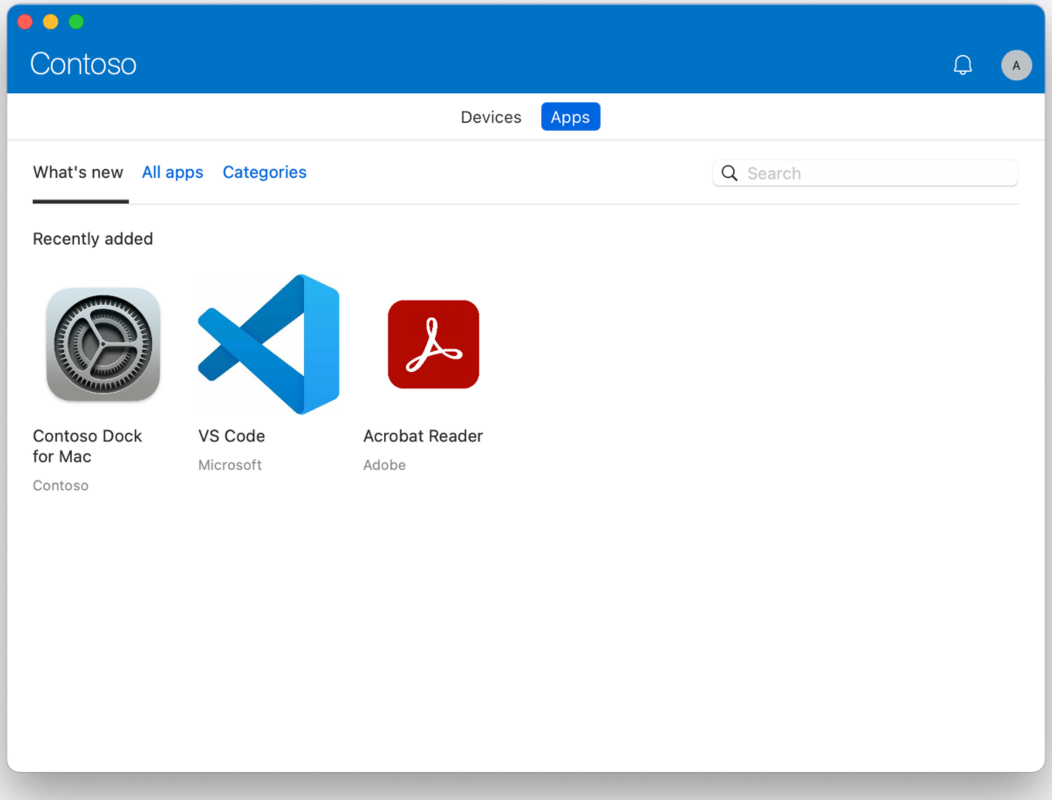
Expanded up to 8 GB per app.

Custom app detection – Coming soon

Available

Agent-installed PKG & DMG as available apps

- Brings the flexibility of app browsing and on-demand install to end-users on Mac Company Portal
- Payload-free packages can be deployed for self-service actions in Company Portal
- How agent-installed apps are detected:
  - (1) built-in search OR (2) Spotlight (`mdfind`) OR (3) install receipt



Recently added

Contoso Dock for Mac
Contoso

VS Code
Microsoft

Acrobat Reader
Adobe

Available apps & actions

Demo

Coming soon

Custom app detection for PKGs

- Provide greater flexibility for admins to define detection logic for PKGs using shell scripts within PKG app policy.
- Admin will be able to choose between “built-in” and “custom” detection options.
- “Custom” option will require a script that will be run before and after the PKG is installed.
- Reporting options:
  - return 0 = success
  - return 1 = failed

Intune Analytics and Automation Roadmap

1 Data as the foundation of modern IT

Asset discovery and Inventory

A rich catalog of attributes from Intune managed entities (devices, apps)

Audit logs

Track and monitor events within your organization with a comprehensive record of all actions taken within Intune

Custom attributes

Subscribe to additional attributes from an extensive catalog with contributions by OEMs and partners

2 End To End Context

Device querying

Quickly assess the state of devices in your environment with filtering and aggregation

Custom dashboarding

Summarize large amounts of data and generate a visual representation of any part or aspect of your IT infrastructure

AI/ML Analytics

Feed data for clustering, anomaly detection, and other algorithms

3 Automation to simplify IT

Execute one-time action

Run a device or backend action, script, remediation -- against a list of devices

Apply configuration

Send a permanent payload or configure policy to each device meeting the specified criteria (e.g., upgrade app version, block app)

Dynamic workflows

Orchestrate policy, app, device configuration workflows based on attributes through a modern, no-code interface

Cross-platform

iOS

Resource explorer

Demo

Device query

Demo

Key takeaways

Security above all else

Establishing new standards across our products, operations, and culture to better protect ourselves and our customers.

Best managed Mac experience for M365 customers

Cloud-native management delivering scalable, reliable, and secure macOS experiences.

Simplify and consolidate endpoint management

Cut cost and complexity while unifying endpoint management and security tools – All you need is Microsoft 365.

Generative AI and automation simplify IT

Unlock better outcomes for IT and end-users through data, end-to-end context and automation.