Intune & Entra ID Automation

MDM On-Demand Actions ⚡

Live Analytics, Insights & Actions

Version 0.66

Written by Satish Singhi — March 2026 | GitHub Repository

Table of Contents

1. Overview & Mission
2. Highlights
3. Features — Group Management
4. Features — Device Management
5. Productivity Features
6. Prerequisites
7. Permissions
8. Safety, Validation & Auth Design
9. Getting Started
10. Roadmap

Overview & Mission

MDM-ODA is a PowerShell & WPF based plug-n-play tool for Entra & Intune on-demand operations. Built with attention to detail for the granular challenges faced by support teams, enabling project teams to get reliable, meaningful, up-to-date insights and reports on the go. Built with safeguards to prevent accidental actions, keeping Zero Trust and least privilege as top priority.

Project Mission

- To maximize operational efficiency
- To automate variety of On-Demand actions that need to be performed on the go
- To deliver a thoughtful, well-crafted experience that IT professionals genuinely enjoy using
- To bring together data from different portals/pages using a single page — no browser tab madness
- To surface actionable insights directly — no Excel exports, no manual pivot tables, just immediate clarity for faster triage
- To automate bulk actions on-demand that are natively not possible
- To reduce human errors using validation workflows
- To save hours of efforts and endless fatigue caused by repetitive tasks
- No manual setup needed, no admin rights needed — just plug and play
- To make Click-Ops great again

Highlights

Lightweight & Powerful

Enterprise-grade functionality with polished visuals, built entirely on native Windows components — PowerShell 7 and WPF. Zero third-party dependencies, zero licensing. All data is live from Microsoft Graph — no Power BI refresh cycles, no stale dashboards.

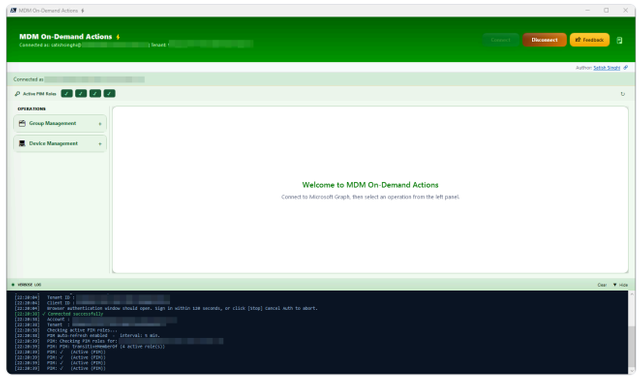
Security & Guardrails

Delegated auth flow for least privilege — use your Tenant & Client ID. Validation & preview before each write action. Live verbose logging for transparency. No admin rights required.

Productivity

Complex on-demand actions with minimum effort. In-page live table output with flexibility to select cells, copy individual cell/row/all, or export to XLSX.

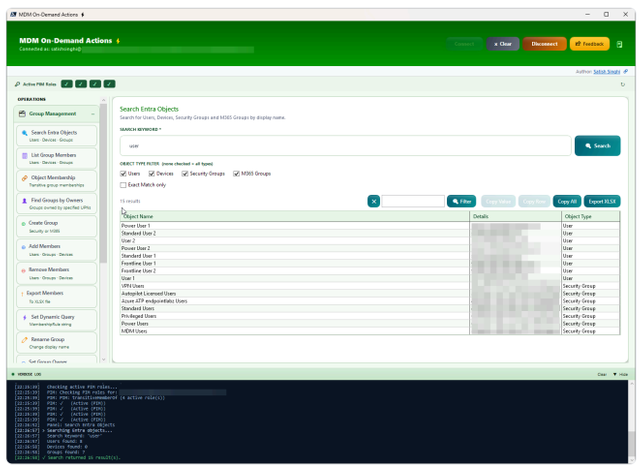
Features — Group Management



MDM-ODA Group Management interface showing all available operations

Search Entra Objects

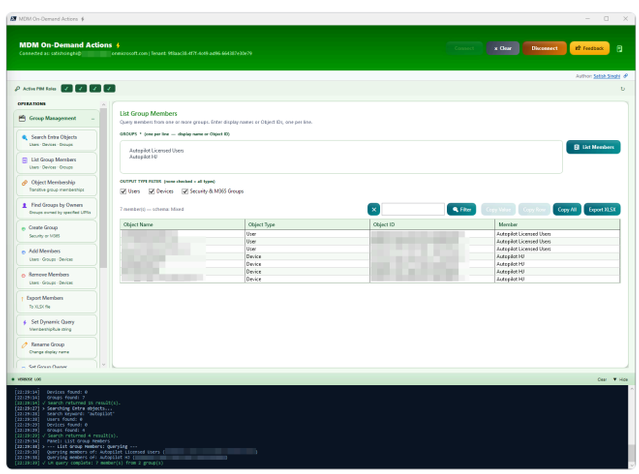
Keyword search across multiple Entra object types from a single page. Filter by object type using keywords.



Search across Users, Groups, Devices, and Service Principals with real-time filtering

List Group Members

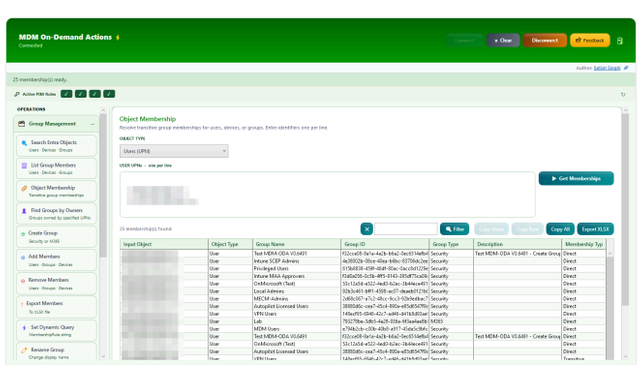
List members from multiple groups with a single click. View Object Name/UPN, Object Type, Object ID and source group.



Query members from multiple groups simultaneously with comprehensive details

Object Membership

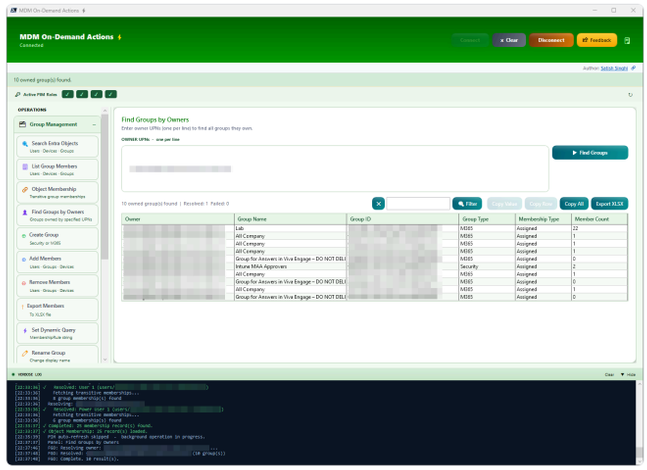
Find group membership for bulk items (Users/Devices/Groups).



Bulk lookup of group membership across users, devices, and groups

Find Groups by Owners

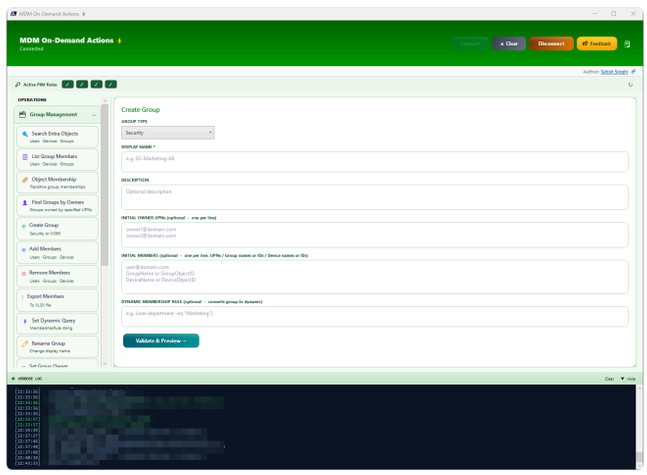
Enter UPNs, get all groups they own with Group Type, Membership Type, and Member Count.



Identify all groups owned by specific users with detailed ownership insights

Create Group

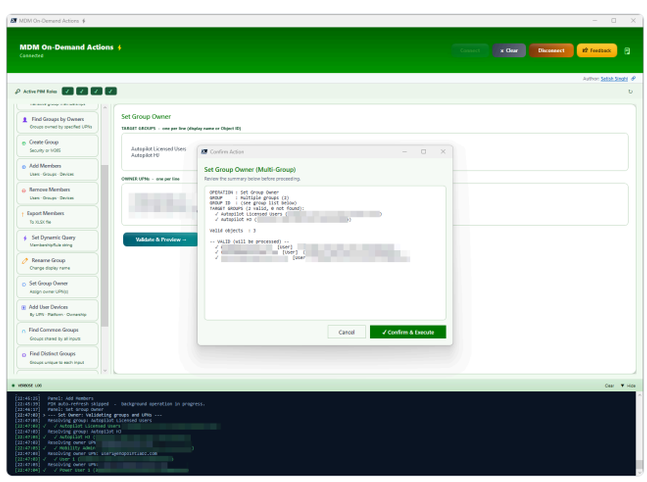
Create Security/M365 Group while assigning bulk owners and adding bulk members (UPN, Device Name/ID, Group Name/ID) or set a dynamic query — all from a single page. No CSV, no browser navigation.



One-page group creation with bulk owner assignment and dynamic membership rules

Set Bulk Owners on Bulk Groups

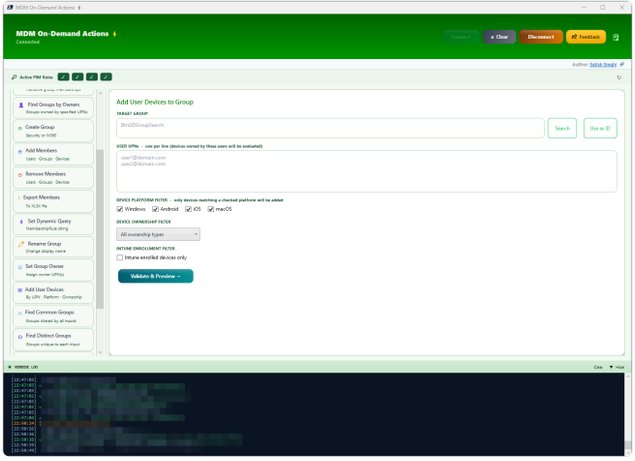
Many-to-many owner assignment. Un-owned groups haunt every organization — groups without owners or with outdated ownership cause confusion about use, purpose and accountability.



Assign multiple owners to multiple groups in a single operation

Add User Devices to Groups

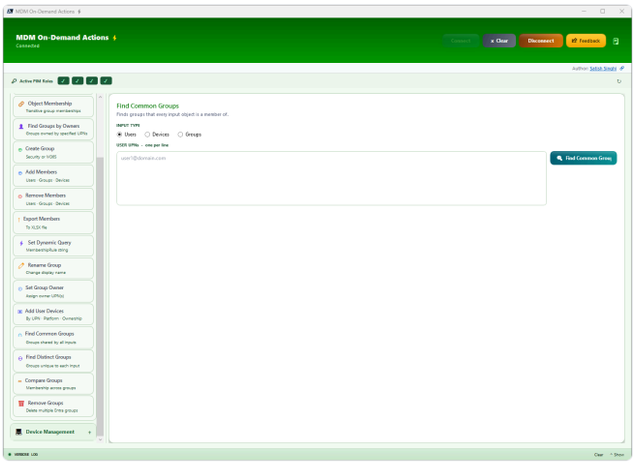
Game changer. Bulk add user devices to groups with filters for Platform, Ownership and Intune enrollment state. What was once a nightmare is now a cakewalk.



Intelligently add user devices to groups with comprehensive filtering options

Find Common/Distinct Groups

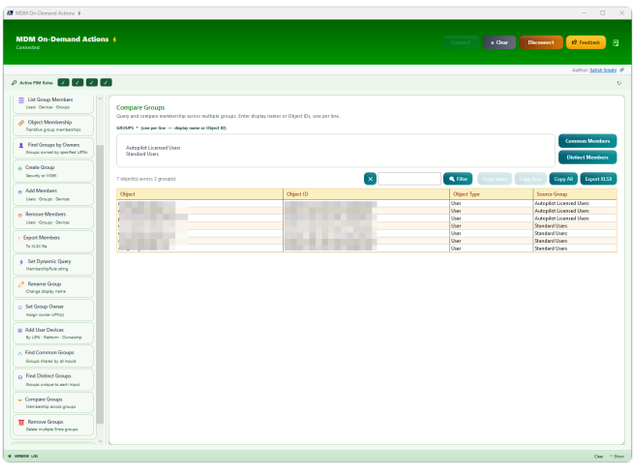
Compare multiple objects to find commonalities or distinction in group membership. No more CSV exports and VLOOKUPs.



Venn diagram analysis of group membership across multiple users or devices

Compare Groups

Compare members of multiple groups and identify Common or Distinct members between them.



Side-by-side group comparison with common and distinct member identification

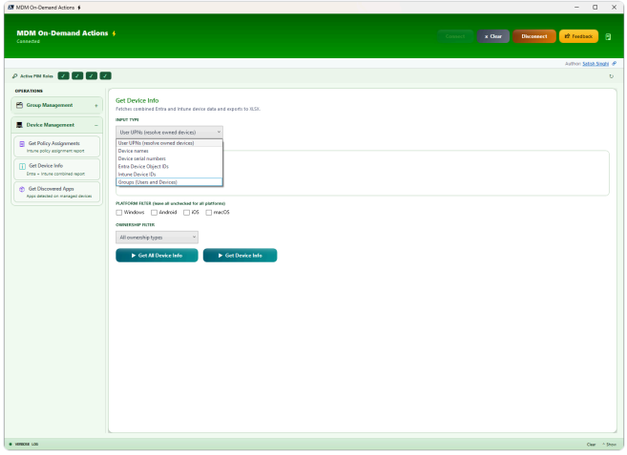
Additional Group Management Features

Beyond the primary operations above, MDM-ODA also supports **Remove Groups**, **Rename Groups**, **Set Dynamic Query on Existing Groups**, and **Export Members**. These operations follow the same validation-before-write paradigm and integrate seamlessly with the broader group management workflow. Additionally, **Bulk Group Removal** enables safe deletion of multiple groups with preview and confirmation steps, making organizational cleanup a structured and auditable process.

Features — Device Management

Device Info

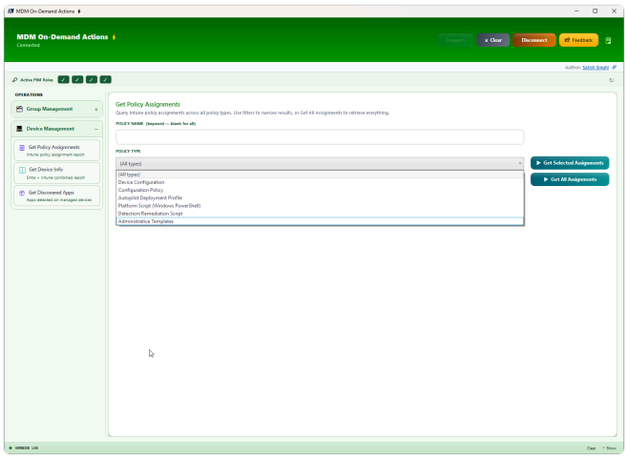
Comprehensive User & Device info from Entra & Intune based on UPNs, Serial Numbers, Object IDs and even User/Device Groups (recursive object detection). Uses filters for Platform & Ownership. Shows 30+ fields including Entra/Intune device details, OS info, ownership, activity ranges, Autopilot status, and user info.



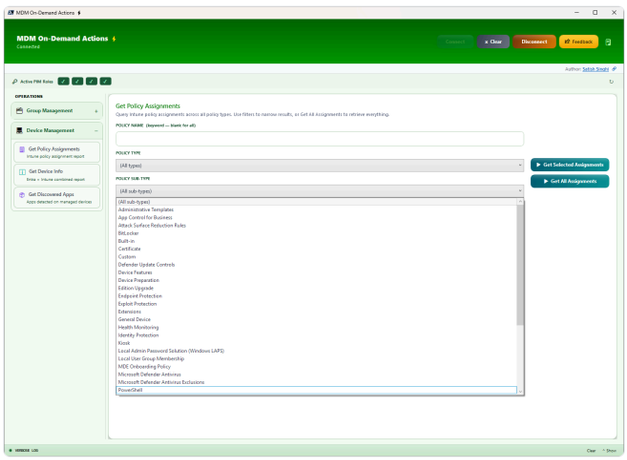
Unified device information from Entra ID and Intune with extensive field coverage

Intune Policy Assignments

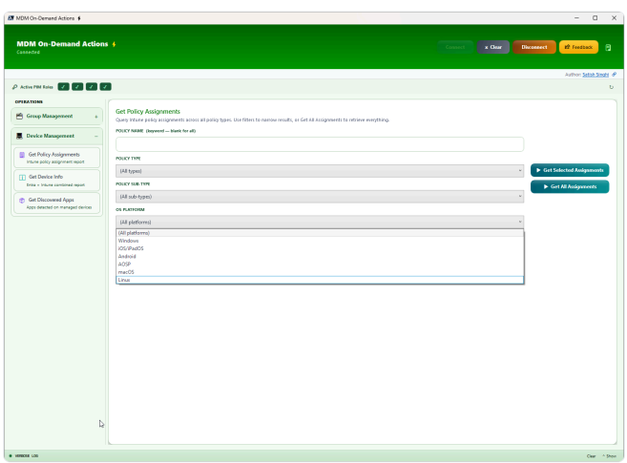
Runtime or project decisions, get instant insights about Intune policies, Assignment Groups, Assignment Filters and associated Filter Types. Generate output filtered by keywords, Policy Type, Sub-Type, OS platform.



Browse all Intune policies with assignment group visibility



Filter policies by type, sub-type, and platform for targeted insights

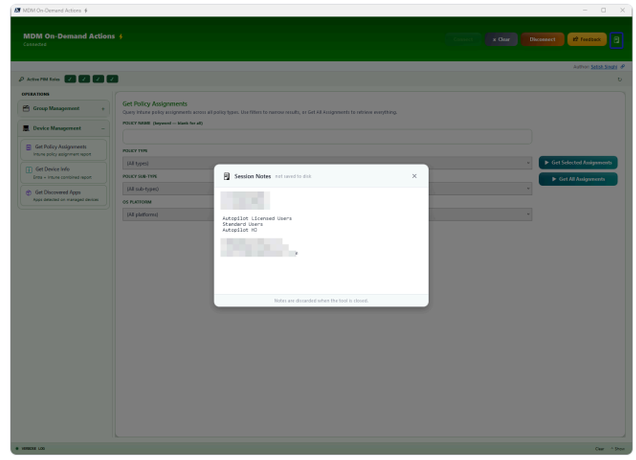


View assignment filters and their associated filter types

Productivity Features

Session Notes

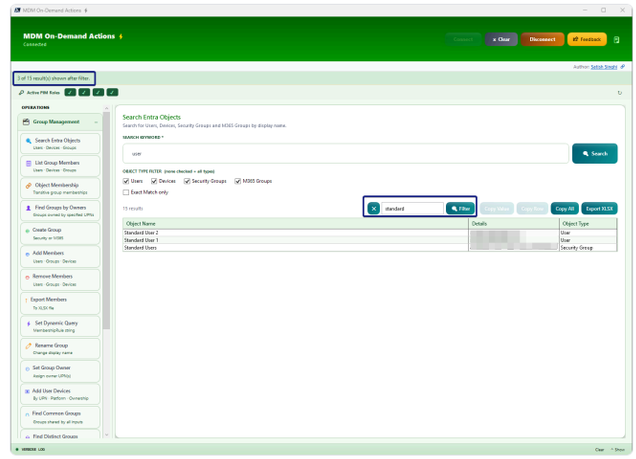
Built-in lightweight floating notepad, easy to bring up or minimize. Holds notes during the session, no disk storage.



In-session notes panel for quick reference and task tracking

Keyword Filter

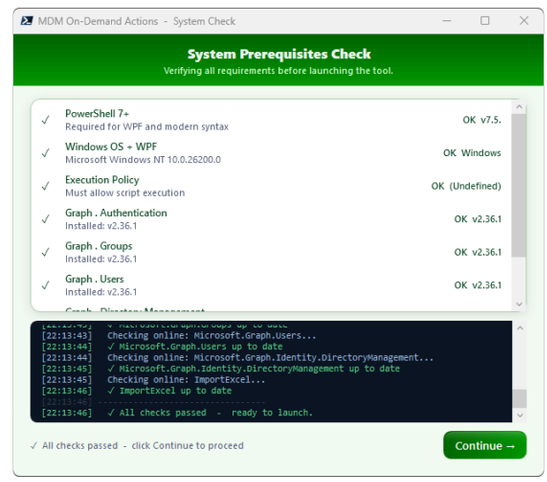
Every table output has a single filter across all columns. Type any keyword to instantly filter results across all columns in real-time.



Type any keyword to instantly filter results across all columns in real-time

Verbose Logging

Real-time verbose logging of every operation. Logs stored locally for audit trails and troubleshooting.



Real-time verbose log output showing operation progress and API call details

Additional Productivity Controls

- **Clear Inputs** — Clear the page and start fresh with a single click
- **Stop Operation** — Cancel ongoing operations at any time without waiting for completion
- **Feedback** — Built-in feedback mechanism to report issues or suggest improvements

---

Prerequisites

System Requirements

1. **Windows 11 with WPF**

   Windows Presentation Foundation is built-in to Windows 11. No additional installation needed.

2. **PowerShell 7**

   Handled automatically by the script. Auto-installs via winget if missing. Requires internet connectivity to PowerShell Gallery and GitHub winget repository.

3. **Internet Connectivity**

   Required for downloading PowerShell modules from PowerShell Gallery and for connecting to Microsoft Graph API endpoints.

4. **No Admin Rights Required**

   MDM-ODA runs in user context. Admin elevation is not necessary for standard operations.

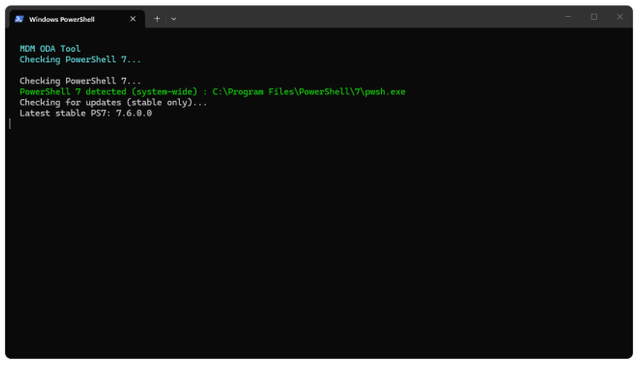
5. **Code Signing & WDAC**

   If Windows Defender Application Control (WDAC) or script execution policies are enforced, code signing adjustments may be needed. Consult with your security team if required.

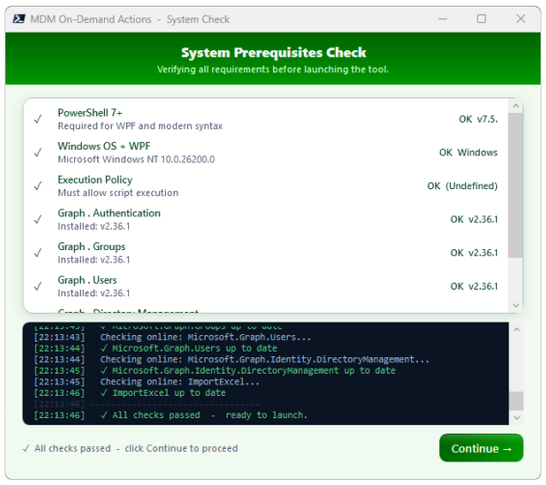
Prerequisite Handling

MDM-ODA includes automatic prerequisite detection and installation. The tool proactively checks for missing components and handles setup without manual intervention.

The orchestrator can be launched from a standard **PowerShell 5.1** host. On startup, it detects the running PowerShell version and, if PowerShell 7 is not already active, automatically locates or installs PowerShell 7 via `winget` — then re-launches itself in the PS7 runtime. This ensures the full WPF interface and Microsoft Graph SDK modules load correctly without any manual intervention from the user.



Automatic detection of system prerequisites



Installation progress and status reporting

Permissions

Delegated App Permissions

MDM-ODA requires the following Microsoft Graph delegated permissions to function:

Permission	Purpose
`User.Read`	Sign-in and read current user profile (/me for PIM checks)
`User.Read.All`	Resolve UPN inputs and read user properties across all functions

`Group.Read.All`	Read group properties, list groups, read types and membership rules
`GroupMember.Read.All`	List group members and query member counts
`Directory.Read.All`	TransitiveMemberOf for PIM role detection and object membership
`Device.Read.All`	Resolve devices, read properties, query registered users
`DeviceManagementConfiguration.Read.All`	Read Intune config profiles and policies for assignment lookups
`DeviceManagementManagedDevices.Read.All`	Query managed devices by Azure AD device ID or serial number
`DeviceManagementRBAC.Read.All`	Read Intune RBAC settings (role assignments and role definitions)
`offline_access`	Maintain refresh token for persistent session

> **Key Caveat:** The documented least-privileged permissions for group write operations are `Group.ReadWrite.All` and `GroupMember.ReadWrite.All`. However, based on testing, group owners with scoped Intune RBAC roles can perform all write operations (create groups, add/remove members, set owners, rename, update dynamic rules) with only the read-only scopes above. This is undocumented behaviour — it could change if Microsoft tightens enforcement. If you want to guarantee write access regardless of ownership, add `Group.ReadWrite.All` and `GroupMember.ReadWrite.All`. If you prefer least-privilege and your users are always owners of the groups they manage, the read-only set above is sufficient today.

User Permissions

Entra built-in roles or custom RBAC roles determine which specific resources a user can access. The app permissions set the API surface ceiling, but Intune RBAC and group ownership scope the actual access. Exact role requirements vary by operation — **Group Owners** is sufficient for most group management operations. For comprehensive device and policy insights, users may benefit from **Intune Reader** or **Intune Administrator** roles depending on scope.

Web Application Redirect URI

For WAM (Web Account Manager) based authentication, configure the following redirect URI in your Entra app registration:

```
ms-appx-web://Microsoft.AAD.BrokerPlugin/{Client-ID}
```

Replace `{Client-ID}` with your actual Application (client) ID from Entra.

Safety, Validation & Auth Design

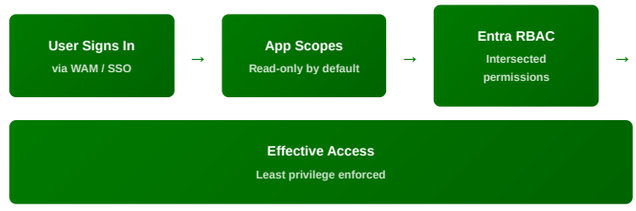
Preventing Accidental Actions

Every write operation in MDM-ODA is guarded by a multi-step validation pipeline. Before any change is committed to Entra or Intune, the tool enforces preview-before-write — users see exactly what will happen before it happens. Confirmation dialogs with explicit action summaries ensure that bulk operations like adding 50 devices to a group or setting owners on 20 groups cannot fire by a stray click. The Stop button is wired into every background runspace, allowing graceful cancellation mid-operation. Clear Inputs resets the entire page state without side effects. These aren't afterthoughts — they're core design decisions baked into every panel from the ground up.

Delegated Auth Flow — Least Privilege by Design

MDM-ODA uses the OAuth 2.0 delegated flow exclusively — the app never holds standalone permissions. Every API call executes in the context of the signed-in user, meaning the effective permission is always the intersection of what the app registration allows and what the user's Entra/Intune roles permit. This is a deliberate design choice that prevents privilege escalation: even if the app registration has broad scopes, a user without the right RBAC role cannot perform actions beyond their assignment.

The recommended configuration uses **read-only API scopes** for everyday operations — browsing groups, querying devices, viewing policies. Write permissions are only needed when the user actively performs create, update, or delete operations, and even then, group ownership often provides sufficient access without requiring write-level app permissions. This encourages organisations to start with the minimum surface area and only expand when a specific workflow demands it.



Validation Workflow for Write Actions

All write actions — group creation, member additions, owner assignments, dynamic query updates, renames, and removals — follow a strict validation-before-commit workflow. The tool validates input format, checks for duplicates, resolves object identities against Graph, and presents a structured preview of pending changes. Only after the user explicitly confirms does the operation execute. Failures during execution are caught per-item with detailed error reporting, so a single bad entry never derails an entire bulk operation.

> **Dynamic Query Safeguard:** Setting a dynamic membership query on an existing group is blocked if the group already has statically assigned members or if the group is already configured as Dynamic. This prevents accidental member loss from a query conversion and avoids conflicting membership rules — a guardrail that the Entra portal itself does not enforce as explicitly.

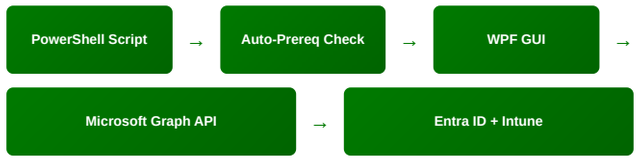
Getting Started

Quick Start

1. **Clone the repository:** `git clone https://github.com/satishsinghi-gh/mdm-oda.git`
2. **Configure credentials (optional):** Pre-populate your Tenant ID and Client ID in the script from your Entra app registration — or enter them manually at launch
3. **Launch the downloaded script:** No parameters, no admin rights needed — prerequisites are handled automatically
4. **Connect and go:** Authenticate with your Entra credentials and start using the tool

Architecture & Flow

Under the hood, MDM-ODA is a single self-contained PowerShell 7 script with an embedded WPF (XAML) interface. It uses background STA runspaces with ConcurrentQueues and a DispatcherTimer to keep the UI responsive during Graph API calls. Authentication leverages WAM (Web Account Manager) for seamless SSO with your Entra credentials. The Microsoft Graph PowerShell SDK handles all API interactions — from reading group memberships to creating resources — while the WPF DataGrid provides live, sortable, filterable table output with cell-level copy and Excel export. Prerequisite detection and installation (PowerShell 7, Graph modules) is fully automated on first run.



What's Included

- Fully functional PowerShell 7 script with embedded WPF UI
- Automatic prerequisite detection and installation
- Microsoft Graph SDK integration for reliable API calls
- Real-time verbose logging to local file system
- Validation workflows for write operations
- Export to Excel (XLSX) capability
- Complete source code and documentation

Roadmap

MDM-ODA is actively evolving. Here's what's planned for upcoming releases:

Input-Based Bulk Actions

Excluding destructive actions like Wipe/Delete — focused on safe, repeatable operations:

- **Sync** — Trigger device sync across bulk devices on-demand
- **Remediation** — Execute remediation scripts at scale with targeted input

Comprehensive Update Insights

Deep visibility into the Windows Update landscape across your fleet:

- **Quality Updates** — Patch compliance, pending installs, failure tracking
- **Feature Updates** — Rollout status, eligibility, readiness signals
- **Driver Updates** — Driver deployment state and version coverage

Application Landscape

End-to-end application lifecycle visibility and management:

- **Platforms** — Cross-platform app inventory (Windows, macOS, iOS, Android)
- **Assignments** — Assignment group mapping and coverage analysis
- **Deployment States** — Install success/failure rates and trend analysis
- **Filters** — Assignment filter integration for targeted deployments
- **App Creation/Modification Workflows** — Streamlined app packaging and configuration

Defender Integration

Bringing Microsoft Defender for Endpoint data into the same operational view:

- **Timeline Events** — Device activity timelines for incident investigation
- **Advanced Hunting** — KQL query integration for threat hunting
- **Vulnerability State** — CVE exposure and remediation tracking
- **Software Inventory** — Discovered software with risk scoring

Advanced Policy Management Actions

Extended policy operations beyond read-only insights — targeted modifications, cloning, and bulk assignment management.

Advanced Dynamic Group Query Builder

A visual query builder for constructing complex dynamic membership rules with syntax validation, preview, and testing before applying to groups.

Log Analytics Integration

Query extended Hardware Inventory and Audit data from Log Analytics that is not available natively through Microsoft Graph — bridging the gap between Intune's built-in reporting and the richer telemetry available in your Log Analytics workspace.

Intune | Entra ID | PowerShell | WPF | Microsoft Graph | Zero Trust | Group Management | Device Management | Policy Assignments | Open Source

⚠ **Disclaimer:** This tool is provided "as-is" without warranty of any kind, express or implied. The author assumes no liability for any damages arising from its use. Always validate operations in a non-production environment before deploying to production tenants.

Written by **Satish Singhi** — March 2026

MDM-ODA is an open-source tool built to empower IT professionals with granular control and insights into their Entra ID and Intune deployments. Built with attention to security, usability, and operational excellence.