



SDM Software Change Manager for Group Policy/Intune®

Version 1.5

Release Notes

Revisions:

Document Version:

1.1.....May 10, 2023

1.0.....May 5, 2023

Overview

The 1.5 release of Change Manager for Group Policy/Intune® introduces many improved features over 1.0, including added support for change control of Intune Configuration Profiles. In addition, issues that were encountered in 1.0 and resolved in this release are listed below.

What's New/Improved

- Change control of Microsoft Intune Configuration Profiles are supported, including the following types:
 - Administrative templates
 - Settings Catalogs
 - Shell scripts
 - Custom attributes
 - PowerShell scripts

In addition, the following template types are supported:

- Android device administrator
 - Device restrictions
 - Trusted certificate
 - Wi-Fi
- Android (AOSP)
 - Device restrictions
 - Trusted certificate
 - Android Enterprise
 - Device restrictions
 - Trusted certificate
- iOS/iPadOS
 - Custom
 - Device restrictions
 - Edition upgrade and mode switch
 - PKCS certificate
 - Secure assessment (Education)
 - Trusted certificate
- macOS
 - Device features
 - Device restrictions
 - Endpoint protection
 - Extensions
 - PKCS certificate
 - Preference file
 - Trusted certificate
- Windows 10 and later
 - Administrative templates

- Delivery optimization
 - Device firmware configuration interface
 - Device restrictions
 - Device restrictions (Windows 10 Team)
 - Domain join
 - Email
 - Endpoint protection
 - Identity protection
 - Imported Administrative templates
 - Kiosk
 - Network boundary
 - Secure assessment
 - Shared multi-user device
 - Trusted certificate
 - Windows health monitoring
- Added support for Integrated Windows Authentication (IWA) at logon
 - Product Administrators can require editor's comment on check-in
 - The UI allows setting DC affinity per domain
 - Removed requirement for port 8000 access to CMGP server from client (all traffic now goes over 443)
 - The Details pane automatically expands when a managed object is selected
 - A user in the Break Glass role can cancel a check-out that was started by another user
 - A user in the Approver role can cancel an approval or cancel a scheduled deployment
 - WMI filters can be set on a GPO within the change control process
 - Block inheritance can be set on Containers within the change control process
 - An email will notify an object's Editor if the object stays in the checked out state for more than x days
 - An email will notify an object's Approver if an approval is pending for more than x days
 - An email will notify an object's Editor when a scheduled deployment succeeds
 - An Object History View shows a history of all operations that have been performed on an object
 - Audit log events can be sent to a custom Windows event log
 - GPOs under control have a Settings report that displays its current settings

Resolved Issues

- Containers that were previously taken control of in CMGP, and then subsequently deleted from AD, could not be removed from the application
- Setcmgpermissions.exe didn't properly recurse containers when the -recurse option was used
- The version difference report wasn't reflecting GPO link order or status changes
- Delay in seeing action menu items after navigating to or checking out an object, especially in environments with many OUs

- GPOs with folder redirection policy would fail on take control
- Selecting an action twice (e.g. Check out or Check in) would result in unexpected behavior