



# **SDM Software Change Manager for Group Policy/Intune®**

Version 1.9

## **Release Notes**

Revisions:

Document Version:

1.0.....March 1, 2025

## Overview

The 1.9 release of Change Manager for Group Policy/Intune® introduces many new features over 1.8, in addition to issues that were encountered in 1.8 and resolved in this release. These are listed below.

## What's New/Improved in 1.9

- New Restricted Settings feature allows you to control which policy areas within a GPO can be edited by a GPO editor. This allows you to prevent, for example, an editor from modifying security settings on a GPO that otherwise would contain those settings, while still allowing the editor to create other settings within other policy areas.
- Ability to look up users and groups within AD or Entra ID when assigning delegation. The product will not give hints when you are typing in users or groups, based on what is found within the connected identity systems (e.g. AD or Entra ID).
- The product will now support Intune Configuration profiles that contain secret fields (e.g. passwords). You will be prompted when checking out such a profile to provide the password, and again when the profile is checked in—allowing you to edit profiles that contain such policy types.
- Added the option to automatically send CMGPI support logs to an internal SMB network share, rather than just locally or to Azure Blob Storage.
- Added a new optional level of approval, separate the approver and deployer roles to provide 3 levels of approval for any object that is subject to change control. This option can be enabled after installation.
- Added support for export of GPOs that are in a checked-out state. This allows a user who is editing a GPO to export the current checked out GPO to a GPMC backup, which can then be imported into a test environment for further testing of the change impact.
- Support for Microsoft Teams alerting added. You can now send specific notifications from the product to a MS Teams channel.
- Added GPO naming standards enforcement—the ability to enforce naming of GPOs on new GPO creation or renaming of existing GPOs using a regex expression.
- Added support for installation on Windows Server 2025.
- Added support for silent installation of the CMGPI server.

## Resolved Issues

- Resolved an issue where OUs with '/' characters in their name or other Unicode characters prevented the product from taking control of those objects.
- Resolved an issue where configured WMI filters were not displaying in Details pane of a GPO.
- Resolved an issue that allow duplicate DNs to be stored for container objects

In addition, the following list shows what was introduced in version 1.8 of the product:

## What's New/Improved in 1.8

- Added support for Entra ID Single Sign-On (SSO) and ability to delegate roles within the product to Entra users and groups
- Added new “Administrative Containers” feature that allows an administrator to organize GPOs, Containers and Intune Profiles into logical groupings for the purposes of delegation
- Added a new global settings search feature that allows a user to search for a particular Group Policy or Intune setting across all controlled GPOs and Intune Configuration Profiles
- Added support for Azure SQL as an alternative database to SQL Server
- Added ability to recover deleted GPOs and their links
- Added severity and change ticket number fields to check-in dialog
- All connection strings encrypted using DPAPI
- Added support to modify permissions on individual GPOs using SetCMGPPermissions utility
- Added support for recursive selection of containers during Take Control
- Newly added GPO links are now enabled by default
- Maintenancetool utility now lets you retrieve current database connection string
- Improved modification of certificates using AddressHostname script
- When hovering over a container name, you get the full DN of the container
- Externalized Azure URIs to allow support for other Azure clouds (e.g. GovCloud) in Intune and SSO support
- User now can create “support bundle” from CMGPI UI to download logs for troubleshooting
- Optional ability to continuously upload CMGPI logs to Azure blob storage for troubleshooting
- Email alerts will be sent when Azure and Intune related secrets are close to expiration
- Provide support for High Availability (HA) deployment of CMGPI server

## Known Issues

- If an Entra ID security group is assigned as an approver, they won't receive an email notification that an object is due for approval. Entra ID security groups do not support email enablement