



SDM Software Change Manager for Group Policy/Intune®

Version 1.9

User Guide

Revisions:

Document Version 1.2....March 18, 2025

Document Version 1.1....March 6, 2025

Document Version 1.0.....Feb 25,2025

Contents

Overview	4
Using the Product	4
Global Product Roles.....	4
Product Administrator	4
GPO Creator	4
Break Glass.....	5
Auditor	5
Object-Specific Roles.....	5
Editor.....	5
Approver	5
Deployer.....	5
CMGPI Dashboard.....	6
CMGPI Navigation.....	6
Restricted GPO Policies.....	9
Naming Rules for GPOs.....	10
System and CMGPI Notifications	12
Setting Up Alerts	12
Settings Search.....	13
Intune Search	15
Using Administrative Containers	16
The Change Control Process	20
Understanding AD vs. Entra ID Editors & Approvers	20
Editing GPOs.....	22
Handling Out-of-Band Changes.....	23
Creating a new GPO	26
Deleting a GPO	27
Restoring a Deleted GPO	27
Renaming a GPO	28
Changing WMI filters	28

Changing GPO Delegation	29
Check in a GPO	30
Approving and Deploying GPO Changes	31
Editing AD Containers	33
Approving and Deploying Container Changes	34
Preparing to edit Intune Profiles.....	35
Editing Intune Profiles.....	36
Rename an Intune Profile	39
Editing Intune Scope Tags	39
Editing Intune Assignments	40
Approving and Deploying Intune Profiles	41
Audit Log	42
Licensing.....	43
Appendix A: Using the SetCMGPPermissions.exe to grant initial permissions required by CMGPI	44
Appendix B: Customizable User Settings within CMGPI	46
Appendix C: Modifying CMGPI Application Configuration	48
Appendix D: The CMGPI PowerShell Module	49
Appendix E: Customizing SSL Certificates and Using Host Aliases.....	53
Appendix F: Configuring Intune connectivity from Script.....	56
Intune Configuration from Script.....	56
Appendix G: Configuring Entra ID SSO from Script	58
SSO Configuration from Script	58
Appendix H: Configuring Entra ID SSO Manually	60
Appendix I: Supported types of Intune Configuration Profiles.....	64
Appendix J: Troubleshooting and Logging	66
Appendix K: Configuring Connectivity to Other Azure Clouds.....	68

Overview

SDM Software's Change Manager for Group Policy/Intune® (CMGPI) brings modern Group Policy and Intune® change management processes to organizations that leverage GP or Intune to configure and secure their Windows systems. Change Manager for GP/Intune provides web-based workflow to allow you to delegate control of GPO editing and GPO linking and Intune profile editing and assignment, to appropriate personnel to ensure the security and integrity of your Group Policy or Intune environments. In this document, we'll describe the requirements to install, configure and use the CMGPI product, as well as some best practices for doing so.

To see what's new in this version of CMGPI, refer to the Release Notes document for this release.

Using the Product

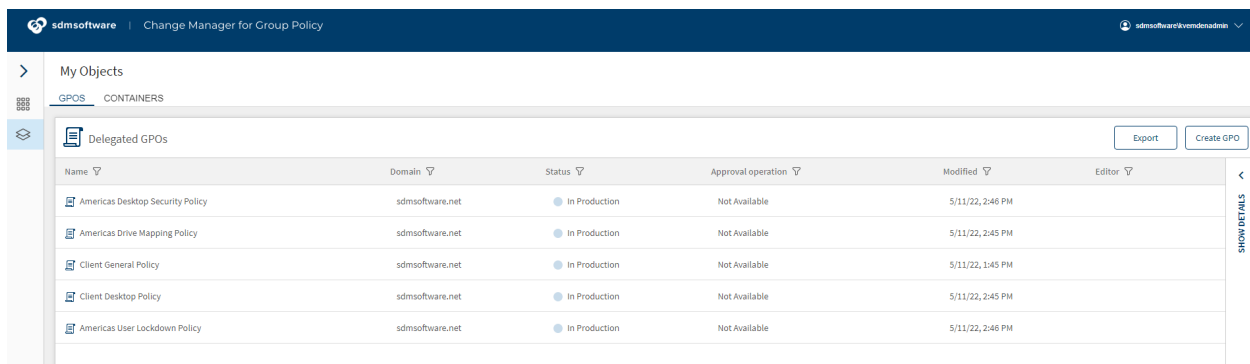
Once the product is installed and configured (see the CMGPI Installation Guide for a detailed walkthrough of the installation process), you can begin using it to manage change within your Group Policy and Intune environments. Logging into the product is as simple as providing an AD username and password in the form of <domain\username>. If you have enabled Entra ID SSO in the product, you can also log in using those credentials, assuming your Entra ID has been granted the appropriate roles. The ability to log in to CMGPI is governed by the roles that the product supports -- Editor, Approver, and Deployer -- but the product also contains several global (product-wide) roles, defined below.

Global Product Roles

The **Product Administrator** role is the only role that can delegate product roles. Role delegation is accessible from the CMGPI menu under **Delegation, Product Roles**.

Product Administrator: Anyone with this role can control all aspects of CMGPI configuration, including logging in to the console, taking control of objects (GPOs, containers and Intune profiles), setting delegation on objects, configuring application settings, managing licensing and viewing statistics and audit events across all managed objects. The user who installs CMGPI has the Product Administrators role by default, but the role can be delegated to other users, too. The one limitation Product Administrators have is that they are prevented from making themselves approvers or deployers for any GPO or container.

GPO Creator: While users who are in the Editors role can perform most tasks related to GPO management, they cannot create new GPOs. That job is reserved for members of the GPO Creator role. Members of this role will have a "Create GPO" button on the upper right of their My Objects screen that will allow for GPO creation, as shown below. Once created, those GPOs are subject to approval and deployment.



The screenshot shows the 'My Objects' section of the 'Change Manager for Group Policy' application. It displays a table of 'Delegated GPOs' with columns for Name, Domain, Status, Approval operation, Modified, and Editor. The table lists five GPOs, all with a status of 'In Production' and 'Not Available' for approval operations. The interface includes navigation tabs for 'GPOS' and 'CONTAINERS', and buttons for 'Export' and 'Create GPO'.

Name	Domain	Status	Approval operation	Modified	Editor
Americas Desktop Security Policy	sdmsoftware.net	In Production	Not Available	5/11/22, 2:46 PM	
Americas Drive Mapping Policy	sdmsoftware.net	In Production	Not Available	5/11/22, 2:45 PM	
Client General Policy	sdmsoftware.net	In Production	Not Available	5/11/22, 1:45 PM	
Client Desktop Policy	sdmsoftware.net	In Production	Not Available	5/11/22, 2:45 PM	
Americas User Lockdown Policy	sdmsoftware.net	In Production	Not Available	5/11/22, 2:46 PM	

A user with GPO Creator Role

Break Glass: The Break Glass role is a special role within CMGPI. It should be granted to users only under emergency situations. It allows a user to temporarily bypass approval-based workflows when needing to make urgent changes to objects. A user in this role does not need to explicitly be made an editor, approver, or deployer of an object. They can check out and edit any object under control by CMGPI and approve and deploy those changes themselves. This removes any oversight from the object change control process. The main purpose of this role is to allow temporary, urgent changes to occur without the overhead of an approval process. An additional permission of the Break Glass user is that they can undo an existing checkout that was performed by another user. The editor of any given object has the ability to undo their own checked-out objects, but it can be granted to a Break Glass user to provide a way to cancel a checked out object in the event that the editor who checked out that object is unavailable. In all other aspects of the change control process, a Break Glass user cannot take over an ongoing change control process.

Auditor: The Auditor role allows read-only access to certain aspects of CMGPI. Auditors can see all objects that have been delegated in CMGPI, and what their current state is, as well as differences in previous versions of the object. And they can view the [CMGPI Audit Log](#), which displays what activities have occurred by all users of the product.

Object-Specific Roles

Editor: Users with the Editor role are responsible for modifying GPOs, container links, and Intune profiles controlled by CMGPI. Editors can perform most tasks related to GPOs, except for the creation of new GPOs, unless they are assigned the GPO Creator role by a product administrator.

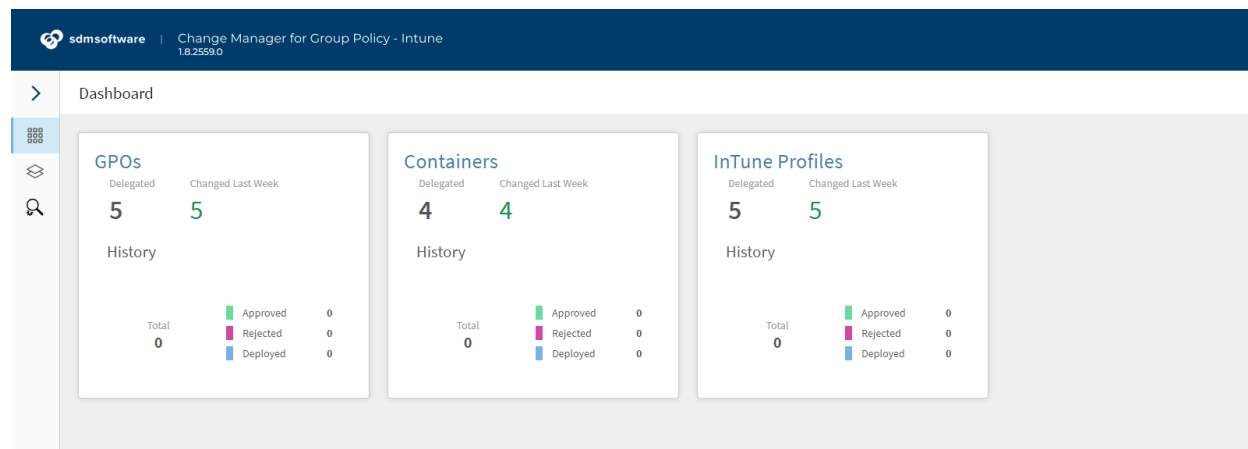
Approver: The Approver role is responsible for reviewing and approving changes made to objects before they are deployed. In environments where separate deployer roles are not enabled, approvers are also responsible for deploying the approved changes, completing the full change management cycle.

Deployer: The Deployer role allows an administrator to separate approval and deployment responsibilities. This enhances flexibility, enabling one user to approve a change while a different user, such as a dedicated deployment specialist, deploys the change. Users with the Deployer role receive automated email notifications for approved objects, including deployment options, failure alerts, and overdue deployment reminders.

By default, the Deployer and Approver roles are combined in the product. To separate the roles, you need to enable the Deployer role in the product configuration. For more details on customizing user settings within CMGPI, see [Appendix B](#).

CMGPI Dashboard

When a user who is delegated as an approver, editor, or deployer to an object logs into the CMGPI web application, they see a Dashboard of high-level statistics for their role, as shown below:




The CMGPI Dashboard

The dashboard has three sections that display statistics about objects under control by the product—the left-hand is for GPOs, the middle box for Active Directory containers, and the right-hand box for Intune Profiles. When an approver, editor, or deployer logs in, they see statistics that are relevant to them. For example, the “GPOs Delegated” statistic shows how many GPOs are currently delegated to just them. The “Changed Last Week” number shows the number of objects that have been newly delegated to them in the last week.

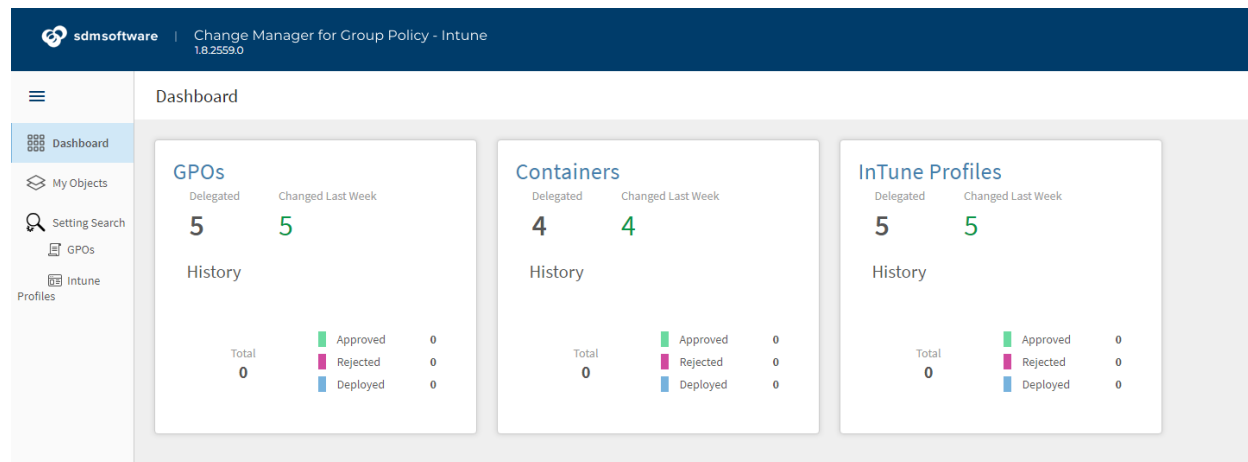
The History section shows the status of any objects that the user is either the approver, editor, or deployer for. So, if you, as an editor of GPOs, log into CMGPI, you will see the number of any GPOs (or containers or Intune profiles) that were approved, rejected or deployed, that you were the editor for, even though you were not the one that did the approving, rejecting or deploying. The history data shows activity for the last 60 days.

The behavior of the Dashboard is slightly different if the user is a member of the Product Administrator role. In that case, the Product Administrator sees data for all objects delegated to all users.

CMGPI Navigation

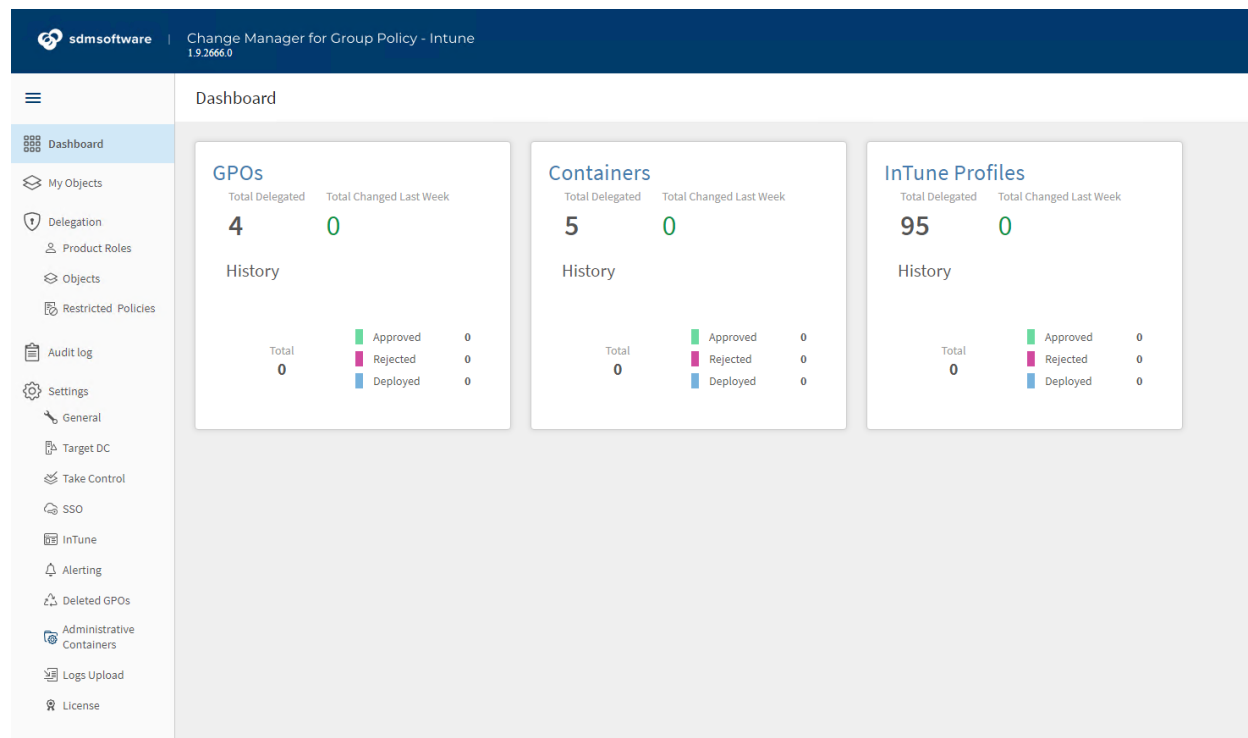
Navigating around CMGPI is done by using the menu bar on the left-hand side of the product, which can be expanded and contracted using the  widget in the upper left of the menu pane. The menu bar

options change depending on what role the logged in user has. For example, an editor, approver, or deployer will see three options on the left, as shown here:



Viewing the CMGPI menu

A product administrator will see more options:



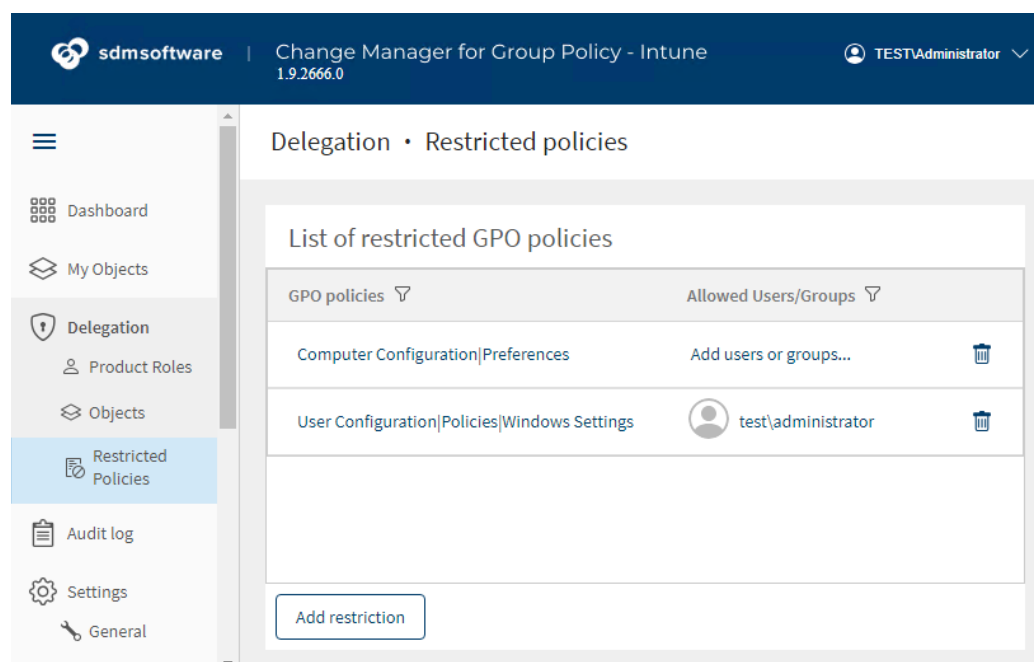
The full set of CMGPI menu options

Each menu option is described here:

- **Dashboard:** Displays the CMGPI dashboard page.
- **My Objects:** Shows the list of GPOs, containers and Intune Profiles that the user is either an editor, approver, or deployer for, separated into three tabs. In the case of product administrator, break glass or auditor roles, all objects under control are shown.
- **Delegation, Product Roles:** Allows the product administrator to delegate users to CMGPI [product roles](#).
- **Delegation, Objects:** Allows a product administrator to manage the delegation of GPOs, containers and Intune Profiles that have been taken control of. This is where a product administrator can change which users and groups are editors, approvers, or deployers of a GPO, AD container, Intune Profile or Administrative Container.
- **Delegation, Restricted Policies:** Allows a product administrator to control access to GPO policy areas for individual users and groups.
- **Audit Log:** Provides the product administrator or auditor with access to the audit log, which is a record of all activities performed within CMGPI.
- **Settings, General:** Allows the product administrator to configure default approvers and/or deployers, require comments on check-in, enforce naming conventions for GPOs, change the audit events lifetime, and configure SMTP settings.
- **Settings, Target DC:** This section allows the product administrator to control which Active Directory Domain Controllers are used to initiate changes to GPOs and containers per domain. The default target DC will be the PDC emulator in each managed domain, but you can select other DCs from the list for each domain under management from this dialog.
- **Settings, Take Control:** Allows the product administrator to take control of GPOs, containers, or Intune Profiles that were not taken control of during the Welcome Wizard, or to remove control.
- **Settings, SSO:** Allows a product administrator to define the configuration for integrating CMGPI into Entra ID Single Sign-on (SSO).
- **Settings, InTune:** Allows a product administrator to define the configuration for integrating CMGPI into Intune Profiles for the purposes of Intune change control.
- **Settings, Alerting:** Allows a product administrator to configure system alerts to be sent to a designated email address or to set up Microsoft Teams notifications for specific users or groups, providing immediate notification about actions performed within CMGPI.
- **Settings, Deleted GPOs:** Allows a product administrator to view and restore deleted GPOs.
- **Settings, Administrative Containers:** Allows a product administrator to create, edit and delete administrative containers and their member objects.
- **Settings, Logs Upload:** Allows a product administrator to optionally configure continuous CMGPI support log upload to an Azure blob storage account.
- **Settings, License:** Allows the product administrator to view and update the license that is in use by CMGPI.

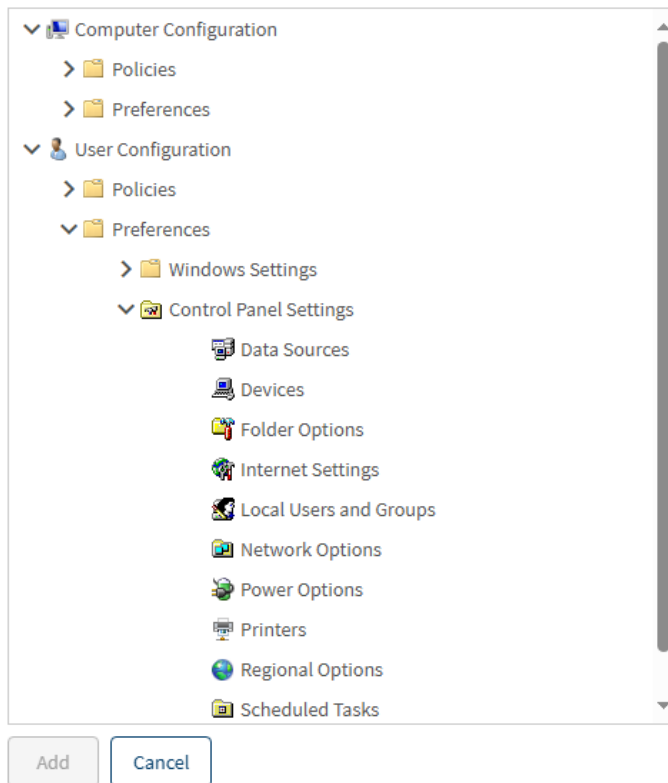
Restricted GPO Policies

CMGPI 1.9 introduces granular access control for GPO policy areas, allowing administrators to define which users or groups can access specific policy areas within GPOs. For example, a product administrator can grant full access to "Computer Configuration\Windows Settings" while restricting access to "User Configuration\Windows Settings" or even individual policy areas within those sections. It's important to note that restricted policies operate at the policy area level—not at the individual setting level. A product administrator can configure these restrictions under **Delegation, Restricted Policies** in the CMGPI menu as shown below:



To add a restriction, click the “Add restriction” button at the bottom of the screen. You’ll be presented with a tree view of the GPO settings namespace, as shown here:

Add restricted GPO policy



Drill down into the policy area you wish to restrict, select that node in the tree and press the “Add” button to add it to the restriction list. Note that you can only select one policy area node at a time. Once you’ve added the policy area to the list, the restriction will not be effective until you choose at least one Allowed user or group. Press the “Add users or groups...” link on the setting you just added and add the Active Directory (or Entra ID if SSO is enabled) user or group you wish to allow access to this policy area.

When you add a policy area and select allowed users or groups, that means that all other users and groups who are editors of GPOs have an implicit deny over that policy area. This means that when they check out a GPO with such a restriction, they will receive a warning that it contains restricted policies. If they try and change, add or delete any policy settings under a restricted area, they will be blocked from checking that GPO back in for approval, until they remove the restricted settings change they made.

Naming Rules for GPOs

Starting with CMGPI version 1.9, the product supports naming rules for GPOs. Administrators can define a specific naming rule using regular expressions, ensuring all new and renamed GPOs adhere to the rule. The product verifies the entered name against the rule in real-time, providing immediate feedback if it doesn't conform to the defined pattern. This feature ensures consistent naming conventions across your

GPO environment, promoting better organization and management. This option is available under **Settings, General** in the CMGPI menu.

Edit GPO naming standard

Enter rule:

Enter test name:

the rule and test name are correct

Enter the naming rule, enter a sample name and press verify to see if your name passes the standard.

show more ▾

To illustrate how regular expressions work, here are a few examples:

Policy_\\w*-\\w*-\\d*

This regular expression enforces a naming convention that starts with "Policy_" followed by two text strings separated by hyphens (-) and ending with digits, as in: *Policy_Marketing-Desktop-15*

Users_\\w*\\d*_\\w*

This regular expression enforces a naming convention that starts with "Users_" followed by a platform name, then an underscore, and ending with a text string, as in: *Users_Win10_DriveMappings*

You can use any online regex expression tester to check your expressions, for example, <https://regex101.com/>.

For more details on using regular expressions, refer to <https://learn.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference>.

System and CMGPI Notifications

CMGPI's enhanced notification system provides administrators with two communication channels:

- An administrator can configure a dedicated email address to receive system alerts about significant events, such as configuration changes, user activities, or system errors.
- CMGPI 1.9 supports integration with Microsoft Teams, allowing administrators to receive notifications about CMGPI actions directly within their Teams workspace. This eliminates the need to switch between applications and ensures you stay informed about important events.

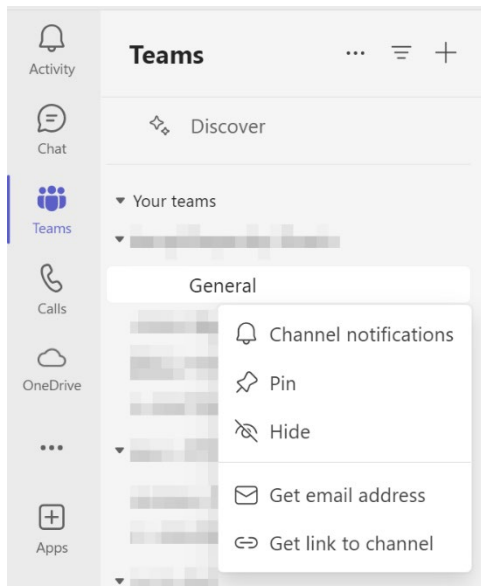
The screenshot shows the 'Settings - Alerting settings' page in the SDM Software Change Manager for Group Policy - Intune interface. The left sidebar contains a navigation menu with options: Dashboard, My Objects, Delegation, Product Roles, Objects, Restricted Policies, Audit log, Settings (selected), General, Target DC, Take Control, SSO, InTune, Alerting (highlighted), Deleted GPOs, Administrative Containers, Logs Upload, and License. The main content area is titled 'Settings - Alerting settings' and contains two sections: 'Enter email for system alerts' with an 'Email:' input field, and 'Enter Teams connection settings and actions to alert' with an 'Email:' input field and a list of actions with checkboxes. The actions listed are: Approve, Cancel Deployment, Check-in, Check-out, Create GPO, Delete, Deploy, Edit, Grant role, Reject, Remove control, Restore deleted object, Revoke role, Rollback, Schedule Deployment, Stop Editing, Take control, and Undo Check-out. A 'Save' button is located at the bottom of the actions list.

Setting Up Alerts

A product administrator can configure these settings under **Settings, Alerting** in the CMGPI menu.

- **Email for system alerts:** Specify an email for system alerts under **Enter email for system alerts**.
- **Microsoft Teams integration:** To set up integration with Microsoft Teams, enter the email address of the user or Teams channel under **Enter Teams connection settings and actions to alert** and select the actions for which you'd like to receive notifications.

To find the email address associated with a Teams channel, select the channel in Microsoft Teams, click the three dots next to its name, and then click **Get email address**.



To send to multiple channels, you can add multiple email addresses by separating them with commas.

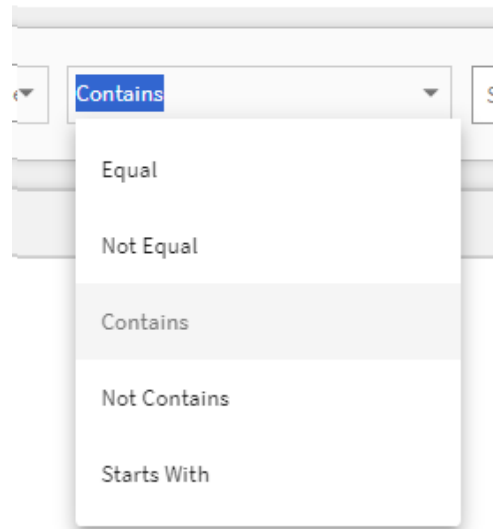
Settings Search

Settings search allows CMGPI users to search for a full or partial path of a setting in either all GPOs or all Intune profiles under control within the product. With this powerful feature, you can use Settings Search to determine a particular setting has already been implemented within a given GPO.

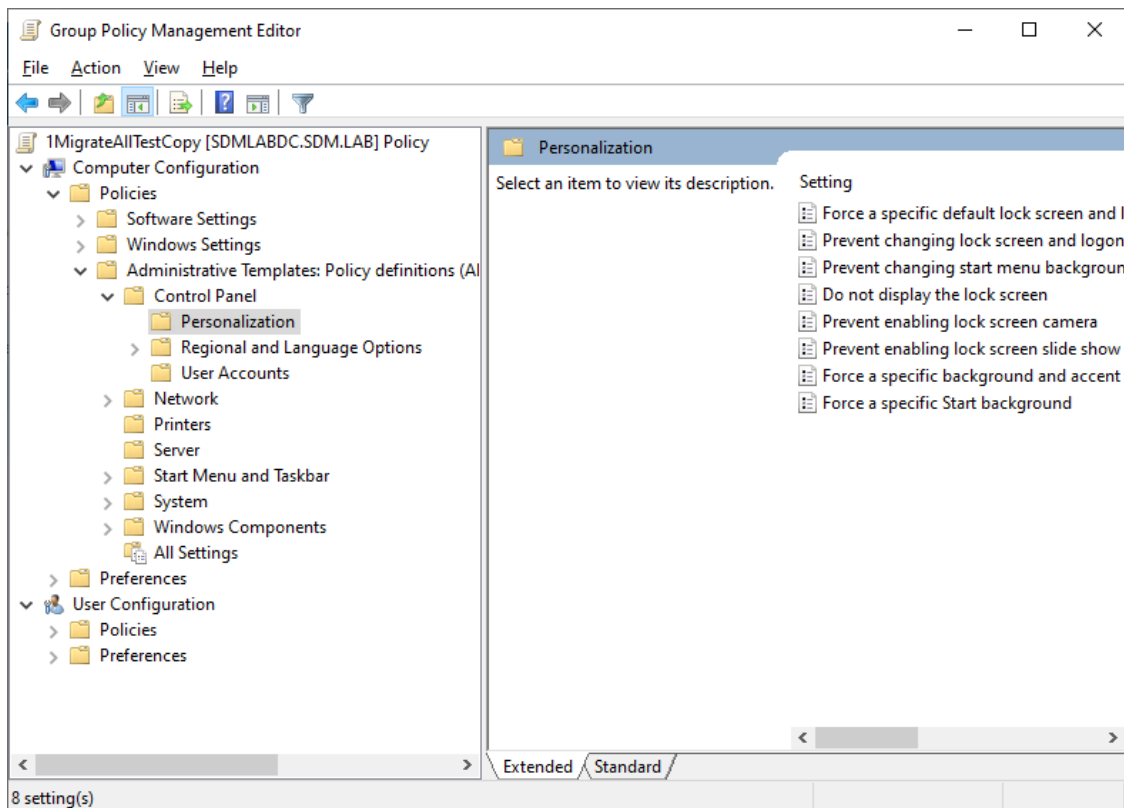
Settings Search is accessible from the navigation menu for any user who is an Editor, Approver, Deployer or a member of the Break Glass role. as shown below:



Select to search for GPO or Intune profile settings within a Setting Path or a Setting Value, or both. You can also choose the operator to use in your search:



Then enter the search text you want to look for. Settings paths should be delimited using a pipe (|) symbol. For example, let's say you want to look for a GPO setting within the following path (Personalization):



You would enter a Path search that Contains “Control Panel\Personalization” as shown here:

The screenshot shows the 'Settings Search' interface for GPOs. The search criteria are set to 'Path' and 'Contains' with the value 'Control Panel\Personalization'. The results table lists 18 settings, all of which contain the specified path. The settings are organized by Name, Domain, Setting Path, and Setting Value.

Name	Domain	Setting Path	Setting Value
1MigrateAllTest	sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific default lock screen and logon image\Path to lock screen image\Value
1MigrateAllTest	sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific default lock screen and logon image\State
1MigrateAllTest	sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific default lock screen and logon image\Turn off fun facts, tips, tricks, and more on lock screen\State
1MigrateAllTestCopy	sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific default lock screen and logon image\Path to lock screen image\Value
1MigrateAllTestCopy	sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific default lock screen and logon image\State
1MigrateAllTestCopy	sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific default lock screen and logon image\Turn off fun facts, tips, tricks, and more on lock screen\State
1newFri	child.sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific default lock screen and logon image\Path to lock screen image\Value
1newFri	child.sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific default lock screen and logon image\State
1newFri	child.sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific default lock screen and logon image\Turn off fun facts, tips, tricks, and more on lock screen\State
1NewMonDisabled	sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific background and accent color\State
1NewMonDisabled	sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Prevent changing lock screen and logon image\State
1NewMonDisabled	sdm.lab	User Configuration\Policies\Administrative Templates\Control Panel\Personalization	Prevent changing desktop background\State
1NewMonEnabled	sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific background and accent color\Accent color\Value
1NewMonEnabled	sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific background and accent color\Start background color\Value
1NewMonEnabled	sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Force a specific background and accent color\State
1NewMonEnabled	sdm.lab	Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization	Prevent changing lock screen and logon image\State

And the search returns a highlighted list of every GPO setting that contains this path. If you click on a setting path, the Details pane will expand to show more information about the setting. You'll also see a “More Details” link in the Details pane, as shown below:

The screenshot shows the 'Settings Search' interface with the 'More Details' pane expanded for the GPO '1MigrateAllTestCopy'. The details pane displays information such as Type, Created, WMI Filter, Approver, Current Approver, DN, Version, Checked out by, Display Date, Comment, Editor comment, and Linked to. A red box highlights the 'More Details' link in the bottom right corner of the details pane.

Select More Details, and CMGPI takes you to the My Objects page and highlights the selected GPO, assuming your user account has editor privileges over it. If not, the My Objects page will simply show the GPOs that you have control over.

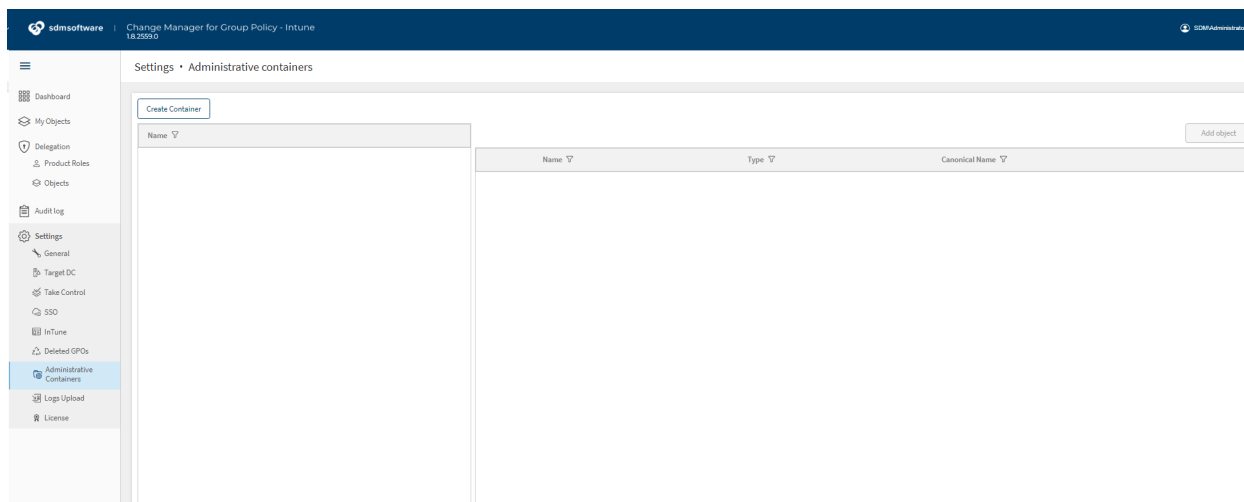
Intune Search

Intune Profile settings search works similar to GPO search. Since there are many types of settings within Intune, the setting path will vary by type, but you can continue to use the | symbol to delimit paths within Intune, or just use the setting name as it appears in the Intune portal.

Using Administrative Containers

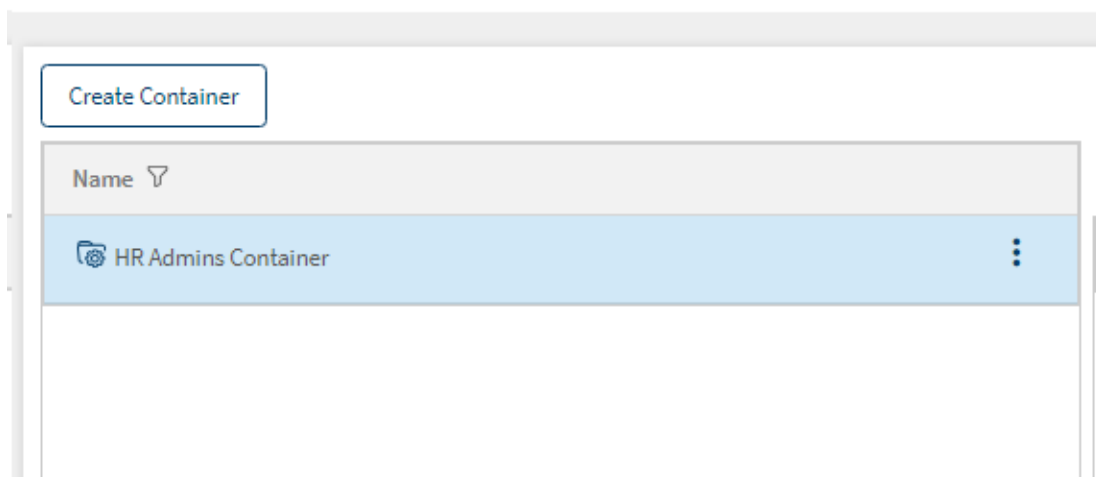
Think of Administrative Containers (ACs) as a “virtual OU” for the purposes of delegating roles. You can use ACs to group GPOs, AD containers and Intune Profiles that are related. For example, you might have a set of OUs and the GPOs linked to them that are managed by one team. Instead of having to delegate access to each object for that team, you can simply create an AC that contains all the relevant OUs and GPOs and delegate editor, approver, and deployer access to it. Any objects that live within the AC automatically inherit the AC’s editors, approvers, and deployers.

To create and manage ACs, you need to be a member of the Global Product Administrator role. ACs are managed from the menu under Settings, as shown here:




The first step is to create a Container by clicking the Create Container button. Once the AC is created, you can either edit its name or description or delete it, by pressing the 3 dots shown to the right of the AC name:

Settings • Administrative containers



Once named and created, to add objects to it, click the Add Object button on the right-hand side of the screen, while the AC is selected. The Add Object dialog will display a list of all objects currently under control within CMGPI, any of which can be added to the container as shown here:

Add Object

<input type="checkbox"/>	Name ▾	Type ▾ ↑	Canonical Name ▾
<input type="checkbox"/>	sdm	Domain	sdm.lab/
<input type="checkbox"/>	child	Domain	child.sdm.lab/
<input type="checkbox"/>	DenyTest1	GPO	sdm.lab/System/Policies/{AEB60C20-7249-44ED-9E54-028E594B8585}
<input type="checkbox"/>	 1NewMonEnabled	GPO	sdm.lab/System/Policies/{AF7409AE-84FB-451C-A586-3EF7AA84A78F}
<input type="checkbox"/>	MultiLinkDelete	GPO	sdm.lab/System/Policies/{39ef35ac-b3e0-40b5-bc0e-a2c323c9c73f}
<input type="checkbox"/>	Test GPO 2 has some settings	GPO	sdm.lab/System/Policies/{f05468e8-3565-46ea-8eeb-f4d09337119f}
<input type="checkbox"/>	Blank GPO	GPO	child.sdm.lab/System/Policies/{fa84be01-2a51-4b9c-be4d-a7b6c171fc0c}
<input type="checkbox"/>	5newFri	GPO	child.sdm.lab/System/Policies/{53799586-6A68-4BC1-838E-21A00CE364E2}
<input type="checkbox"/>	1MigrateAllTest	GPO	sdm.lab/System/Policies/{B0AB62FD-EB22-4BFF-83B3-977BB3DF100D}
<input type="checkbox"/>	1NewMonDisabled	GPO	sdm.lab/System/Policies/{8DA31A0F-8BD2-4A51-A872-1EF3369A8BB3}
<input checked="" type="checkbox"/>	1MigratorMasterNonAdmin	GPO	sdm.lab/System/Policies/{FB8B4CFB-C6DB-4EFB-8196-4241A0425107}
<input type="checkbox"/>	Copy of Test GPO	GPO	sdm.lab/System/Policies/{608F2AA7-DE04-4810-924B-247FFC82D36C}
<input checked="" type="checkbox"/>	Enforce Local Admin and UNC hardening	GPO	sdm.lab/System/Policies/{D8572F9D-9062-434C-889F-DC516B470F0C}
<input type="checkbox"/>	TakeControlTest	GPO	sdm.lab/System/Policies/{416A9759-5A1C-47E6-8E17-BD0EAD344114}
<input type="checkbox"/>	1newFri	GPO	child.sdm.lab/System/Policies/{2180CF28-4D10-42F2-8449-ED8A48F1D2D7}
<input type="checkbox"/>	DeleteTest	GPO	sdm.lab/System/Policies/{f7af2143-41ea-4f9e-b5ca-97bdfa5dfb91}
<input type="checkbox"/>	2FriNewHasSettings	GPO	sdm.lab/System/Policies/{f3727629-c21d-4175-bbbd-1b2321083e65}



Some objects in the list may be grayed out. This indicates that the object is currently in the middle of a change control process (e.g. checked-out or waiting for deployment) and cannot be added to the AC. Likewise, you cannot remove objects from an AC if they are in the middle of change control.

Once you've selected the objects you want in your AC, click OK. Some of the objects you've included in your AC might already contain delegations for editor, approver, and deployer roles, so you'll see this warning:



Some objects in this administrative container already have an editor or approver delegation, which will be ignored.

List of conflicting objects

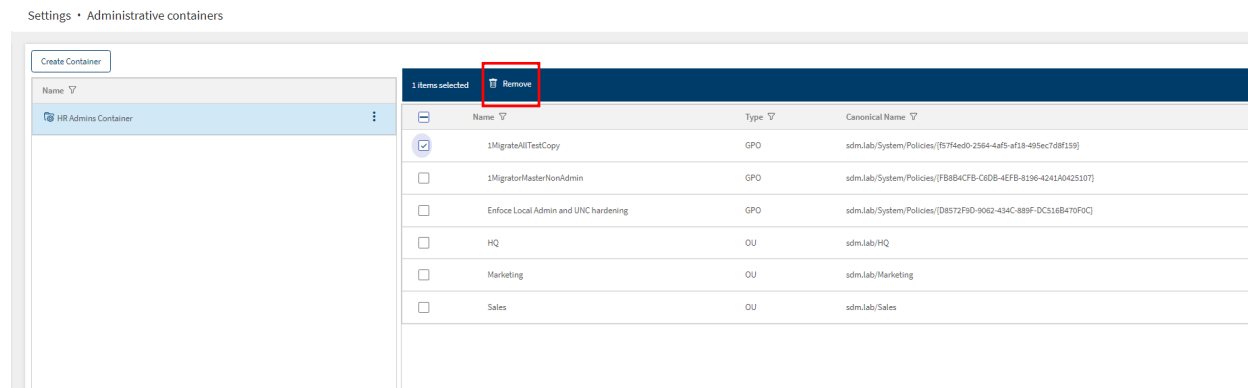
Name ▼	Ignore ▼
 Marketing	SDM\mbaker;SDM\jkelly
 Sales	SDM\mbaker;SDM\jkelly

Ok

Cancel

This indicates that any previously defined CMGPI delegations on these objects will be overridden by those that you specify on the AC itself. An object that is part of an AC does not also have its own separate delegation—it can only have one set of editor, approver or deployer that is controlled by the AC.


Once objects are added to the AC, you can remove one or more of them by selecting the object(s) and clicking Remove above the list:



As a Product Administrator, grant editor, approver, and deployer access to ACs the same way you would individual objects such as GPOs, AD Containers and Intune Profiles, from the **Delegation, Objects** menu. After creating an AC, it appears in the list of objects under control, as shown here:

List of Objects:

<input type="checkbox"/>	Name ▾	Type ▾	Canonical Name ▾	Approver(s) ▾	Editor(s) ▾
<input type="checkbox"/>	Test Android Profile	Intune Profile	Android device administrator/Template/Test Android Profile	Add approver ...	Add editor ...
<input type="checkbox"/>	1NewMonDisabled	GPO	sdm.lab/System/Policies/{8DA31A0F-8BD2-4A51-A872-1EF3369A8B83}	Add approver ...	Add editor ...
<input type="checkbox"/>	Copy of Test GPO	GPO	sdm.lab/System/Policies/{008F2AA7-DE04-4819-924B-247FFC82D36C}	Add approver ...	Add editor ...
<input type="checkbox"/>	TakeControlTest	GPO	sdm.lab/System/Policies/{416A9759-5A3C-47E6-8E17-BD0EAD344114}	Add approver ...	Add editor ...
<input type="checkbox"/>	Users	OU	sdm.lab/Marketing/Users	Add approver ...	Add editor ...
<input type="checkbox"/>	BaselineX	Intune Profile	Windows 10 and later/Administrative Templates/BaselineX	Add approver ...	Add editor ...
<input type="checkbox"/>	1testFri	GPO	child.adm.lab/System/Policies/{2180CF28-4D10-42F2-8449-ED8A48F1D2D7}	Add approver ...	Add editor ...
<input type="checkbox"/>	DeleteTest	GPO	sdm.lab/System/Policies/{7A72143-41ea-4f9e-b5ca-97bdf45dfb91}	Add approver ...	Add editor ...
<input type="checkbox"/>	2FullEventLogSettings	GPO	sdm.lab/System/Policies/{D727629-c21d-4175-bbbd-1b2321083e65}	Add approver ...	Add editor ...
<input type="checkbox"/>	Engineering	OU	sdm.lab/Engineering	Add approver ...	Add editor ...
<input type="checkbox"/>	HR Admins Container	Administrative Container		Add approver ...	Add editor ...
<input type="checkbox"/>	1FridayView	GPO	sdm.lab/System/Policies/{d858df28-98c1-4cfa-80a0-7d42dca0fc33}	Add approver ...	Add editor ...
<input type="checkbox"/>	1testMon	GPO	sdm.lab/System/Policies/{7bb30ea0-46e8-4287-b4a0-9f01045b0cb1}	Add approver ...	Add editor ...
<input type="checkbox"/>	Clean_GPPPlug	GPO	sdm.lab/System/Policies/{C8CA0A5E-240A-429C-8F1B-7EFD2140E733}	Add approver ...	Add editor ...
<input type="checkbox"/>	Android (AOISP) - Device restrictionX	Intune Profile	Android (AOISP)/Template/Android (AOISP) - Device restrictionX	Add approver ...	Add editor ...
<input type="checkbox"/>	child	Domain	child.adm.lab/	Add approver ...	Add editor ...







Notice a  symbol next to the name of the AC. Select it to expand and show all of the objects assigned to it, as shown here:

HR Admins Container

Administrative Container

Add approver ...

Add editor ...

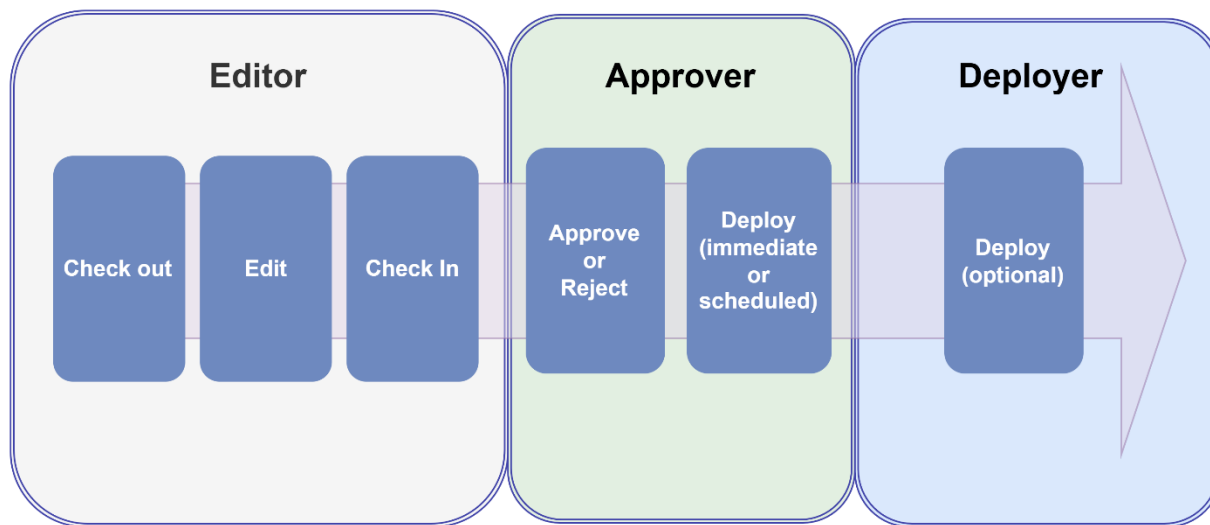
Name ▾	Type ▾	Canonical Name ▾
 Sales	OU	sdm.lab/Sales
 Marketing	OU	sdm.lab/Marketing
 HQ	OU	sdm.lab/HQ
 MigrateMasterNonAdmin	GPO	sdm.lab/System/Policies/{FB8B4CFB-C6DB-4EFB-8196-4241A0425107}
 Enforce Local Admin and UNC hardening	GPO	sdm.lab/System/Policies/{D8572F9D-9062-434C-889F-DC516B470F0C}
 MigrateAllTestCopy	GPO	sdm.lab/System/Policies/{574ed0-2564-4af5-af18-495ec7d8f159}

When you set an editor, approver, and deployer for the AC, all of the objects within the AC inherit those roles. Also, when searching for an object by name, that is within an AC, using the column-based filters

for each column, the result will show the AC that contains the object, which you'll need to expand to see the object itself.

The Change Control Process

The main goal of CMGPI is to provide an approval-based workflow to facilitate controlled changes to GPOs, containers and Intune Profiles and their deployment within the environment. The change process within CMGPI follows this progression:



The CMGPI Change Workflow

Understanding AD vs. Entra ID Editors & Approvers

CMGPI supports the use of Entra ID for SSO for delegation to both global and per-object roles. You can specify Entra ID users or groups as members of a role, by entering the User Principal Name (UPN) of the Entra ID User or the Display name of the Entra ID group as shown below:

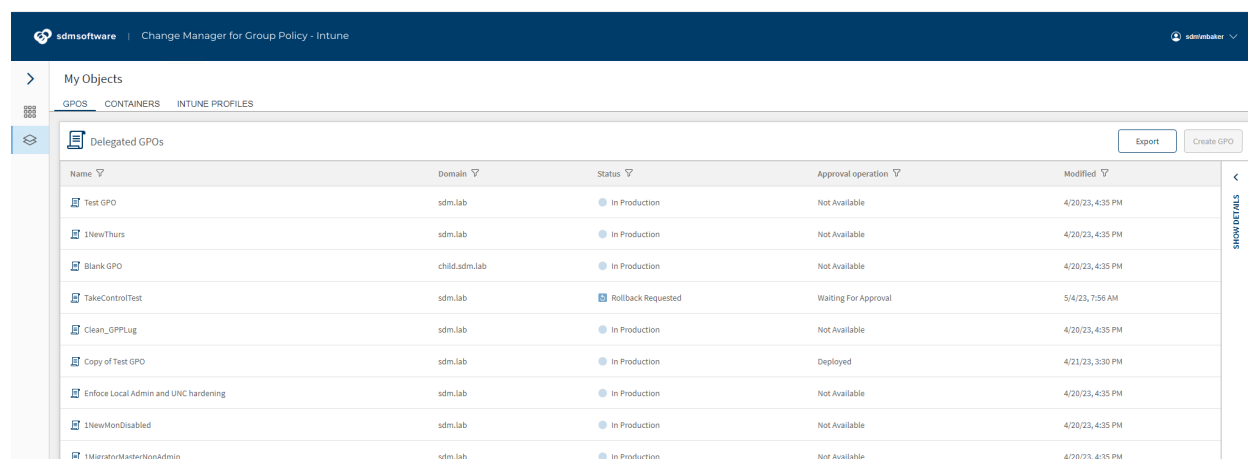
The screenshot shows the 'Delegation - Objects' interface in CMGPI. It displays a table of objects with columns for Name, Type, Canonical Name, Approver(s), and Editor(s). A modal window is open for adding editors, showing a list of roles and a search bar. The roles listed are 'CMGPI Entra Editors' and 'jkelly@sdmqlab.onmicrosoft.com'.

Name	Type	Canonical Name	Approver(s)	Editor(s)
Custom Attribute script	Intune Profile	macOS/Custom attribute/Custom Attribute script	Add approver ...	Add editor ...
simple settings catalog	Intune Profile	Windows 10 and later/Settings Catalog/simple settings catalog	Add approver ...	Add editor ...
MigrateAllTest	GPO	sdm.lab/System/Policies/(B0A862FD-EB22-4BFF-83B3-977B83DF100D)	Add approver ...	CMGPI Entra Editors, jkelly@sdmqlab.onmicrosoft.com
Android (AOSP) - Trusted certificate	Intune Profile	Android (AOSP)/Template/Android (AOSP) - Trusted certificate	Add approver ...	Add editor ...
Test Android Profile	Intune Profile	Android device administrator/Template/Test Android Profile	Add approver ...	Add editor ...
NewMonDisabled	GPO	sdm.lab/System/Policies/(BDA31A0F-8BD2-4A31-8872-1EF336BA8B3)	Add approver ...	Add editor ...
Copy of Test GPO	GPO	sdm.lab/System/Policies/(608F2A7-DE04-4810-924B-247FFC82D36C)	Add approver ...	Add editor ...
TakeControlTest	GPO	sdm.lab/System/Policies/(A16A9759-5A1C-47E6-8E17-BD0EAD344114)	Add approver ...	Add editor ...

There are some considerations around object editing that you'll need to think about, but in general the following rules apply when enabling Entra ID SSO within the product:

- You can log in to the product as either an AD or Entra ID user (or member of an AD or Entra ID security group) as long as you've been granted access to either a CMGPI global role or an object-based role.
- To edit GPOs as an Entra ID user, you need a corresponding AD account. When CMGPI launches the GP Editor out of the web application, you're prompted for **AD credentials**. This is because editing GPOs is still an AD operation—and is not “Entra ID-aware.” When an Entra ID user checks out a GPO, the temporary GPO that gets created by CMGPI gets permissioned with the corresponding AD account that's associated with the Entra ID user who performed the check-out. This assumes that you are synchronizing AD objects with Entra ID and using the AD-based **mS-DS-ConsistencyGuid** attribute to map the AD user to its Entra ID equivalent. This is a requirement for editing GPOs as an Entra ID user.
- Conversely, to edit Intune Configuration Profiles as an AD user, CMGPI expects you to authenticate to the temporary Intune profile that gets created on check-out, using the corresponding Entra ID user that is being synchronized from the AD user who performed the check-out.

As an editor, the starting point after logging in to the CMGPI console is the **My Objects** page:

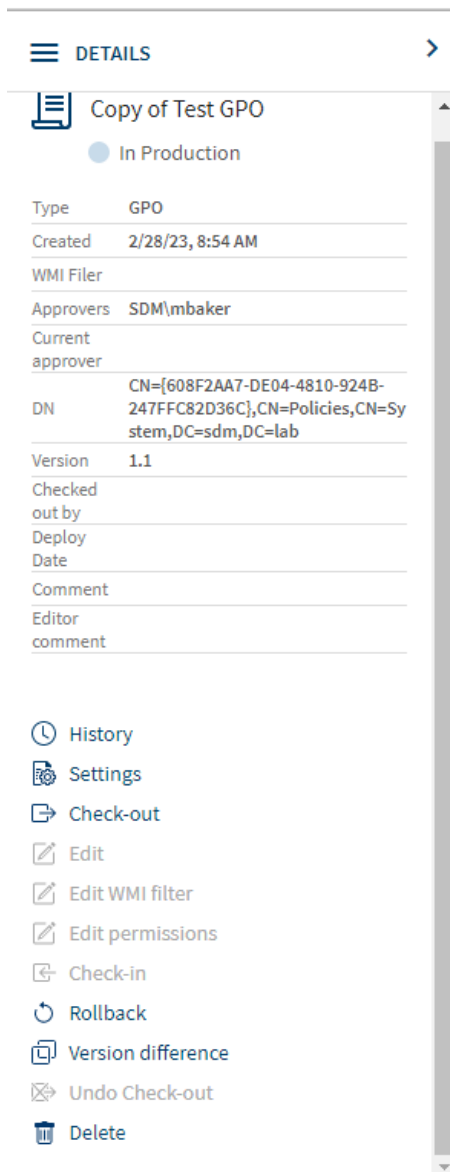


Name	Domain	Status	Approval operation	Modified
Test GPO	sdm.lab	In Production	Not Available	4/20/23, 4:35 PM
1NewThurs	sdm.lab	In Production	Not Available	4/20/23, 4:35 PM
Blank GPO	child.sdm.lab	In Production	Not Available	4/20/23, 4:35 PM
TakeControlTest	sdm.lab	Rollback Requested	Waiting For Approval	5/4/23, 7:56 AM
Clean_GPPLug	sdm.lab	In Production	Not Available	4/20/23, 4:35 PM
Copy of Test GPO	sdm.lab	In Production	Deployed	4/21/23, 3:30 PM
Enforce Local Admin and UNC hardening	sdm.lab	In Production	Not Available	4/20/23, 4:35 PM
1NewMonDisabled	sdm.lab	In Production	Not Available	4/20/23, 4:35 PM
1MigratorMasterNonAdmin	sdm.lab	In Production	Not Available	4/20/23, 4:35 PM

The My Objects page

There are three tabs across the top of the grid, for GPOs, containers, and Intune Profiles. Each shows the objects for which the current user is editor, approver, or deployer.

To manage an object, select its row, and the **Details** pane on the right-hand side of the grid will expand for it. The details pane shows properties of the object as well as the actions you can perform against it, as shown below:



The Details Pane of an object

Actions currently available are shown as dark text, while grayed out options are not available in the current state.

As an editor, the first step is to check out the object in question. Let's walk through the editing process for GPOs, containers, and InTune Profiles.

Editing GPOs

Once you click Check-out, you will see a status message appear in the upper right of the window, as shown below:

A dark blue horizontal bar with a lighter blue rounded rectangle in the center containing the text "Check-Out in progress".

Check-Out in progress

Handling Out-of-Band Changes

CMGPI checks for changes that have happened to controlled GPOs, AD containers or Intune profiles outside of the product. At check-out time, if such an out-of-band change is detected, you'll see the following dialog appear:

Check-out

Production version of this object is not consistent with the last approved version.

[Show difference report](#)

- ☒ Roll-back the production version to the last controlled version.
- ☐ Check-out anyway, ignoring the difference.

Ok

Cancel

From this dialog, you can view the difference report to show the difference between what's currently in production and what CMGPI knows is the last known good version deployed, and choose how to handle it. The first option, "Roll-back the production version to the last controlled version," overwrites what's in production with the backup of the last known good object held by CMGPI. This creates a new check-in event that an approver has to approve, to deploy the rollback. If you choose the second option, "Check-out anyway, ignoring the difference," CMGPI will check out the existing version as it stands, and any changes you make will incorporate those out-of-band changes (unless they are undone during the edit).

Once the check-out is complete, you will see different action items available on the details pane and the status column for that GPO will show "Checked Out." You then have access to the following things:

- **History:** View the history of what changes have been committed to the GPO since the product took control of it.
- **Settings:** Display the current settings within the production GPO.
- **Export:** Create a zip archive containing a GPMC backup of the GPO to facilitate transfer of the object to another environment for testing.
- **Edit:** Launch the GPO Editor against the checked out GPO.

- **Edit WMI Filter:** Add or remove an existing WMI filter to the GPO.
- **Edit Permissions:** Edit the delegation on the GPO to create security filters (users, computers or groups that can read or apply the GPO).
- **Check In:** Finish the editing process, add a comment and submit the change for approval.
- **Version Difference:** Show the GPO differences between different versions.
- **Undo Check out:** Cancel the check out process and discard any changes.
- **Delete:** Mark the GPO for deletion (an approver still has to approve the change to delete the actual GPO).

Behind the scenes in CMGPI, when you check out a GPO, a temporary copy of that GPO is created in AD. These copies are only manageable by the CMGPI service account and the editor who checked it out, and they have a very distinct naming structure, as shown here:

temp-{0BC734DB-92DB-4A82-8F9D-A38DC37A9D46}_e9fbd8a-6f8c-4ae0-9168-d7def1055478_{31B3C418-1848-438B-AE3B-C86841D8BA09}

Scope	Details	Settings	Delegation	Status
Domain:	sdmssoftware.net			
Owner:	svc cmgp (svc.cmgp@sdmssoftware.net)			
Created:	5/16/2022 9:30:19 PM			
Modified:	5/16/2022 9:30:04 PM			
User version:	1 (AD), 1 (SYSVOL)			
Computer version:	1 (AD), 1 (SYSVOL)			
Unique ID:	{7B3DB312-9923-44A4-A5F6-0E9FD2E9F459}			
GPO Status:	Enabled			
Comment:				

Newly created GPOs get a temporary name that starts with “new-“. Existing GPOs get a name that starts with “temp-“.

They should not be removed or modified manually. CMGPI will clean up these temporary GPOs when a check-in is either deployed or cancelled.

When you select edit, a couple of things happen. First, there is a special GP Editor tool launcher utility that gets installed the first time CMGPI is run on a given Windows machine. This application can be pre-installed using the link from the CMGPI home page (for CMGPI Product Administrators) or as an editor, when they select Edit from the Detail action menu. You will see the following tab open in the browser:



If Group Policy Editor does not open after a few seconds please [download group.policy.editor.tool.launcher](#)

Click the link above to download the MSI installer for the Group Policy editor tool launcher and then run the installation. This only needs to be done one time for any machine where GPO editing is occurring. (The MSI installer can also be found in the following folder on the CMGPI server: C:\Program Files\SDM Software\CMGPI\UI\Setup.)

Any user who is editing GPOs on a given client system, will need administrative access on that system to launch the GP Editor.

Once the editor tool launcher is installed, close the tab and select the Edit action again.

*The CMGPI editor client requires that **Microsoft GPMC** be installed on any system where GPO editing is occurring.*

The first time through, the following message will appear:

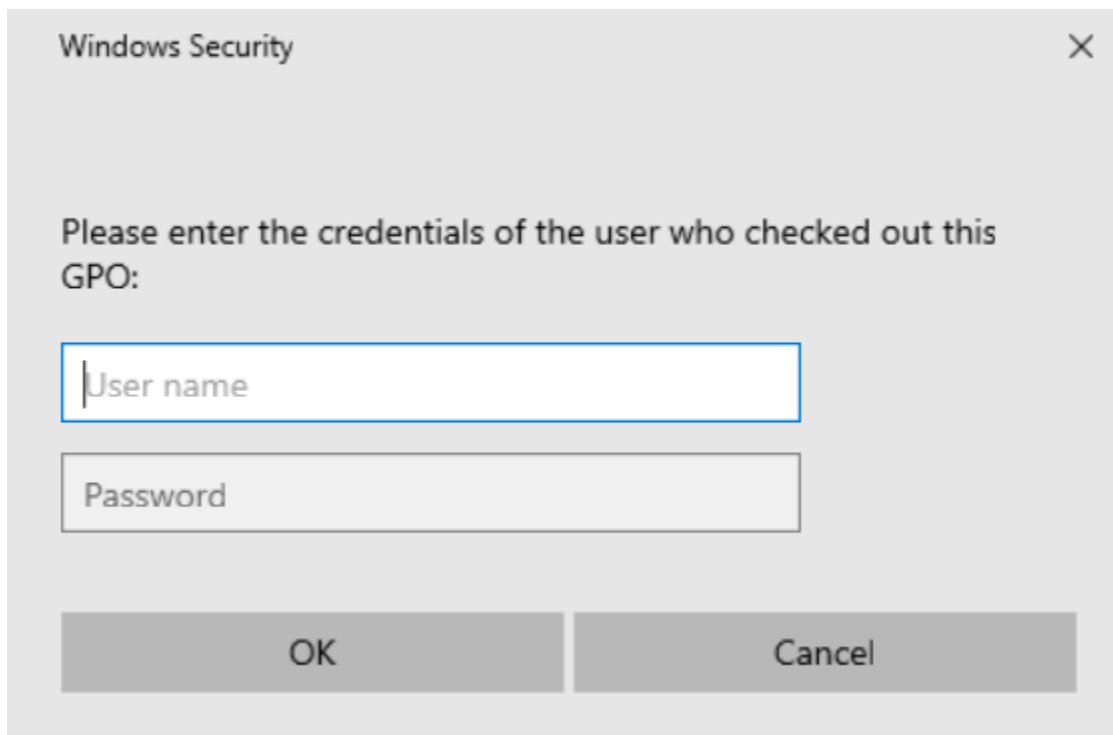
Open Change Manager ...cy GPMC Driver?

https://cmgp-sdm.sdmsoftware.net wants to open this application.

☐ Always allow cmgp-sdm.sdmsoftware.net to open links of this type in the associated app

[Open Change Manager for Group Policy GPMC Driver](#) [Cancel](#)

Select to “Always allow...” if you want to trust the application to associate itself with the link that launches it on this machine. Then press the “Open Change Manager for Group Policy GPMC Driver” button to launch the GP editor. **The editor user will need to enter their AD credentials at the following Windows prompt:**

A screenshot of a Windows Security dialog box. The title bar says "Windows Security" with a close button (X) on the right. The main text reads: "Please enter the credentials of the user who checked out this GPO:". Below this text are two input fields: the first is labeled "User name" and the second is labeled "Password". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Entering credentials to launch the GP Editor

Once credentials are entered, the familiar GP editor screen will appear, focused on the checked out GPO, and you can make GPO settings changes as you normally would. When you are finished making changes to the GPO, close the GP Editor.

After a change has been made, it is not yet deployed (or even approved). You can make other changes to a GPO while it's checked out. For instance, you can rename a GPO, and you can edit delegation on a GPO, before checking it back in for approval.

Creating a new GPO

The GPO creation process requires the user to have the **GPO Creator** role. From the My Objects page, when logged in with a GPO Creator user, the **Create GPO** button on the upper right allows you to create a new GPO. When you click the button, you have the option of creating a new, empty GPO, or creating a copy of an existing GPO, where that source GPO's settings and delegation are copied to the new GPO. You can also choose to check out the newly created GPO once it's created. This allows you to modify settings on that new GPO and send it through the same change process as any other GPO. If you don't choose to check out the GPO on creation, it will be created and automatically checked in, waiting for approval. Note that since you are creating a new GPO, the default approver that was specified in the product's General, Settings page will be the one who can approve this GPO unless a Product Administrator specifies another approver for it.

Deleting a GPO

An editor can issue a request to delete a GPO. The **Delete** option appears at the bottom of the Details pane. When the editor creates a delete request, they can associate a comment with that request, as shown here:

×

Warning

If you delete this GPO, all links to controlled containers in any managed domains will be deleted.

Comment to approver:

Submit

Cancel

When they submit the request, the GPO is automatically placed in “Waiting for Approval” mode, and the approver can approve the deletion process and “deploy” it to production, which results in the GPO being deleted from Active Directory.

When a GPO is deleted in CMGPI, any links to that GPO are also removed, including links in other domains that are under control by CMGPI.

Restoring a Deleted GPO

When a GPO that has been managed by CMGPI is deleted, it can be restored by the CMGPI Product Administrator. Deleted GPOs are listed in the Settings, Deleted GPOs menu item for Product Administrators, as shown here:

Dashboard

My Objects

Delegation

Product Roles

Objects

Audit log

Settings

General

Target DC

Take Control

SSO

InTune

Deleted GPOs

Administrative Containers


Logs Upload

License

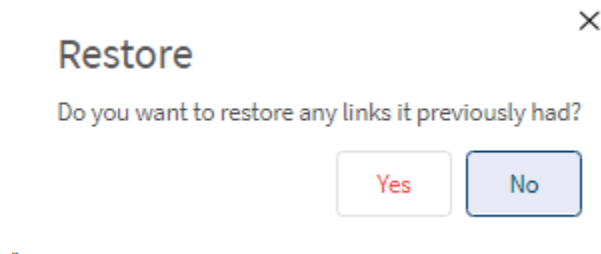
Settings • Deleted GPOs

Deleted GPOs

Name ▾	Domain ▾	DN ▾	Modified ▾	Approver ▾	Editor ▾
MultiLinkDelete	sdm.lab	CN=39e55ac-b3e0-40b5-bc0e-a2c323dc73f5,CN=System,DC=sdm,DC=lab	6/24/24, 3:43 PM	SDM_jkelly	SDM_umbaker

Only Product Administrators can restore Deleted GPOs. You can initiate a GPO restore by clicking the  at the right end of the row listing the GPO to be restored.

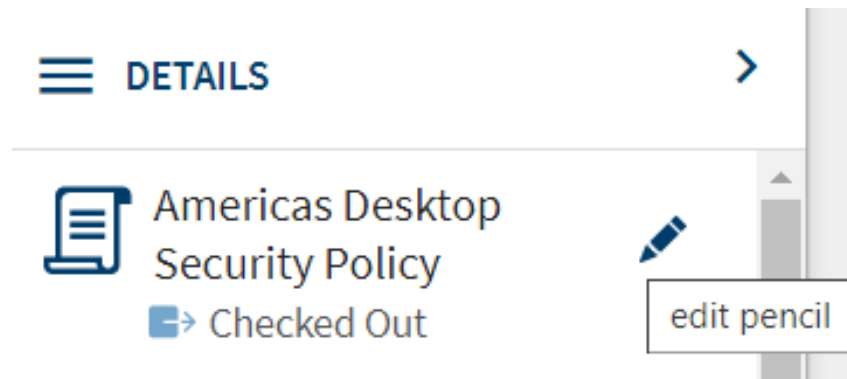
You'll be prompted to confirm the restore. You will then be prompted 'Yes' or 'No' to restore any links that the GPO had before it was deleted.



Note that any links, both within the GPO's domain as well as other domains managed by CMGPI, will be restored if you choose 'Yes.' Be aware that the restore process does not go through a change control workflow. Once a Product Administrator restores a GPO, it is live in the environment again without need for approval.

[Renaming a GPO](#)

To rename a GPO while it's checked out, select the pencil icon that appears to the right of the GPO name in the Details pane, as shown here:



When you click the edit pencil, you can change the name of the GPO and click the check mark to accept the change. The name change is a valid change event within CMGPI and will need to go through the same approval-based workflow as any other GPO change.

[Changing WMI filters](#)

You can add or remove a WMI filter from a GPO as part of the change process, from the GPO's Details pane. Select an existing WMI filter from the dropdown, as shown below, or choosing <None> to remove an existing WMI filter.

Edit WMI Filter



This GPO is linked to the following WMI filter:

Name:

Changing GPO Delegation

GPO delegation can also be changed as part of the change approval process, from the GPO's Details pane. Delegation of GPOs controls elements such as which computers and users can process a GPO. Once a GPO is checked out, you can make delegation changes by selecting the **Edit Permissions** link on the Details pane. The dialog that appears will show all security principals that currently have read or read and apply permissions on the GPO. You can add new ones or edit existing ones as shown below:

Delegations

Americas Desktop Security Policy

Group and users: Permissions:

Name	Permissions	
NT AUTHORITY\Authenticated Users		
SDMSOFTWARE\GPO Admins	Read	no
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	no

Modifying GPO Delegation

You can only set read, apply and deny apply permissions on a GPO.

CMGPI does not expose edit settings or edit settings, delete and modify security permissions on GPOs because those could be used to circumvent the controls that are put in place when a GPO is taken under control by CMGPI.

Check in a GPO

For an editor, once the edits to the GPO have been made, it's time to check in the GPO. Choose **Check-in** from the Details pane on the currently selected GPO. You will receive a popup that allows you to record comments related to the GPO change you just performed. You can also optionally record the severity of the change and a "change ticket" number associated with the change. These comments and details are stored with the change through its lifetime and can be referenced when you view differences on a given GPO or from the **History** view on the Details pane.

The Product Administrator can require that comments be added to any check-in from the Settings, General menu.

Check-in



1NewMonEnabled

Severity:

Urgent

Ticket number:

33495600

Comment to Approver:

Updating local Administrators group membership on Engineering Servers

Ok


Cancel

Comments recorded with a GPO change


Once the check-in process completes, the job turns to the approver for that GPO.


Approving and Deploying GPO Changes

Once an editor has checked in a GPO change, any designated approver for that GPO will be notified via email, as shown here:

 Americas Drive Mapping Policy
Waiting Approval

Difference Report

Added: 1 Removed: 0 Changed: 0	V.1.1 Modified: 2022-05-18T17:44:07.4630000Z	Checked-in version
Computer Configuration>Policies>Windows Settings>Security Settings>Account Policies		
Password Policies		
Enforce password history		10 

 More Details

Approve

Reject

Approver email notification

The approver can approve or reject this request by clicking the buttons in the email, which will direct them to the appropriate page in the CMGPI application (this implies that the user has access to the CMGPI web UI from the device where they're reading their email). The email also includes a difference report of what has changed. These changes can also be seen from the Details pane when the checked-in GPO is selected within the web application.


If the approver decides to reject a checked-in GPO, the approval request is discarded and the object is returned to the Checked Out state for the editor to address it. The editor will receive an email from CMGPI letting them know it was rejected and needs their attention.

Once the approver has logged in and approved the outstanding change, the state of the GPO enables the **Deploy** option on the Details pane. If you have enabled the separation between the approver and deployer roles, introduced in version 1.9 (see the CMGPI Installation Guide for information on how to enable this feature), then an email notification will be sent to the designated Deployer for this object. If not, then as an Approver, you can press Deploy from the Details menu, which presents a dialog that allows the approver to either deploy the change immediately or schedule it for deployment at a future day/time, as shown below:

Deploy

- ☐ Deploy immediately
☒ Schedule to Deploy

Schedule deployment date

5/20/2022, 23:30:00 

☐ Roll back to production version if scheduled deployment fails.

Ok

Cancel

Scheduling a deployment

The workflow for deploying a change is the same regardless of whether you are an approver or a deployer. The main difference between the two is that once a change is approved by the approver, a separate deployer user will be notified via email about the change waiting to be deployed, and they can log into the CMGPI console and schedule the deployment.

If you decide to schedule a deployment in the future, you can optionally check the box to roll back the attempted deployment if it fails. If you choose this option, then if a scheduled deployment fails, CMGPI will take the last known-good backup of the object being changed and apply it to production.

When a scheduled deployment completes, regardless of success or failure, an email notification will be sent to the editor, approver, and deployer, indicating the status of the deployment. This applies to all types of deployments—GPOs, AD containers and Intune Profiles.

When an object is deployed, the My Objects page's status, approval operation and modified columns will be updated to reflect the new state of the object.

*If a GPO, container or Intune profile has been checked out by an editor and that check out lingers past **7 days** (default), an email notification will be sent to the editor reminding them that the checkout has been lingering. In addition, if an editor has*

*checked in a change and the approver has not responded to that within **5 days**, the approver is sent an email to indicate that the approval is overdue. Both intervals can be adjusted using the CMGPI PowerShell cmdlet Set-CMSettings, and the option is described in [Appendix B: Customizable settings within CMGPI](#).*

Editing AD Containers

The container editing workflow is very similar to the GPO one. But of course, in the case of containers, you are editing GPO links on those containers rather than the GPOs themselves.






The first step as an editor for a set of containers is to select the container you wish to change from the My Objects page, and then from the Details pane, select Check-out. Click the Edit button to bring up the container links editor, as shown here:

Edit Containers links

Look for existing GPO in the domain:


Select existing GPO:

Linked to:

Name 		Domain 	
	Enforce Local	sdm.lab	
	 Admin and UNC hardening		

☒ Block inheritance

Editing container links

As the figure shows, any existing links on this container (site, domain or OU) will appear in the list in the order that they are linked (i.e. the first GPO in the list is in link order 1, etc.). You can change link order by left-clicking, holding and dragging a GPO up or down in the list. If you click the three dots to the right of the link () you can choose to disable, enforce or delete a link. To add a new GPO link, select the domain that houses the GPO you wish to link to this container, then choose the dropdown list under **Select existing GPO** to choose a GPO. Click the Add button to add the GPO to the link list. The GPO will be added to the end of the list.



Click OK when you're done editing the link list and then click Check-in from the Details pane to commit the change.

Note that you can also control the container Block Inheritance flag by checking or un-checking the box in the lower left of the dialog, entitled "Block Inheritance."



Approving and Deploying Container Changes


The approver will be notified via email when a container is waiting for approval, as shown here:

From: SDMSOFTWARE\kvmedenadmin
Comment: Added Americas drive mapping link

 EMEA
 Waiting Approval

Difference Report

Added: 1 Removed: 0 Changed: 0	V.1.0 Modified: 2022-05-12T22:35:30.5300000Z	Checked-in version
sdmssoftware.net/Americas Drive Mapping Policy		
Enabled		True 
Enforced		False 

 More Details

The approver can click the links in the email to either approve or reject the link change. Or they can click "More Details" to be taken to their My Objects page within the CMGPI application.

Once the link change is approved, the approver (or deployer, if you've enabled the separate approver and deployer roles) can then choose to deploy it immediately or on a schedule, as with GPO changes. The same options are available as shown in the figure above.

Once deployed, the GPO link will be updated in production and the status on the My Objects page will reflect that change.

For scheduled deployments of either GPOs, containers or Intune Profiles, an approver or deployer can choose to cancel the deployment by selecting the "Cancel Deployment" option on the object from the Details pane.

Preparing to edit Intune Profiles

The process of editing Intune profiles is slightly different from editing GPOs and containers. When an Intune profile is taken under control by CMGPI, a CMGPI-specific “scope tag” is added to the profile, which prevents regular Intune administrators from being able to edit that profile. That scope tag is called **CMGPI_Controlled**.

The process of designating editors and approvers to Intune profiles is the same as for GPOs and containers. However, there’s an extra step you must take to allow Intune profile editing. Currently, when you assign editors and approvers to Intune profiles in CMGPI, you are assigning Active Directory or Entra ID users or groups to those roles. However, when it comes time for an editor to actually edit a profile, they will authenticate to Entra ID using their Entra ID credentials. For example, if you assign the AD user *mycompany\joesmith* as an editor for an Intune profile in CMGPI, when that user logs into the CMGPI console and selects the Edit option for that profile, they will be prompted to authenticate using their corresponding synchronized Entra ID user (see the section entitled [Understanding AD vs. Entra ID Editors & Approvers](#) for more information) in order to edit that profile.

Before they can do that, you will need to grant access to Entra ID users whom you designate as Intune profile editors in CMGPI ahead of time. This is done using a provided PowerShell script called **GrantAccess.ps1**, which is found in %programfiles%\SDM Software\CMGPI\Svc.

This script does a few things. The first time it runs, it creates an Entra ID security group called **CMGPI Intune Editors**. It also creates an Entra ID custom role called **CMGPI editing temporary entities role**, and adds the CMGPI Intune Editors group to it. This role is then scoped to the scope tag called **CMGPI_Temporary_Entity** (more on this in a bit). Finally, the script adds any user who will be editing Intune profiles, to the CMGPI Intune Editors group.

*You will need to run **GrantAccess.ps1** for all Entra ID users who will be editing Intune profiles within CMGPI.*

So as an example, for our user *mycompany\joesmith* the script would be run as follows:

```
.\Grantaccess.ps1 -Username joe.smith@mycompany.com -CMGPIServerName <CMGPI Server FQDN>  
-Tenant ID <GUID of your Entra ID tenant> -AccountID <user principal name of the Entra ID user who  
has the ability to create and update groups in Entra ID>
```

Where [joe.smith@mycompany.com](#) is the user’s Entra ID user principal name.

When you run the script, you’ll be prompted for the Entra ID credentials of the user specified in the AccountID parameter, which should have the ability to add a security group and custom role to your Entra ID tenant.

Editing Intune Profiles

When an Intune editor checks out an Intune profile, CMGPI will create a temporary profile within the Intune tenant, which is a copy of the original. It is the temporary copy that a CMGPI Intune editor edits when they have the profile checked out. CMGPI provides the ability to change the following aspects of an Intune Configuration Profile when it's checked out:

- Profile Name
- Profile Description
- Settings within the profile
- Scope tags assigned to the profile
- Assignments to the profile

From version 1.9, CMGPI supports secret fields, such as passwords or encryption keys, within Intune profiles. When checking out an Intune profile containing secret fields, CMGPI requires the user to provide the associated passwords for verification purposes. To ensure accuracy, the user must confirm the password by re-entering it.

Secret fields

Some settings contains secret fields

Field Name	Setting Name	Password	Re-type password
Profile Removal Password	Removal Password
Air Play aa	Password		
Air Play bb	Password		

Everything except the settings within the profile can be modified within the CMGPI web application. Settings, however, are only modified directly from the temporary copy of the profile created within Intune. When a CMGPI editor clicks Edit on a profile, a new browser window is opened focused on the temporary Intune profile, as shown here:

Microsoft Intune admin center

Home >

temp-TestSettingsCatalog_b24ecd05-7bee-480a-a126-5fbb2c860718 ✨ ...

Device configuration profile

Delete

Device and user check-in status

Succeeded | Error | Conflict | Not applicable | In Progress

0 | 0 | 0 | 0 | 0

[View report](#)

Device assignment status

This report shows all the devices that are targeted by the policy, including devices in a pending policy assignment state.

Per setting status

View the configuration status of each setting for this policy across all devices and users.

Properties

Basics [Edit](#)

Name: temp-TestSettingsCatalog_b24ecd05-7bee-480a-a126-5fbb2c860718

Description: --

Platform: Windows 10 and later

Assignments [Edit](#)

Included groups

Group	Filter	Filter mode
No results.		

Excluded groups

Group

You will edit Intune settings on this profile just as you would any other Intune profile.

You should NOT use this Edit Settings interface to try and edit scope tags or assignments for the profile. That is done from the CMGPI Edit links next to Scope Tags and Assignments on the Details pane of a checked-out profile.

The options you have available when managing an Intune Profile are presented in the following figure and described below:

DETAILS

TestSettingsCatalog

In Production

Created

7/18/22, 9:54 AM

Approvers

SDM\mbaker

Current approver

CN

Windows 10 and later/Settings Catalog/TestSettingsCatalog

Version

1.1

Checked out by

Deploy Date

Editor comment

Description:

Scope Tags:

Default

CMGPI_Controlled

Assignments:

Include groups

0

Exclude groups

0

History

Settings

Check-out

Edit Settings

Check-in

Rollback

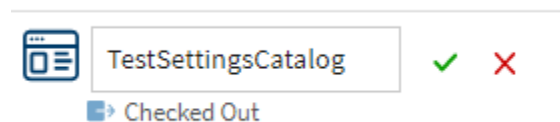
Version difference

Undo Check-out

This is very similar to both GPOs and containers with a few exceptions, such as the ability to edit scope tags and assignments.

Rename an Intune Profile

You can rename an existing Intune profile by clicking the pencil icon on the name of the profile after it's been checked out:





Once you've changed the name, click the green check box to confirm, or red x to cancel the edit.

Editing Intune Scope Tags

To edit scope tags that are applied to a profile, click the edit link next to the Scope Tags section on the details pane. Once you do that, the existing tags on the profile are presented and you can choose to add or remove its tags from here. Note that the list of available scope tags are defined in your Intune tenant and cannot be added or deleted from CMGPI:

Scope Tags

	Name 
<input checked="" type="checkbox"/>	Default
<input type="checkbox"/>	CMGPI_Temporary_Entity
<input type="checkbox"/>	Test2
<input checked="" type="checkbox"/>	CMGPI_Controlled
<input type="checkbox"/>	Test 3
<input type="checkbox"/>	TestTag

Also note that tags that are applied by CMGPI when it takes control of a profile cannot be removed and are shown as greyed out.


Editing Intune Assignments

You can edit assignments on a profile as part of the CMGPI change control process. Note that assignments control what users/groups/machines will apply an Intune profile. Just as with scope tags, you can edit assignments in CMGPI by clicking the Edit link next to the Assignments section of the Details pane, which will bring up a dialog as shown here:

Assignments


Include groups ☒ Groups ☐ All users/devices

Type group or user name

Name 	Filter mode	Filter
--	-------------	--------

Exclude groups

Type group or user name

Name 

This dialog mimics the capabilities in Intune itself. Notably, you can both include and exclude groups, and that can include either Entra ID groups or users or all users/devices. If you are adding groups, you can start typing the name of the Entra ID group in the text box and CMGPI will query your Intune tenant for available groups. Once you add a group, you can click the pencil icon on the group entry and alternately select to include or exclude an existing Intune filter (note that you cannot edit or create filters within CMGPI) as shown here:

Assignments

Include groups ☒ Groups ☐ All users/devices

Name ▾	Filter mode	Filter		
SDM Software Marketing	Include ▾ ...	TestFilter (Windows 10 and I	✓	✗

Exclude groups

Name ▾

A similar capability for searching excluded groups also exists in that dialog and you can choose to add excluded groups to this profile's assignments from this screen.

Approving and Deploying Intune Profiles

Once an Intune profile change is checked in by an editor, assigned approvers may log in and respond to the check-in. Just as with GPOs and containers, you can approve and then deploy immediately or on a schedule. And, as in the case with GPOs and containers, if you've separated the approver and deployer roles, an approver can only approve the changes, while the deployer can deploy them. As in the case of GPOs, when you deploy a profile change, the temporary Intune profile created by CMGPI will be written to the production profile, along with its assignments and scope tags, and the temporary profile will be deleted.

Audit Log

All activities performed within CMGPI are logged to the audit log, as shown in the figure below:

Audit log

Events found: 114					
Date and Time ▾	Activity ▾	Object ▾	Location ▾	Status ▾	User ▾
5/20/22, 5:22 PM	✔ Approve	EMEA	sdmsoftware.net	Success	sdmsoftware\lgrangeradmin
5/20/22, 5:22 PM	✔ Approve	EMEA	sdmsoftware.net	Started	sdmsoftware\lgrangeradmin
5/20/22, 5:09 PM	✔ Check-in	EMEA	sdmsoftware.net	Success	sdmsoftware\kvendenadmin
5/20/22, 5:09 PM	✔ Check-in	EMEA	sdmsoftware.net	Started	sdmsoftware\kvendenadmin
5/20/22, 4:45 PM	✔ Check-out	EMEA	sdmsoftware.net	Success	sdmsoftware\kvendenadmin
5/20/22, 4:45 PM	✔ Check-out	EMEA	sdmsoftware.net	Started	sdmsoftware\kvendenadmin
5/20/22, 4:34 PM	✘ Reject	Client Desktop Policy	sdmsoftware.net	Success	sdmsoftware\lgrangeradmin
5/20/22, 4:34 PM	✘ Reject	Client Desktop Policy	sdmsoftware.net	Started	sdmsoftware\lgrangeradmin
5/20/22, 4:31 PM	✔ Deploy	Americas Desktop Security Policy	sdmsoftware.net	Success	sdmsoftware\lgrangeradmin
5/20/22, 4:31 PM	✔ Deploy	Americas Desktop Security Policy	sdmsoftware.net	Started	sdmsoftware\lgrangeradmin

DETAILS

EMEA

✔ Approve

Date and Time5/20/22, 5:22 PM

Locationsdmsoftware.net

Usersdmsoftware\lgrangeradmin

StatusSuccess

Canonical Namesdmsoftware.net/EMEA

Viewing the CMGPI audit log

The log reports the date and time of the activity, the type of activity performed, the object on which it was performed, the domain where that object resides, the status of the activity and the user who performed the activity. Note that each activity typically has a “start” event that indicates the activity was initiated by the user, and then a second activity that indicates whether it was successful or generated an error. You can view the details of a selected activity from the Details pane on the right of the audit list. To extract a list of audit events from CMGPI, click the Export button at the upper right of the log, or use the PowerShell cmdlet **Get-CMEvents**.

All audit log entries are recorded to a custom event log within the Windows event log. This event log can be found in Event Viewer under **Applications and Services Logs** and is called **CMGPI**.

Licensing

Licensing can be viewed and managed only by a CMGPI product administrator. They can see and manage licensing from the Settings, License page, as shown here:

Settings • License

License Mode:	<input type="text" value="Demo"/>
Company:	<input type="text"/>
Contact:	<input type="text"/>
Time Remaining:	<input type="text" value="17 day(s)"/>
Expiration Date:	<input type="text"/>
License count:	<input type="text" value="0"/>
License status:	Valid
Activate a new license:	<button>Upload new license</button>

Viewing and managing the CMGPI license

License details include the mode of the license and the days remaining as well as the number of computer accounts you are licensed for, in the case of a customer license. When you receive a new license file from SDM Software, you can activate it by clicking the “Upload new license” button and browsing to the license file you received. Once the new license is activated, the details in the license page will update with the new information. If you have issues activating your CMGPI license, contact support@sdmsoftware.com to get more details.

Appendix A: Using the SetCMGPPermissions.exe to grant initial permissions required by CMGPI

A prerequisite for using CMGPI is to ensure that the proper native delegation permissions exist on your GPOs and AD containers, prior to taking control of those objects. This process requires granting your CMGPI service account the ability to modify the permissions of GPOs and AD containers. For GPOs, this amounts to granting the CMGPI service account the “Edit settings, delete and modify security” permission on GPOs that are managed by CMGPI. For AD containers (AD sites, domains and OUs) the permission required by the CMGPI service account in order to take control is simply the “modify permissions” right. This allows the service account to control who can link GPOs to containers, by controlling write permissions on the gpLink and gpOptions attributes on those containers.

CMGPI provides a command-line utility called **SetCMGPPermissions.exe** that sets the correct permissions on GPOs and containers that are required for CMGPI to function.

The SetCMGPPermissions utility must be run under an AD account that has sufficient permissions to modify the underlying GPO and AD container objects.

The utility is installed by default when you install CMGPI, in the **C:\Program Files\SDM Software\CMGPI\Svc** folder, and supports the following syntax:

```
usage: SetCMGPPermissions.exe -Trustee <Domain\Username format of account to grant
access> [GPOs] <cmnd> [option] [<cmnd> [params] ...]
to modify GPOs supply one or more domains to search and optionally comma-separated list of
GPO IDs
-Domain <DNS Domain Name> -All
-Domain <DNS Domain Name> -GPOIDs <ID[,ID...]>

commands are:
-GPOCreator
-GPOModify
-Container <Optional DN of parent container--OU or domain DN>
-Site <Optional DN of site or parent of all sites>
-Recurse
-Server <server name>
```

The -Trustee and -Domain parameters are mandatory. The Trustee you provide is the name of the CMGPI service account in the form of <domain\username>. The Domain parameter should be the DNS domain of the domain or forest you are changing. Here is an explanation of what each parameter does:

- **GPOCreator:** Grants the CMGPI service account GPO creator rights on the domain. This is required to ensure that CMGPI functions properly.

SetCMGPPermissions.exe -trustee sdmsoftware\svc.CMGPI -domain sdmsoftware.net -GPOCreator

- **GPOModify:** Grants the CMGPI service account modify rights over either all GPOs (as shown in the example below) in the specified domain or a list of GPO GUIDs specified using the GPOIDs option.

SetCMGPPermissions.exe -trustee sdmsoftware\svc.CMGPI -domain sdmsoftware.net -All -GPOModify

- **Container:** Grants the CMGPI service account modify permissions rights over the specified container or, when used in conjunction with -Recurse, with the specified container and all child containers.

SetCMGPPermissions.exe -trustee sdmsoftware\svc.CMGPI -domain sdmsoftware.net -Container "OU=Machines,DC=sdmsoftware,DC=net" -Recurse

- **Site:** Grants the CMGPI service account modify permissions rights over the specified AD sites or, when provided with the DN of the parent site object, it will modify all sites' permissions, as shown in the example here:

SetCMGPPermissions.exe -trustee sdmsoftware\svc.CMGPI -domain sdmsoftware.net -Site "CN=Sites,CN=Configuration,DC=sdmsoftware,DC=net"

Appendix B: Customizable User Settings within CMGPI

There are a number of settings that can be configured within CMGPI, that are not exposed through the web application. These settings are typically only adjusted under direction from SDM Software support, or if you need to change the default behavior of CMGPI. The settings can be retrieved and set using two PowerShell cmdlets from the CMGPI PowerShell Module (called SDM-CMGPI). The cmdlets are:

Get-CMSettings

Set-CMSettings

This section describes the available configurable settings and gives their default values:

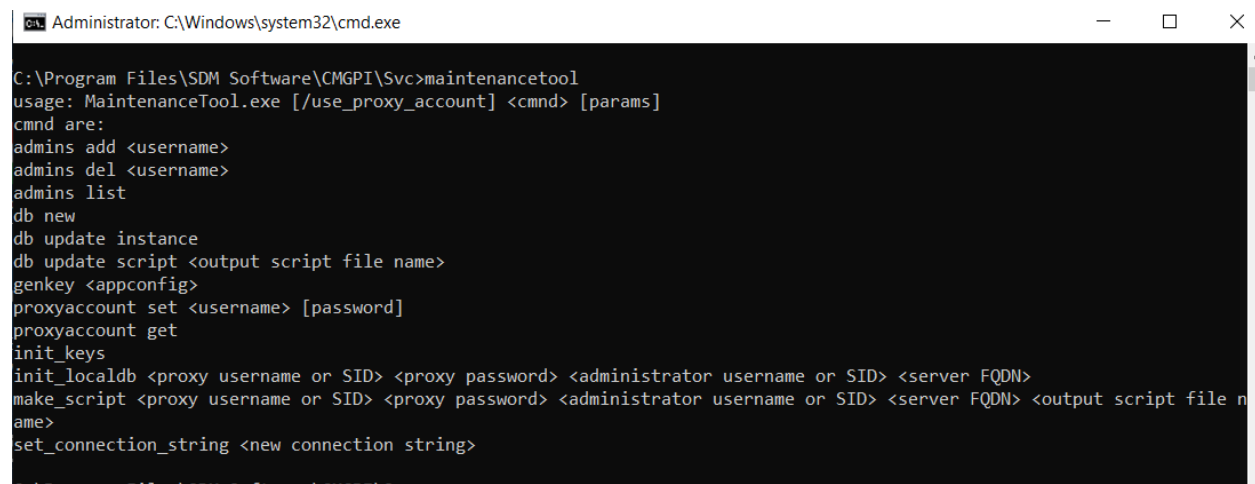
Setting Name	Description	Default Value
DefaultApprovers	Semi-colon separated list of the defined default approvers	Blank (unless set in the UI)
DeployerRoleEnabled	Enables the Deployer role within CMGPI	"False"
FrontendBaseURISettingName	Base URI used in all messages that reference the CMGPI front-end	URI used during setup
OperationsLogQueryLimit	Max count of audit log entries to retrieve	1000
EventsTTLDays	Duration after which CMGPI audit logs will be purged	60
LocksTTLMinutes	Timeout after which any object locked by CMGPI for some operation will be automatically unlocked	5
WaitingActionsTTLHours	Timeout after which pending actions will be purged	24
MassOperationLimitPcs	Mass number of operations such as take/untake control that can be performed at once	20
WasInitialSetupCompleted	Controls whether the Welcome Wizard appears	"True" (until Welcome Wizard appears)
MaxDurationInCheckOutStateMinutes	Timeout after which an object that has been checked out will be flagged and an email reminder will be sent to the editor	1080 (7 days)
MaxDurationInApprovalStateMinutes	Timeout after which an object that has been checked in and waiting for approval	7200 (5 days)

	will be flagged and an email reminder will be sent to the approver	
AutoUploadIntervalMinutes	Interval in between automated support log upload to Azure blob storage	10 (minutes)
RequireEditorComment	Controls whether to require a comment on check-in	"False"
IntuneTagsUpdateIntervalSeconds	Interval for caching Intune Scope Tags	300 (seconds)
ImmutableIdCounterpartAttribute	The AD attribute used to match AD principals with synchronized Entra ID ones	mS-DS-ConsistencyGuid
EMailForUrgementLetters	Email address used for system alerts	
EnableLogsAutoUpload	Enables automated troubleshooting log upload	"False"
LogsBlobSAS_ReadWrite	The Shared Access Signature (SAS) used to upload logs to Azure blob storage	
LogsUploadDir	Local directory to upload logs	
MaxDurationInApprovedStateMinutes	Time to consider a deployment overdue	7200 (5 days)
EmailToForwardEventsToTeams	Used to hold the email address(es) for sending alerts to Teams channel(s)	
EnableGPONameStandards	Determines whether to enforce GPO naming standards	False
GPONameStandardsMask	Regular expression that governs GPO naming standards	

Appendix C: Modifying CMGPI Application Configuration

There are some settings that you might need to modify after installation of CMGPI. Some of these include updating the username or password for the CMGPI service/proxy account, updating the CMGPI database connection string or adding product roles to given users outside of the UI. For these tasks CMGPI includes the command line tool **Maintenancetool.exe**, which is located in %programfile%\sdm software\cmgp\svc

The options for the command are shown here:



```
Administrator: C:\Windows\system32\cmd.exe
C:\Program Files\SDM Software\CMGPI\Svc>maintenancetool
usage: MaintenanceTool.exe [/use_proxy_account] <cmd> [params]
cmd are:
admins add <username>
admins del <username>
admins list
db new
db update instance
db update script <output script file name>
genkey <appconfig>
proxyaccount set <username> [password]
proxyaccount get
init_keys
init_localdb <proxy username or SID> <proxy password> <administrator username or SID> <server FQDN>
make_script <proxy username or SID> <proxy password> <administrator username or SID> <server FQDN> <output script file name>
set_connection_string <new connection string>
```

Here are some examples of usage for the various commands the tool supports:

List current users in the Product Administrator role:

Maintenancetool admins list

Add a user to the Product Administrator role:

Maintenancetool admins add mycompany\joeadmin

Change the CMGPI service account user name and/or password:

Maintenancetool proxyaccount set mycompany\svc_cmgp PasswOrd#!!

Show the current CMGPI Service account:

Maintenancetool proxyaccount get

Retrieve and Change the database connection string to point to a SQL Server instance called SQL1\Apps running on port 50019 where the database name is CMGP:

To retrieve the current database connection string:

Maintenancetool connection db get

Maintenancetool connection db set " Server=SQL1\Apps,50019; Database=CMGP; Integrated Security = SSPI; TrustServerCertificate=True "

Enabling the separation of approver and deployer roles within CMGPI (note that this is a one-time, one-way change. Once enabled, it cannot be disabled):

Maintenancetool deployer_role enable

To retrieve the current state of the deployer role:

Maintenancetool deployer_role check

Appendix D: The CMGPI PowerShell Module

CMGPI provides a separate PowerShell module, which can be installed by using the **CMGPI-PSSetup.exe** installer file that ships in the CMGPI download. The CMGPI PowerShell module provides a set of 85 cmdlets within a module called **SDM-CMGP** that allows you to automate many aspects of CMGPI operation and management.

The most important cmdlet to remember is the **Connect-CMServer** cmdlet. This cmdlet is used to connect to the CMGPI server and must be run before any of the other cmdlets can be used. When running this cmdlet to connect to CMGPI, it must run in the context of a valid CMGPI user, as defined by the Product Roles. The syntax for making a connection is simply:

Connect-CMServer -Server <FQDN of CMGPI Server>

The list below provides a brief description of each of the cmdlets in the Module. Use PowerShell's **get-help** cmdlet for a given CMGPI cmdlet to see a more detailed description of each cmdlet:

Add-CMDomain: Adds a new AD domain to the scope of domains managed by CMGPI

Approve-CMObject: Allows a user in the CMGPI approver role for a given GPO or container (site, domain or OU) to approve an outstanding change

Backup-CMTempGPO: Creates a GPMC backup of a currently checked out GPO. Can only be run by the editor of the GPO.

Compare-CMVersions: Compares two versions of a controlled object in CMGPI. Takes the GUID of a given version to be compared. GUIDs are obtained using the Get-CMHistory cmdlet on the GPO or container in question

Connect-CMServer: Creates an authenticated connection to the CMGPI server—required for all cmdlets to function

Edit-CMContainer: Provides the ability to perform change control actions on AD containers (site, domain or OU) which are under control by CMGPI

Edit-CMEntity: Provides the ability to perform change control actions on Intune Profiles

Edit-CMGPO: Provides the ability to perform change control actions on GPOs which are under control by CMGPI

Find-CMSettingsCatalogSetting: Allows you to search for an implemented Intune Configuration Profile setting within profiles that are under control in CMGPI.

Get-CMAdministrativeContainer: Returns information about all administrative containers

Get-CMAdministrativeContainerMembers: Returns information about the objects that are members of a selected administrative container

Get-CMAllUserContexts Returns username and role of all defined users

Get-CMAssociatedUsers: Returns any users that have a role defined against a given GPO or container

Get-CMAvailableAzureADGroups: Allows you to query Azure AD security groups for matching full or partial name. For use when using groups in assignments for Intune profiles

Get-CMAvailableDCs: Returns the list of available domain controllers for a given AD domain. Must be run by a CMGPI product administrator

Get-CMAvailableGPOSettings: [Internal]

Get-CMAvailableTags: Returns a list of available scope tags currently defined within an Intune tenant

Get-CMBanners: Returns any banner messages currently being displayed in CMGPI. For example, if CMGPI is warning about expiring SSO secrets, this cmdlet would return that message.

Get-CMCollisions: Returns delegation collisions between a container and its members

Get-CMConfiguredGPOSettingsRestrictions: Returns a list of configured restricted policy settings, when those settings are configured in the product.

Get-CMContainer: Gets a list of all container objects, both controlled and uncontrolled, within the forests that have been added to CMGPI

Get-CMContainment: Returns the current delegation on a particular AD container

Get-CMControlled: Returns all GPOs and containers that are under control by CMGPI

Get-CMDelegated: Returns the list of GPOs, containers or Intune Profiles that have been delegated within CMGPI

Get-CMDomain: Returns a list of all AD domains managed by CMGPI

Get-CMDomainDC: Returns the currently selected DC in use by CMGPI for a given AD domain

Get-CMEntityAssignments: Returns the current assignments for an Intune profile that is under control by CMGPI (use Get-CMIntuneEntities to find the DN for a given Intune profile)

Get-CMEntityDescription: Returns the description for an Intune profile that is under control by CMGPI (use Get-CMEntities to find the DN for a given Intune profile)

Get-CMEvents: Retrieves events from the CMGPI audit log

Get-CMGPO: Retrieves all controlled and uncontrolled GPOs along with status information for all domains

Get-CMHistory: Retrieves change history for GPOs and containers managed by CMGPI

Get-CMIntuneEntities: Retrieves a list of all Intune profiles within an Intune tenant

Get-CMIntuneSettings: Retrieves application ID for enterprise application created in Azure AD to connect CMGPI to Intune

Get-CMLicense: Retrieves current license information for the CMGPI product

Get-CMLogs: Retrieves the CMGPI support logs in a binary stream, similar to the “download support bundle” option in the UI. You can use Get-CMLogs | Set-Content 'c:\temp\logs.zip' -Encoding byte to retrieve the logs

Get-CMObject: Returns status information for a GPO or container controlled by CMGPI

Get-CMObjectsStates: Returns the current operational state of a GPO or container

Get-CMRemovedGPOs: Returns the list of GPOs that have been deleted

Get-CMRequestStatistics: [Internal]

Get-CMSettings: Retrieves the value of a configurable setting within CMGPI

Get-CMSMTPSettings: Retrieves the currently set SMTP settings in CMGPI

Get-CMStatistics: Retrieves the dashboard statistics for the current user

Get-CMStored: Retrieves a representation of all controlled and uncontrolled objects from the CMGPI database

Get-CMSystemDelegations: [Internal]

Get-CMUserContext: Retrieves the roles a given user has defined in CMGPI

Get-CMUserPhoto: Retrieves any photo that is associated with a user defined to a role in CMGPI

Get-CMWMIFilters: Retrieves currently defined WMI filters for a selected AD domain. Must be run as a user in the editor role

Grant-CMRole: Lets you assign a user to a particular role in CMGPI

Invoke-CMDeviceManagement: [Internal]

New-CMAdministrativeContainer: Creates a new Administrative Container

New-CMGPO: Creates a new GPO in CMGPI

New-CMSettingInSettingsCatalog: Retrieves Settings Catalog settings that have been implemented within an Intune Configuration Profile.

Publish-CMObject: Performs a Deploy operation of a GPO or container

Register-CMContainer: Takes control over a container (site, domain, OU)

Register-CMGPO: Takes control over a GPO

Register-CMIntuneEntity: Takes control over an Intune profile (use Get-CMEntities to find available profiles)

Register-CMObjects: Allows you to take control of multiple GPOs, containers or Intune Profiles

Remove-CMAdministrativeContainer: Allows you to remove an Administrative Container

Remove-CMDomain: Removes an AD domain that is currently defined within CMGPI

Remove-CMGPO: Creates a GPO Deletion request

Remove-CMGPOSettingRestriction: Allows you to remove a specific restricted policy from the list of configured policies

Rename-CMObject: Allows you to request a GPO rename

Restore-CMDeletedGPO: Allows you to restore a GPO that was previously deleted. Requires Product Administrator role to run

Restore-CMObject: Allows you to rollback a GPO or container object to a prior version

Revoke-CMRole: Revokes or removes a role from a given user

Search-CMContainment: Performs a settings search, based on a search pattern, across GPOs or Intune profiles

Search-CMIdentities: [Internal]

Set-CMAdministrativeContainer: Sets properties on an Administrative Container

Set-CMAdministrativeContainerMembers: Sets new member objects within an existing Administrative Container

Set-CMDomainDC: Sets a given domain controller as the preferred DC for a given domain under control in CMGPI

Set-CMEditorComment: Sets a check-in comment on a GPO or container check-in

Set-CMEntityAssignments: Assigns include/exclude groups/users to a given checked out CMGPI managed Intune profile

Set-CMEntityDescription: Sets the description to a given checked out CMGPI managed Intune profile

Set-CMGPOSettingRestriction: Allows you to define a new restricted policy

Set-CMIntuneSettings: Disables or sets a new application id and secret value for the connection between CMGPI and your Azure AD tenant

Set-CMRoles: Provides an alternate way to set multiple role assignments in CMGPI

Set-CMSettings: Sets configurable options within CMGPI

Set-CMSettingsInSettingsCatalog: [Internal]

Set-CMSMTPSettings: Sets SMTP settings

Set-CMSSOSettings: Initializes single sign on settings (for Azure SSO users)

Set-CMSystemDelegations: [Internal]

Suspend-CMObject: Allows an approver to reject a pending check-in/rollback/deletion

Test-CMAzureAppRegistration: Tests availability of an Intune connection based on supplied parameters. Simulates the Test button in the Settings, Intune UI

Test-CMSetup: Tests whether the first time welcome wizard has been run (you can reset this by setting the WasInitialSetupCompleted value to false in the CMGPI settings—See [Appendix B: Customizable User Settings within CMGPI](#))

Test-CMSMTPSettings: Sends a test email to the configured email sender using existing CMGPI SMTP settings

Unregister-CMContainer: Removes control of a controlled container in CMGPI

Unregister-CMGPO: Removes control of a controlled GPO in CMGPI

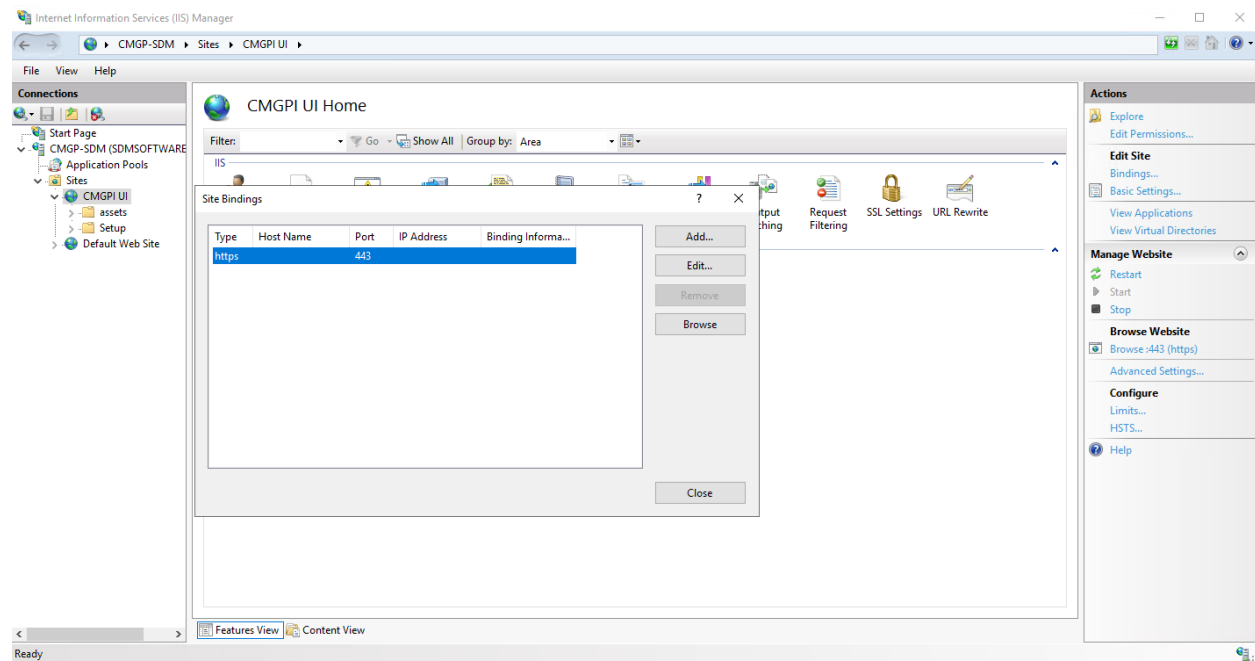
Unregister-CMIntuneEntity: Removes control of a controlled Intune profile in CMGPI

Unregister-CMObjects: Allows for multiple removal of control operations on GPOs, containers or Intune Profiles in a single command

Use-CMLicense: Allows you to activate a CMGPI license

Appendix E: Customizing SSL Certificates and Using Host Aliases

CMGPI ships with a self-signed SSL certificate for the purposes of testing the product. For most customers, you will need to be able to deploy the product with your own certificate. Doing so usually involves assigning your custom certificate with the IIS Administrator tool to the CMGPI web site, as shown here:



Configuring SSL binding for the CMGPI web application

However, CMGPI also has a web service endpoint whose certificate needs to be updated as well. For that reason, we've provided a PowerShell script within the CMGPI download. This script, called **AddressHostname.ps1** (found within the %programfiles%\SDM Software\CMGPI\Svc folder on the CMGP server) provides a way to change the SSL binding of both the front end CMGPI website and the back end CMGPI web service in a single operation. This script should also be used when you are using an alias for the hostname of the CMGP server, since that alias needs to be propagated to CMGPI's configuration. We recommend you use this script when assigning a new certificate. The script should be run on the CMGPI web server in the context of a user with administrative permissions on the CMGPI server and has the following options:

AddressHostname.ps1 -Fqdn <string> -Thumbprint <string> [-CertificateStoreName <string>] [<CommonParameters>]; Simplest form of the command. Use this to change the certificate to the front end and back end, as well as the hostname alias (or simply hostname).

AddressHostname.ps1 -Thumbprint <string> -SetBackendCertificate [<CommonParameters>]; Sets the certificate of the back end only.

AddressHostname.ps1 -Thumbprint <string> -CertificateStoreName <string> -SetFrontendCertificate [<CommonParameters>]; Sets the certificate of the front end only.

AddressHostname.ps1 -GetFrontendFqdn -BackendFqdn <string> [<CommonParameters>]; Retrieves the current FQDN for the front end and back end.

AddressHostname.ps1 -GetBackendFqdn [<CommonParameters>]; Retrieves the FQDN for the back end only.

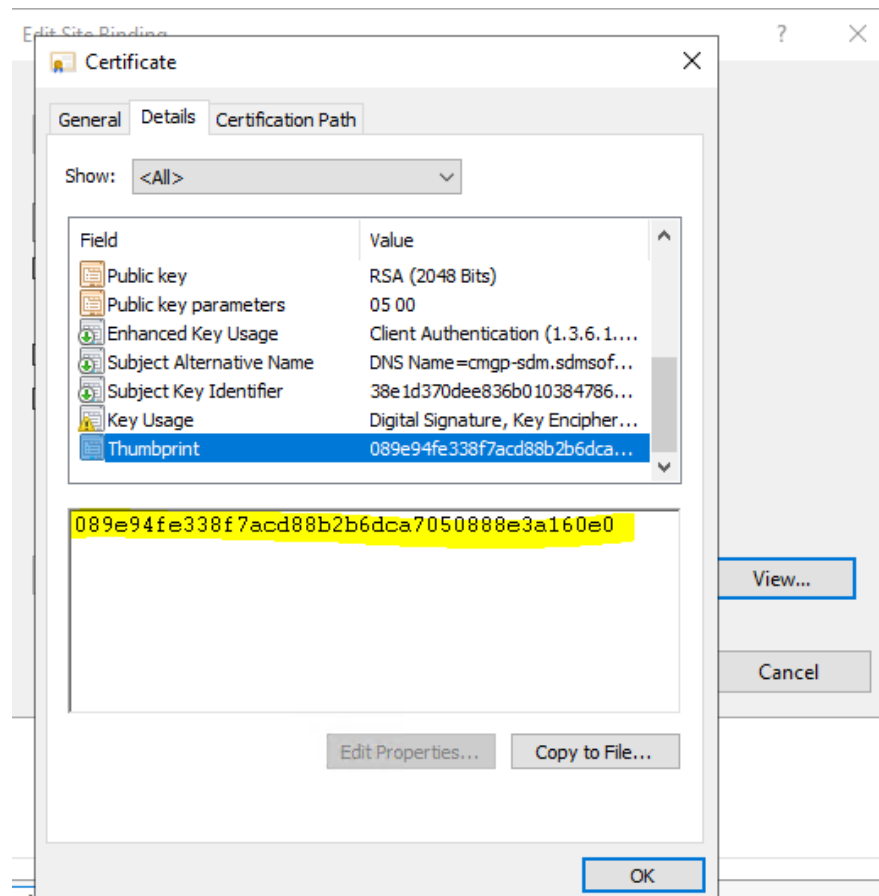
AddressHostname.ps1 -SetFrontendFqdn -BackendFqdn <string> -FrontendFqdn <string> [<CommonParameters>]; Sets just the FQDN for the front end only.

AddressHostname.ps1 -SetBackendFqdn -BackendFqdn <string> [<CommonParameters>]; Sets the FQDN for the back end only.

AddressHostname.ps1 -GetFrontendCertificate [<CommonParameters>]; Retrieves the current front end certificate.

AddressHostname.ps1 -GetBackendCertificate [<CommonParameters>]; Retrieves the current back end certificate.

For commands above that require an SSL thumbprint, the thumbprint you provide is taken from the properties of your SSL certificate. You can see this using a tool like the MMC-based Certificates manager, as shown here:



Here are some examples of using the script in a number of scenarios:

Let's say you want to change the SSL certificate of your CMGPI installation, but not change the hostname. You will need to set the certificate thumbprint for **both** the front end and back end of the CMGP server, as shown in here:

1. Set the certificate for the front end and back end. Hostname alias doesn't change and is CMGP1.mylab.com

```
.\AddressHostname.ps1 -Fqdn cmgp1.mylab.com -Thumbprint  
'DDB44891BAF00C7E8DD072E945FEE837D34C05A8' -CertificateStoreName 'my'
```

2. Set the certificate for the front end and back end. Hostname alias changes to gpomgr.mylab.com

```
.\AddressHostname.ps1 -Fqdn gpomgr.mylab.com -Thumbprint  
'DDB44891BAF00C7E8DD072E945FEE837D34C05A8' -CertificateStoreName 'my'
```

Appendix F: Configuring Intune connectivity from Script

In CMGPI 1.5 we provided a PowerShell script called **ConnectIntune.ps1**, to configure connectivity between CMGPI and your Intune tenant. In version 1.8, that connectivity configuration was moved to the web UI but we still support using the PowerShell script if needed. The difference between performing the configuration in the UI and using the script is that the UI assumes you have already created an application registration in your Entra ID tenant that you will use for Intune connectivity, whereas the script creates the application registration for you. Given that, we've moved the instructions for using the script to this appendix:

Intune Configuration from Script

Prior to logging in the first time, if you plan to use the Intune change control features, you will need to set up the connection to your Intune tenant. CMGPI provides a PowerShell script for this purpose. The script is located in %programfiles%\SDM Software\CMGPI\Svc and is called:

ConnectIntune.ps1

In order to run this script, you'll need the CMGPI PowerShell module installed as well as the following two modules from the Microsoft PowerShell Gallery:

AZ.Accounts

AZ.Resources

You will also need the ability to create an Application Registration within your Azure AD tenant, and the rights to provide Admin Consent to that application. This enterprise application creates the connection between the CMGPI service and a Graph API endpoint within your Azure AD tenant, that allows CMGPI to perform change control tasks within Intune Configuration Profiles. See Intune Change Control Requirements for permissions that are being granted to this application.

You run the script with one parameter, as follows:

.\ConnectIntune.ps1 -CMGPIServerName <fully qualified name of CMGPI server> -TenantID <Tenant Object ID of your Entra ID tenant associated with your Intune account> -AccountID <UPN of the Entra user who has permissions to create a new application registration in your Entra ID tenant>

Once the script runs, it will prompt you to log into Azure AD with an account that can create an enterprise application. Once you complete the Azure AD login, you will see a series of messages in the console as shown here:

```
CMGPI will be connected to mytenant.microsoftonline.com tenant id aa394-7ccd-4a3f-881d-846dbf4f7375
```

```
found CMGPI App Registration with display name 'CMGPI Service' app id is 00a78fb4-1ec3-42fd-e352-81bb1af54eaf object id be057c7c-7d33-48bd-a35b-03deca8a0aa7
```


checking service principal

service principal found id de0bbcb-bb-ae77-45ae-a10d-a1ece3f4c119

setting resources access

opening login window to ask for admin consent

press enter after consents are given:

generated secret 'fd12e`dELpdPcGd3dauysfwdLTZD3czzx0uxkb3N' id 223fde35-a352-4820-b058-4589042b0709 valid from 2023-04-12T00:00:00.0000000Z till 2025-04-11T00:00:00.0000000Z

trying new connection

trying new connection

trying new connection

connected successfully

You will need to click 'Enter' when prompted after agreeing to the Admin Consent window. If you do not click enter, the script will time out. The desired result is that you see the "connected successfully" message after the connection is tried. If you do not get that message, contact SDM Software Support for assistance.

Appendix G: Configuring Entra ID SSO from Script

In CMGPI 1.8 we introduced Single Sign On (SSO) support via Entra ID. As with Intune, you can either configure this support from the CMGPI UI (under Settings, SSO) or using a PowerShell script provided. The difference between performing the configuration in the UI and using the script, is that the UI assumes you have already created an application registration in your Entra ID tenant that you will use for SSO, whereas the script creates the application registration for you. Note that the script creates a secret within the Enterprise Application that is created, and that secret has a lifetime of **2 years**.

SSO Configuration from Script

If you plan to use Entra ID SSO in CMGPI, you will need to set up the connection to your Entra ID tenant. CMGPI provides a PowerShell script for this purpose. The script is located in %programfiles%\SDM Software\CMGPI\Svc and is called:

ConnectEntraID.ps1

In order to run this script, you will need the CMGPI PowerShell module installed as well as the following two modules from the Microsoft PowerShell Gallery:

AZ.Accounts

AZ.Resources

You will also need the ability to create an Enterprise Application within your Azure AD tenant, and the rights to provide Admin Consent to that application. This enterprise application creates the connection between the CMGPI service and a Graph API endpoint within your Azure AD tenant, that allows CMGPI to perform SSO. See Intune Change Control Requirements in the CMGPI 1.8 Installation Guide for permissions that are being granted to this application.

You run the script with one parameter, as follows:

.\ConnectEntraID.ps1 -CMGPIServerName <fully qualified name of CMGPI server> -TenantID <Tenant Object ID of your Entra ID tenant that has the users and groups for SSO> -AccountID <UPN of the Entra user who has permissions to create a new application registration in your Entra ID tenant>

Once the script runs, it will prompt you to log into Azure AD with the account ID that you specified above, that can create an enterprise application. You'll see an Admin Consent prompt appear, which will also require login using your account ID. Once you complete the Azure AD login and consent prompts, you will see a series of messages in the console as shown here:

.\ConnectEntraID.ps1 -CMGPIServerName cmgp1.sdm.lab -TenantID 0c3461d9-74e7-4e08-9159-6e40894d05b3 -AccountID myadmin@mytenant.com

CMGPICommon.ServiceConnection

Please select the account you want to login with.

Retrieving subscriptions for the selection...

[Announcements]

With the new Azure PowerShell login experience, you can select the subscription you want to use more easily. Learn more about it and its configuration at <https://go.microsoft.com/fwlink/?linkid=2271909>.

If you encounter any problem, please open an issue at: <https://aka.ms/azpsissue>

CMGPI will be set to allow users from mytenant.com tenant id 0c3461d9-74e7-4e08-9159-6e40894d05b3

no CMGPI SSO App Registration CMGPI SSO App found. Registering one.

created CMGPI SSO App Registration with app id 7e3f6e46-8ed8-4305-d270-7e8df98d5832 object id 1331ab51-de02-4b70-3df6-fe6a95343e34

setting claims and reply url

opening login window to ask for admin consent

press enter after consents are given:

generated secret 'SDM Software CMGPI 1.8 SSO Secret' 'S9t8Q~WXLVnH75ZiGg9Y~Jl7Vn4Ttv~J6PvOZarp' id 07d9dfa3-a23e-4471-b6c5-53e4ba694407 valid from 2024-06-11T00:00:00Z till 2026-06-11T00:00:00Z

settings have been applied successfully

You will need to click 'Enter' as highlighted above when prompted after agreeing to the Admin Consent window. If you do not click enter, the script will time out. The desired result is that you see the "settings have been applied successfully" message after the connection is tried. If you do not get that message, contact SDM Software Support for assistance.

Appendix H: Configuring Entra ID SSO Manually

If you need to create the SSO configuration required for CMGPI manually, you can do that as well. The following steps describe how you can set up the required application registration from your Entra ID Portal.

1. From the Entra ID portal, go to application registrations and create a new registration for your tenant.

The screenshot shows the 'Register an application' page in the Microsoft Azure portal. The page has a blue header with the 'Microsoft Azure' logo and a search bar. Below the header, the breadcrumb 'Home > App registrations >' is visible. The main heading is 'Register an application'. The form includes a required field for 'Name' with the value 'Test App Reg for CMGPI SSO'. Under 'Supported account types', the first option is selected: 'Accounts in this organizational directory only (SDM Software, Inc. only - Single tenant)'. The 'Redirect URI (optional)' section shows 'Single-page application (SPA)' selected and the URI 'https://ws1.test.local'. At the bottom, there is a link to 'Enterprise applications' and a 'Register' button.

Microsoft Azure

Search resources, services, and docs (G+)

Home > App registrations >

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

Test App Reg for CMGPI SSO ✓

Supported account types
Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (SDM Software, Inc. only - Single tenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Single-page application (SPA) ✓ https://ws1.test.local ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).


By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

2. Add the required permissions to the application.

Request API permissions

[All APIs](#)

 Microsoft Graph
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.


Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Permission	Admin consent required
▼ Directory (1)	
<input checked="" type="checkbox"/> Directory.Read.All ⓘ Read directory data	Yes

Request API permissions

[All APIs](#)

 Microsoft Graph
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Permission	Admin consent required
▼ GroupMember (1)	
<input checked="" type="checkbox"/> GroupMember.Read.All ⓘ Read all group memberships	Yes

3. Grant Admin Consent to the application permissions.

[+ Add a permission](#) ✓ Grant admin consent for SDM Software, Inc.

API / Permissions name	Type	Description	Admin consent requ...	Status
▼ Microsoft Graph (3)				
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for SDM So...
GroupMember.Read.All	Application	Read all group memberships	Yes	⚠ Not granted for SDM So...
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

4. Add the security group claims for the application under Token Configuration.

The screenshot shows the Microsoft Azure portal interface for configuring an application. The left sidebar contains navigation links for Overview, Quickstart, Integration assistant, Manage (Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest), and Support + Troubleshooting. The main area displays the 'Test App Reg for CMGPI SSO' application configuration. The 'Token configuration' tab is active, showing 'Optional claims' and a table for 'Claim' and 'Description'. The right pane, 'Edit groups claim', is open, showing options to select group types (Security groups, Directory roles, All groups) and customize token properties by type (ID, Access, SAML). Under SAML, 'Group ID' is selected.

...so it looks like the following

This screenshot is identical to the one above, showing the Microsoft Azure portal interface for configuring an application. The left sidebar contains navigation links for Overview, Quickstart, Integration assistant, Manage (Branding & properties, Authentication, Certificates & secrets, Token configuration, API permissions, Expose an API, App roles, Owners, Roles and administrators, Manifest), and Support + Troubleshooting. The main area displays the 'Test App Reg for CMGPI SSO' application configuration. The 'Token configuration' tab is active, showing 'Optional claims' and a table for 'Claim' and 'Description'. The right pane, 'Edit groups claim', is open, showing options to select group types (Security groups, Directory roles, All groups) and customize token properties by type (ID, Access, SAML). Under SAML, 'Group ID' is selected.

5. Generate a new secret for CMGPI service access. You can choose any duration. Just be aware you will need to update the secret in CMGPI's configuration when it expires.

[Reg for CMGPI SSO](#)
MGPI SSO | Certificates & secrets

Got feedback?

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) **Client secrets (0)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value	Secret ID
No client secrets have been created for this application.			

Add a client secret

Description

Enter a description for this client secret

Expires

Recommended: 180 days (6 months)

Once this is done, you'll need to copy the secret ID and value and enter it, along with other details, into CMGPI's configuration. This is done as a Product Administrator from the Settings, SSO page, as described in the **CMGPI Installation Guide**.

Appendix I: Supported types of Intune Configuration Profiles

CMGPI supports a subset of the total available Intune configuration profile types. The list of supported profile types is provided here:

- Administrative templates
- Settings Catalogs
- Shell scripts
- Custom attributes
- PowerShell scripts

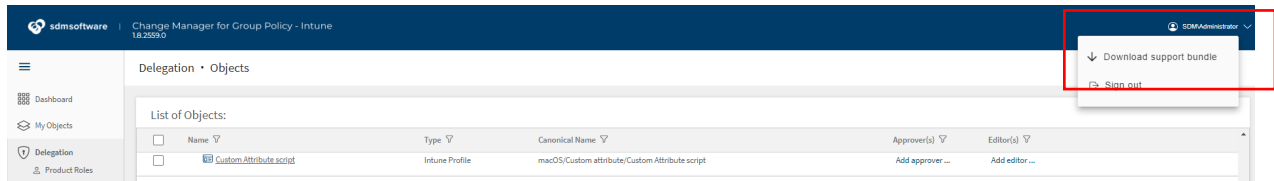
In addition, the following template types are supported:

- 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

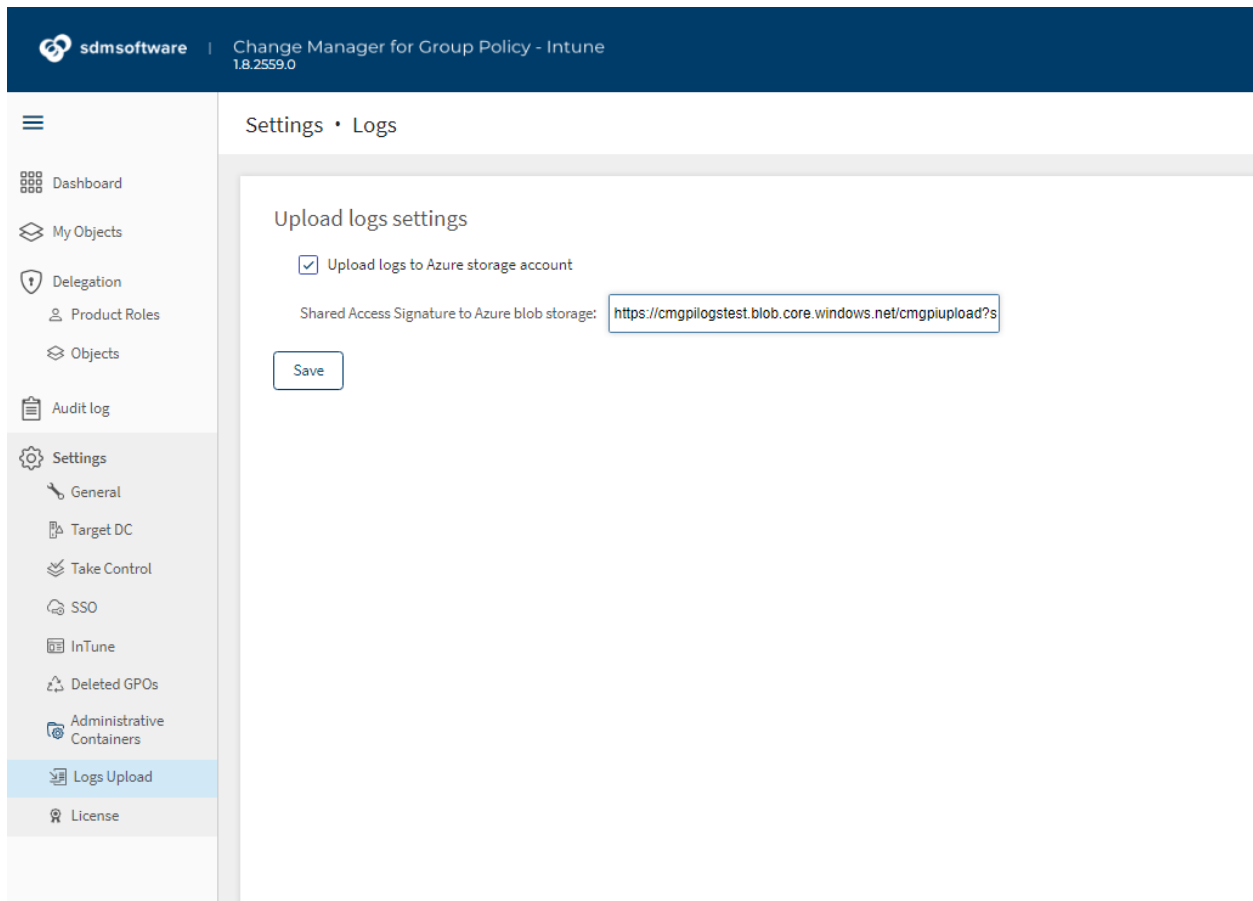
Appendix J: Troubleshooting and Logging

The 1.8 release of CMGPI added the ability to collect logs from the product in the event that you need to report a support issue to SDM Software Support. There are two ways that logs can be collected: The first and simplest way is, when you encounter an issue, select your username from the upper right frame of the application in the browser, to expose the “Download Support Bundle” option, as shown here:



When you select this option, a new browser tab opens up to download the logs and, depending on your browser configuration, a new file called **logs.zip** will be saved to your Downloads folder in the local machine’s file system.

The other option provided for log collection is accessible as a Product Administrator. This option, found on the menu under **Settings, Logs Upload**, allows you to continuously upload logs to an Azure blob storage account, as shown here:



The logs are uploaded to your Azure blob storage account every 10 minutes by default. This can be modified by changing the `AutoUploadIntervalMinutes` setting in CMGPI’s configuration (see [Appendix B](#):

[Customizable User Settings within CMGPI](#) for more information). This kind of continuous upload means you always have a history of activity within CMGPI in case there is an issue. You can give read access to the Azure blob container to SDM Software Support, if you want to use this approach.

The log upload screen in CMGPI expects a Shared Access Signature (SAS) from your Azure Storage Account when you enable it. Simply create a Container in your Azure blob storage account. Using the **Azure Storage Explorer** tool from Microsoft is an easy way to accomplish this. From Azure Storage Explorer you can create the container AND the Shared Access Signature key by right clicking the container you created and choosing “Get Shared Access Signature” from the properties menu.

Ensure that when you create the SAS, you grant all rights to the container for CMGPI to successfully write the logs, as shown here:

Shared Access Signature

Signing key: Account key 'key1'

Access policy: none

Start time: 06/17/2024 05:19 PM

Expiry time: 06/18/2024 05:19 PM

Time zone: ☒ Local ☐ UTC

Permissions:

<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Add	<input checked="" type="checkbox"/> Create	<input checked="" type="checkbox"/> Write
<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Delete version	<input checked="" type="checkbox"/> List	<input checked="" type="checkbox"/> Tag
<input checked="" type="checkbox"/> Find			

Optional parameters:

IP address range: e.g. '168.1.5.165' or '168.1.5.165-168.1.5.170'

Version: e.g. 2021-10-04

API version: e.g. 2021-10-04

Encryption scope:

☐ Allow HTTP (not recommended)

[Learn more about shared access signatures](#)

Create Cancel

When you click the **Create** button here, you’ll see two keys show up. One will say “URL” and the other will say “SAS Token.” Copy and paste the “URL” field into the CMGPI log configuration screen.

Appendix K: Configuring Connectivity to Other Azure Clouds

The default configuration of CMGPI is designed to work against the main Azure endpoints used by most organizations. However, some organizations may use other Azure clouds maintained by Microsoft (e.g. Azure for U.S. Government), and CMGPI can support these alternative endpoints.

Within the %programfiles%\sdm software\cmgpi\svc folder on the CMGPI server is a file called CMGPISvc.exe.config. Within the file are three keys that can be changed to reflect the correct Azure endpoints for the desired Azure environments, as shown here:

```
<add key="CloudInstance" value="login.microsoftonline.com" />
<add key="GraphRoot" value="graph.microsoft.com" />
<add key="GraphSchemeUri" value="https://graph.microsoft.com/beta/$metadata" />
```

Contact SDM Software Support for help with editing these endpoints.