



SDM Software Change Manager for Group Policy/Intune®

Version 1.5

Installation & User Guide

Revisions:

Document Version 1.2.....May 19, 2023

Document Version 1.1.....May 16, 2023

Contents

Overview	4
CMGPI Architecture Overview	4
CMGPI Components	4
Installation Requirements	5
Hardware	5
Software	5
Configuration/Security Rights Required	6
Group Policy Change Control Requirements	6
Intune Change Control Requirements	6
Installation	7
SQL Server Configuration	12
Initial Configuration	12
Intune Configuration	12
Taking Control of GPOs	17
The Take Control Process for GPOs	17
The Take Control Process for AD Containers	20
The Take Control Process for Intune Profiles	22
Delegate Access	23
Editor and Approver Capabilities	23
Settings	25
Using the Product	27
Product Roles	27
Product Administrator	27
GPO Creator	27
Break Glass	28
Auditor	28
CMGPI Dashboard	28
CMGPI Navigation	29
The Change Control Process	31

Editing GPOs.....	32
Editing Containers.....	42
Preparing to edit Intune Profiles.....	44
Editing Intune Profiles.....	45
Approving and Deploying Intune Profiles	50
Audit Log	50
Licensing.....	51
Appendix A: Using the SetCMGPPermissions.exe to grant initial permissions required by CMGPI.....	53
Appendix B: Customizable User Settings within CMGPI	55
Appendix C: Modifying CMGPI Application Configuration	57
Appendix D: The CMGPI PowerShell Module	58
Appendix E: Customizing SSL Certificates and Using Host Aliases.....	61

Overview

SDM Software's Change Manager for Group Policy/Intune® (CMGPI) brings modern Group Policy and Intune® change management processes to all 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. CMGPI can be installed and made functional within minutes of downloading. 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.

CMGPI Architecture Overview

Before we can discuss installation requirements, it's important to look at the components that make up the CMGPI installation. These are shown in Figure 1: the CMGPI Architecture, below:

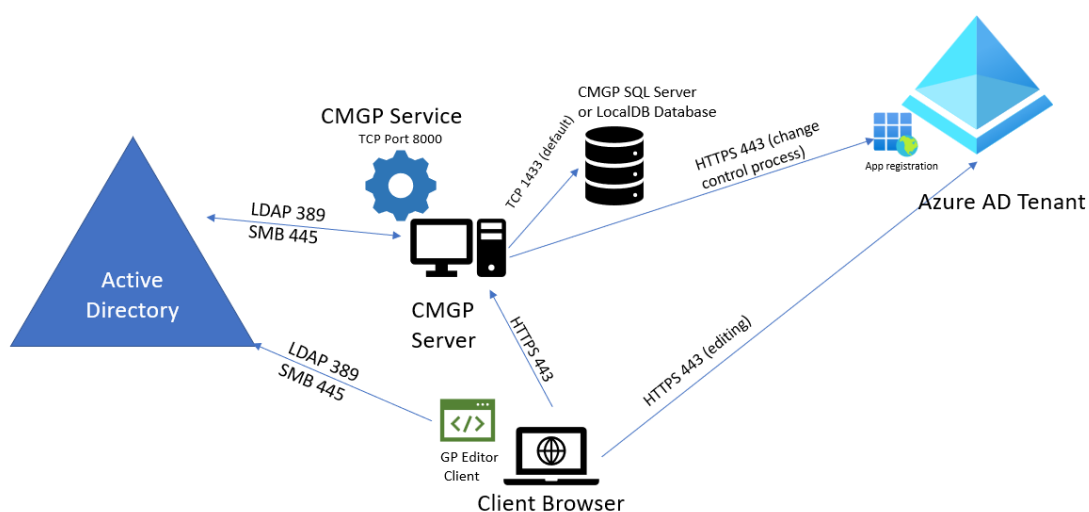


Figure 1: the CMGPI Architecture

CMGPI Components

The following is a description of the components described in Figure 1 above:

- **CMGPI Server:** The main application server for CMGPI, which is composed of the CMGPI web application, running on IIS and the **CMGPI Service**, running as a Windows service.
- **CMGPI Database:** This is the database store for CMGPI. It can be co-located on the CMGPI Server, as would be the case if you choose the LocalDB installation option, or on a separate, shared or standalone Microsoft SQL Server instance.
- **Client Browser:** CMGPI is a web-based app, supporting either **Chrome** or Microsoft **Edge** browsers. In order to edit GPOs, you will need to be able to launch the **GP Editor Client**. The

client requires you to be on a domain-joined machine within a trusting domain under management by CMGPI and needs to have the Microsoft Group Policy Management Console (GPMC) installed.

Installation Requirements

The CMGPI installer provides a signed .msi file that will install aspects of the CMGPI architecture needed for the CMGPI server and database, as shown in Figure 1. There are several hardware, software and security configuration requirements for a successful CMGPI installation. These are listed here:

Hardware

- Virtual or Physical Server supported
- Minimum 100MB of available disk space
- Minimum 100MB of available RAM
- Recommend at least 2 CPU/vCPU for CMGPI application server (more vCPU and memory allows for more concurrent users)

Software

- Windows Server 2012-R2, 2016, 2019 or 2022 required (CMGPI should not be installed on a Domain Controller)
- .Net Framework 4.7.2 or greater
- Microsoft Group Policy Management Console (GPMC) feature installed (both on Management Server as well as any machine that will be performing GPO editing)
- SQL Server 2017 Standard Edition or greater (or SQL Server 2017 LocalDB, included in Installer)
- Chrome or Edge supported as Client Browser

In addition, the following pre-requisite components are installed by the CMGPI MSI Installer during installation time:

- SQL Server 2017 LocalDB (if that option is chosen)
- Microsoft OLE DB Driver for SQL Server (note that if you have an existing, older version of this software installed, it will be upgraded during the CMGPI installation)
- Microsoft IIS URL Rewrite Module 2
- Microsoft Application Request Routing 3.0

When installing and configuring Microsoft Intune support, CMGPI requires the following components also be installed:

- The CMGPI PowerShell module (separate installer)
- The PowerShell modules **Az.Accounts** and **Az.Resources**, available from the Microsoft PowerShell Gallery using the “install-module” cmdlet

Configuration/Security Rights Required

Group Policy Change Control Requirements

- Service account for the CMGPI application server. Service account can be either a regular AD user account or a group Managed Service Account (gMSA). The **service account must have local administrator rights (i.e. a member of the local Administrators group) on the CMGPI server.**
- The CMGPI service account requires “Modify Permission” rights on any GPOs or containers it will be taking control of. In addition, the service account should be made a member of Group Policy Creator Owners group OR be granted create GPO rights on any domain under management using GPMC. (See Appendix A for a description of the command-line tool **SetCMGPPermissions.exe** which can be used to grant the service account the required permissions in preparation for using CMGPI.) Here is the summary of permissions required in AD by the CMGPI service account:
 - For GPOs to be taken under control: **Edit settings, delete and modify security** rights within GPMC and **GPO creation** rights on any domain under CMGPI management
 - For containers (AD sites, domain objects or OUs) to be taken under control: **Modify permissions** rights over those containers
- If SQL Server is used, the CMGPI service account requires read and write access (db_datareader and db_datawriter roles) to the CMGPI database.

Note: If you are upgrading from a prior version of CMGP and have deployed full SQL Server, you will need to provide the CMGP service account with the db_DDLAdmin role for the upgrade or run maintenancetool.exe as a user who has that role.)

- Any user who will be editing GPOs from the CMGPI GP Editor client will require local administrative permissions on the client where the editing occurs, unless User Account Control (UAC) is not configured on that system or the GP Editor client has been excluded from elevation restrictions.

Intune Change Control Requirements

- If using the Intune change control features, you will need to provide an account that can create an enterprise application object, and also provide admin consent for the rights needed by that application. The following Graph API rights are required for the Intune Change Control features:
 - DeviceManagementConfiguration.Read.All
 - DeviceManagementConfiguration.ReadWrite.All
 - DeviceManagementRBAC.Read.All
 - DeviceManagementRBAC.ReadWrite.All
 - Directory.Read.All
 - GroupMember.Read.All
 - User.Read
- In addition, CMGPI will need you to create a “CMGPI Editors” security group in your Azure AD tenant and you will need to have permissions to populate that group with members.

Installation

The CMGPI installer is a signed MSI file that should be extracted from the .zip file and copied to the server where you plan to install the product.

Ensure that you are logged in to Windows with domain-based credentials that have local administrative access on the CMGPI server.

When you run the installer, the first step is to install prerequisites. Figure 2 shows the screen you get when the installer first runs:

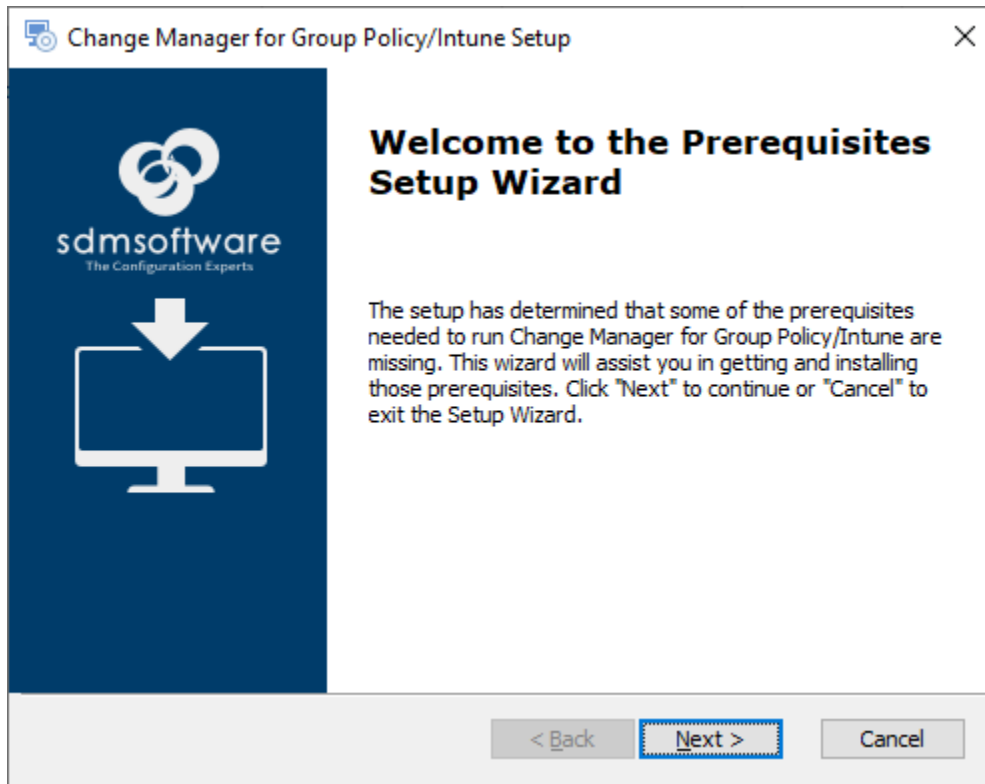


Figure 2

This only appears if you are indeed missing prerequisites that are required for CMGPI to run.

When you press the Next button, the dialog asks if you wish to install SQL Server 2017 LocalDB (Figure 3). You would only choose this option if you are **NOT** planning to deploy full SQL Server to support your CMGPI installation. This would be the case for small environments, or if you are just evaluating CMGPI.

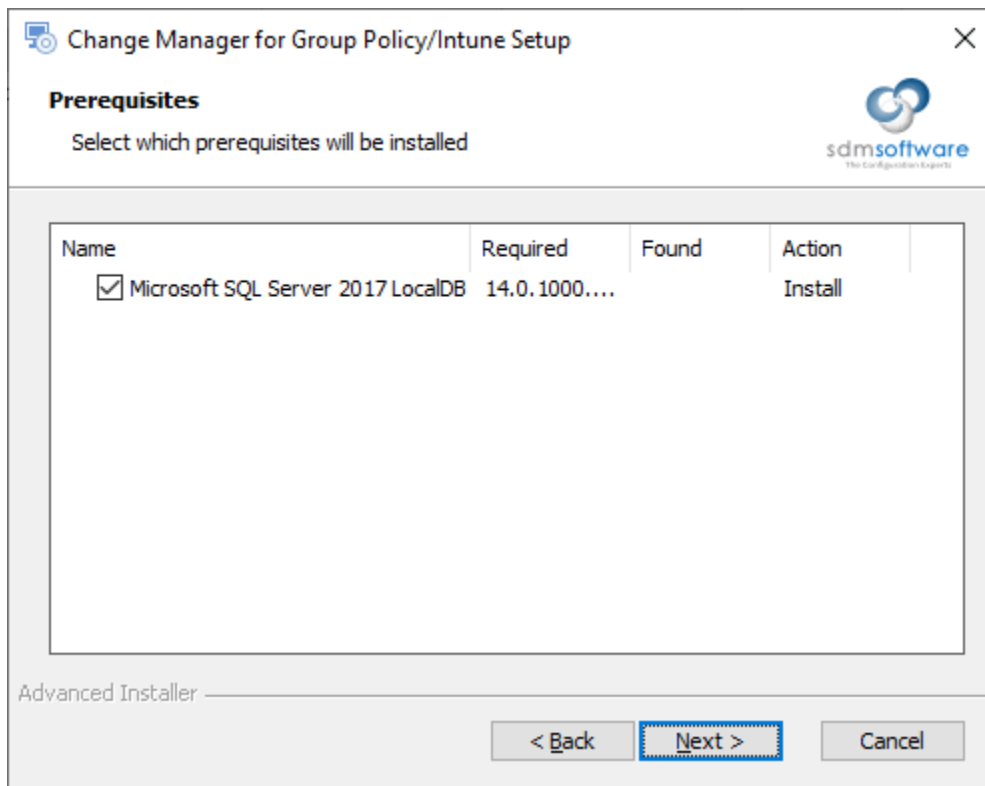


Figure 3

If you select to install LocalDB, a separate installer will launch for that software, and you will need to answer the prompts to complete its installation. This is a Microsoft provided installer, and not part of the CMGPI installation.

Once the LocalDB installation completes, the CMGPI installer will continue. Press Next to accept the EULA. You will then need to provide the username and password of the CMGPI service account, previously created, to be used with the product, as shown in Figure 4.

Change Manager for Group Policy/Intune Setup

Logon Information
Specify user account information

sdmsoftware
The Configuration Experts

User Name:
east\svc_cmgp

Password:
●●●●●●●●●●

Advanced Installer

< Back Next > Cancel

Figure 4

NOTE: If you are using a group Managed Service Account (gMSA) leave the password field blank here.

After entering the service account information, the installer will attempt to validate the account and password with AD. If it's unable to do that (e.g. the account doesn't exist or password is incorrect), the process will prompt you and you will need to correct the account before proceeding.

Once the account is validated, you'll be asked to confirm the installation location, and on the following screen, you'll need to choose whether you plan to use the SQL Server LocalDB instance on the server you're installing on or using a SQL Server installation separate from the CMGPI installer, as shown in Figure 5.

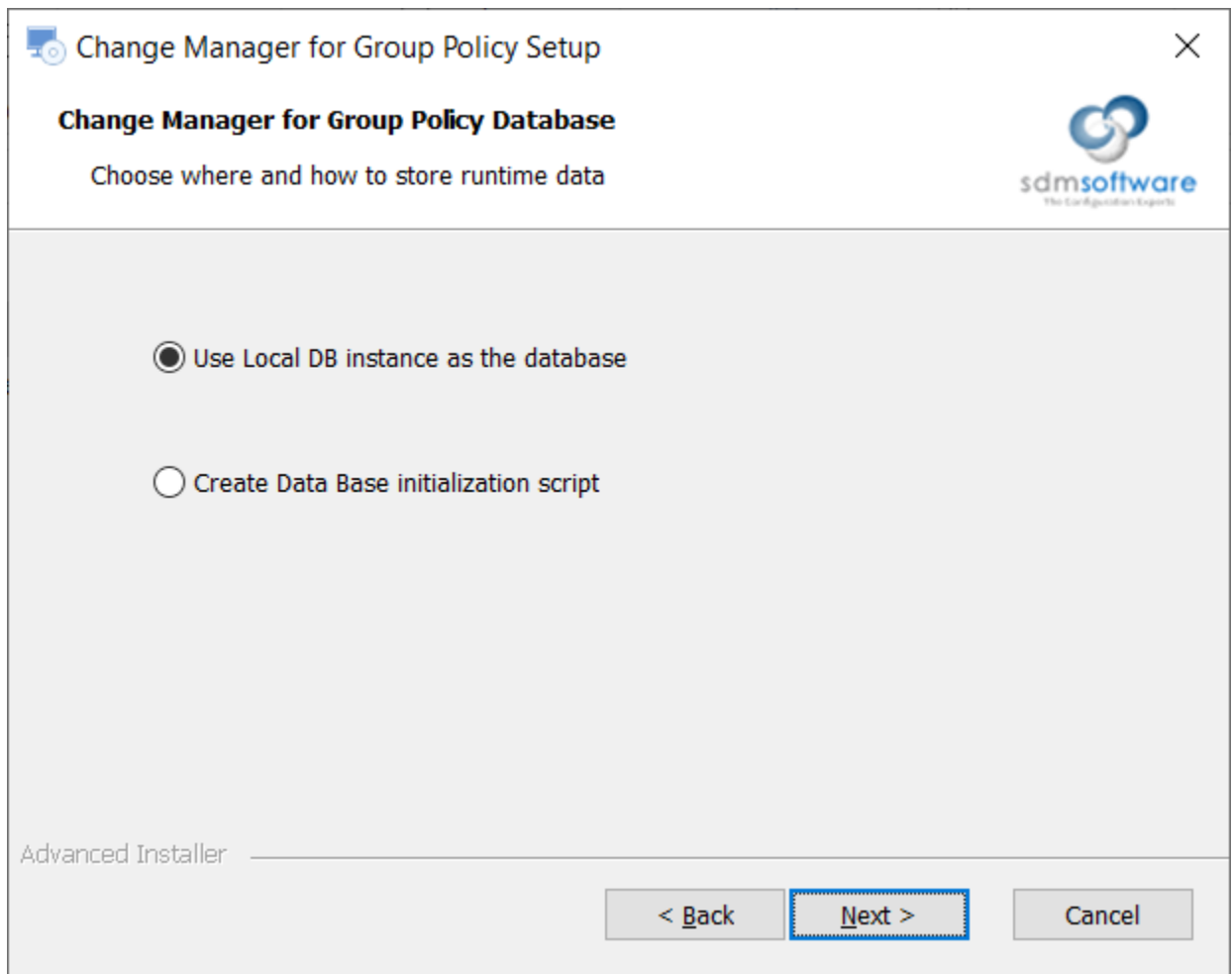


Figure 5

The first option will tell the installer to use the LocalDB instance that was installed earlier in the process. The second option will create a SQL script that will open at the end of the CMGPI installer process, that you can use within Microsoft SQL Server Management Studio to create the CMGPI database. If you choose this option, you'll be asked on the next screen to enter the server and instance name and port for your SQL Server, as shown in Figure 6:

Change Manager for Group Policy Setup

Configure SQL Server connection

Please enter information to connect SQL Server

sdmsoftware
The Configuration Experts

SQL Server Instance:

Port:

Advanced Installer

< Back Next > Cancel

Figure 6

If you are not using a named instance for your SQL Server, just enter the fully qualified domain name of the SQL Server (e.g. SQLServer1.mycompany.com). If you do have a named instance that you are using, enter the fully qualified domain name followed by the instance name in the format of SQLServer1.mycompany.com\InstanceName.

NOTE: If you choose the full SQL Server installation option, you will need to manually start the SDM Software CMGPI Service from the services control panel applet after the CMGPI installer completes.

Once your database choice is specified, the installer will then launch the setup for the OLE DB Driver for SQL Server, which is a required Microsoft component. If the component is already installed on this system, its version will be verified and if it's older than the version the installer needs, it will be updated.

The installer will then complete the remainder of the installation, which includes adding required Windows Features and configuring IIS for the web application.

NOTE: The CMGPI installer installed a self-signed SSL certificate that is used to protect the CMGPI web application, by default. You can use IIS to configure your own trusted SSL cert after the installation is completed.

At the end of the installation process a final dependent component—The Microsoft URL Rewrite Module—will be installed as a final step of the installer. Once that completes the CMGPI Installer will complete.

Once the installation is complete, you should see a web shortcut added to the desktop to allow you to launch the browser, directed at the CMGPI application.

Note also that if you chose to use the full SQL Server setup option, the SQL script will open in Notepad for you to copy/paste to your database. In addition, the script itself is stored on the desktop of the installed server in case you need to retrieve it. If you close Notepad, the CMGPI installer will end, but while Notepad is open, the installer will stay open as well.

SQL Server Configuration

If you run the SQL Server creation script, the database created in SQL Server will be called **CMGPI** and will grant your service account a login to the CMGPI database with db_datareader and db_datawriter permissions on the database itself.

NOTE: After completing the database creation, it's important to ensure that you **start** the service on the CMGPI server called "**SDM Software CMGPI Service.**"

Initial Configuration

After installation, you'll need to log in to the CMGPI web user interface to configure the product. But before doing that, if you plan to use Intune support, follow the directions below:

Intune Configuration

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 will need the CMGP 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 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>

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
```

NOTE: You will need to press 'Enter' when prompted after agreeing to the Admin Consent window. If you do not press 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.

To log into the product, double-click the “SDM Software Change Manager for Group Policy/Intune” web shortcut that was installed on the CMGPI server desktop, to launch a browser target at CMGPI. Or, from a default installation, browsing to <https://<CMGPI Server Name>> should launch the application.

NOTE: CMGPI has been tested with Chrome and Microsoft Edge browsers. Internet Explorer is NOT supported by the application.

From the login screen, **you’ll need to log in using the user account that you used to install the product**, which should be a domain-based account. This account will automatically be granted access to configure the CMGPI product during the installation process. You’ll need to log in using domain-based credentials in the form of <domain\username> as shown in Figure 7 below. You can also press the “Sign in with Windows Authentication” button to use Integrated Windows Authentication (IWA) to log into the portal. In that case, the first time you log in with IWA you will see a pop-up prompt to enter your domain credentials.



Change Manager for Group Policy - Intune

Domain\user name

Password

Sign in


 Sign in with Windows Authentication

Figure 7

After logging in the first time, you will be presented with the Welcome Wizard, as shown in Figure 8:

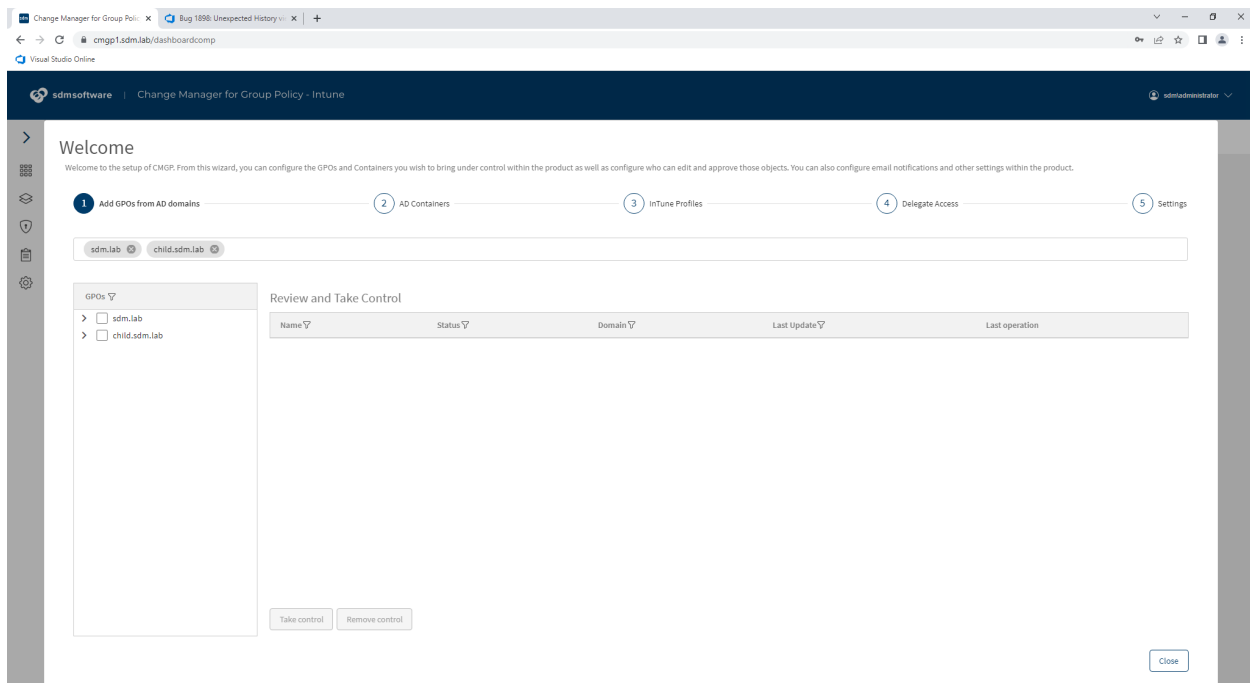


Figure 8: The CMGPI Welcome Wizard

The wizard provides you with a way of setting up the initial product configuration. There are five sections to the wizard:

- **Add GPOs from AD Domains:** Allows you to take control of GPOs to be placed into change control within CMGPI
- **AD Containers:** Allows you to take control of AD containers (sites, domain, or Organizational Units (OUs)) to be placed into change control within CMGPI
- **Intune Profiles:** Allows you to take control of Intune Profiles. Note that the ConnectIntune.ps1 scripts needs to have been run prior to using this wizard, or available Intune profiles will not appear here
- **Delegate Access:** Allows you to assign “editors” and “approvers” within CMGPI for the objects you just took control of in the prior steps
- **Settings:** Allows you to configure general product settings such as the default approvers group, SMTP settings, etc.

It’s important to note that in order to take control of GPOs, or containers, you must have first granted access to these objects natively within GPMC and AD Users and Computers. You can either use the Maintenance Tool utility that comes with CMGPI (see [Appendix A: Using the SetCMGPPermissions.exe to grant initial permissions required by CMGPI](#)) or, if you don’t need to use a least privileged approach, you can place the CMGPI service account into a privileged group such as Domain Admins. This is less desirable of course, because such highly privileged groups should be left to “Tier 0” applications, but this can be done if required.

For Intune Configuration Profiles, you don’t need to do anything special to take control of available profiles. All available configuration profiles will be displayed in the wizard once connection to Intune is made.

Let's walk through each step of the wizard:

Taking Control of GPOs

In order to take control of one or more GPOs, you first have to enter the domain(s) you wish to manage within CMGPI. In the text box below step 1, enter the DNS name of any domain you wish to manage using CMGPI. After entering the first name, press the Enter key to accept the domain and then you can type in additional domain names. Note that you will need to explicitly add domains from a multi-domain forest. They are not added automatically, as is shown in Figure 9 below:

Welcome

Welcome to the setup of CMGP. From this wizard, you can configure the GPOs and Containers you wish to bring under control within the product as well as configure who can edit and approve those objects. You can also configure email notifications and other settings within the product.

1 Add GPOs from AD domains 2 AD Containers 3 Delegate Access 4 Settings

sdmsoftware.net child.sdmsoftware.net

GPOs ▾

- ☐ sdmsoftware.net
 - ☐ Americas Computer Security Policy
 - ☐ Americas Desktop Security Policy
 - ☐ Americas Drive Mapping Policy
 - ☐ Americas User Lockdown Policy
 - ☐ Client Desktop Policy
 - ☐ Client General Policy
 - ☐ Consolidated2-10
 - ☐ ConsolidatedTest

Review and Take Control

Name ▾	Status ▾	Domain ▾	Last Update ▾	Last operation
--------	----------	----------	---------------	----------------

Take control Remove control

Close

Figure 9 Adding domains to manage in CMGPI

Once you add a domain, the product will automatically retrieve all available GPOs within the domain selected and they will populate under the domain name in the tree view, as shown above. Note that if you need to search for particular GPOs, the filter (🔍) icon allows you to filter GPOs by full or partial name.

From the tree view of GPO names, select the GPOs you wish to take under control. Let's first explore what it means to "take control" of a GPO.

The Take Control Process for GPOs

The process of taking control of a GPO in CMGPI is a mechanism by which the permissions of that GPO are altered by the CMGPI service account, to prevent any **regular, non-privileged user** other than the service account from being able to edit, delete or modify permissions on the GPO. The take control process DOES NOT remove default privileged account access to GPOs. This includes:

1. **Domain Admins**
2. **Enterprise Admins**

3. Local System

These three Access Control Entries (ACEs) will remain after a Take Control operation is performed. However, if a “discretionary” user principal was added to the GPO’s delegation that grants either “Edit Settings” or “Edit Settings, Delete, Modify Security” permissions on that GPO, that user principal’s access will be changed to “Read” by the Take Control process. As an example, the following GPO has native delegation prior to the Take Control Operation:

Client General Policy		
Scope	Details	Settings
Delegation	Status	
These groups and users have the specified permission for this GPO		
Groups and users:		
Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (SDMSOFTWARE\Domain Admins)	Edit settings, delete, modify security	No
Enterprise Admins (SDMSOFTWARE\Enterprise Admins)	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
GPO Admins (SDMSOFTWARE\GPO Admins)	Edit settings, delete, modify security	No
Roman Bardet (rbardet@sdmssoftware.net)	Edit settings	No
svc cmgp (svc.cmgp@sdmssoftware.net)	Edit settings, delete, modify security	No
SYSTEM	Edit settings, delete, modify security	No

Figure 10 Native permissions prior to Take Control operation

Note that in Figure 10, the group GPO Admins has full control over the GPO and the user RBardet has “Edit Settings” permissions on the GPO. Also note that the CMGPI service account, in this example called svc.CMGPI, has full control over the GPO by virtue of the **SetCMGPPermissions.exe** being run against all GPOs.

Once I take control of this GPO, notice the change in permissions that occurs on the GPO in Figure 11 below:

Client General Policy		
Scope	Details	Settings
Delegation	Status	
These groups and users have the specified permission for this GPO		
Groups and users:		
Name	Allowed Permissions	Inherited
Authenticated Users	Read (from Security Filtering)	No
Domain Admins (SDMSOFTWARE\Domain Admins)	Edit settings, delete, modify security	No
Enterprise Admins (SDMSOFTWARE\Enterprise Admins)	Edit settings, delete, modify security	No
ENTERPRISE DOMAIN CONTROLLERS	Read	No
GPO Admins (SDMSOFTWARE\GPO Admins)	Read	No
Roman Bardet (rbardet@sdmsoftware.net)	Read	No
svc cmgp (svc.cmgp@sdmsoftware.net)	Edit settings, delete, modify security	No
SYSTEM	Edit settings, delete, modify security	No

Figure 11 Native permissions on the GPO after the Take Control operation

The two discretionary ACEs—for GPO Admins and RBardet—have been modified to Read-only access. These users/groups will now no longer be able to edit this GPO outside of CMGPI.

To perform the take control operation, select the GPOs you wish to take control of (or check the box at the domain level to select all GPOs). Once a GPO is selected, it appears in the Review and Take Control list. Press the Take Control button to perform the operation. A counter will appear at the top of the list to show progress, as shown in Figure 12:

Welcome

1 Add GPOs from AD domains

2 AD Containers

3 Delegate Access

4 Settings

sdmsoftware.net

Type domain name

GPOs

sdmsoftware.net

Americas Computer Security Policy

Americas Desktop Security Policy

Americas Drive Mapping Policy

Americas User Lockdown Policy

Client Desktop Policy

Client General Policy

Consolidated2-10

ConsolidatedTest

ConsolidatedTest2

Default Domain Controllers Policy

Default Domain Policy

Desktop Security Settings

Domain General Security Policy

Domain Policy Test

Domain-wide Security Settings

Review and Take Control

Operation in progress. 6 of 7 objects completed

Name	Status	Domain	Last Update	Last operation
Americas Computer Security Policy	Controlled	sdmsoftware.net		Success
Americas Desktop Security Policy	Controlled	sdmsoftware.net		Success
Americas Drive Mapping Policy	Controlled	sdmsoftware.net		Success
Americas User Lockdown Policy	Controlled	sdmsoftware.net		Success
Default Domain Controllers Policy	Controlled	sdmsoftware.net		Success
Default Domain Policy		sdmsoftware.net		
Client Desktop Policy	Controlled	sdmsoftware.net		Success
Client General Policy	Controlled	sdmsoftware.net		Success

Take control

Remove control

Close

Figure 12 Taking control of GPOs

SDM Software Change Manager for Group Policy/Intune® Installation & User Guide

Page | 19

Any errors that appear will be shown as “Failed” in the Last Operation column. You can click on the error to see more details of the problem. Next, let’s look at taking control of AD Containers.

The Take Control Process for AD Containers

There are two parts to managing change within Group Policy. The first part is managing the change to the GPO itself. The second part is managing the linking/unlinking/changing of links to containers where GPOs can be linked. By containers, we mean an **AD site**, the **domain object** in a given domain, or an **Organizational Unit (OU)**. When you have completed taking control of GPOs, select the “Step 2 AD Containers” option in the Welcome Wizard, as shown below:

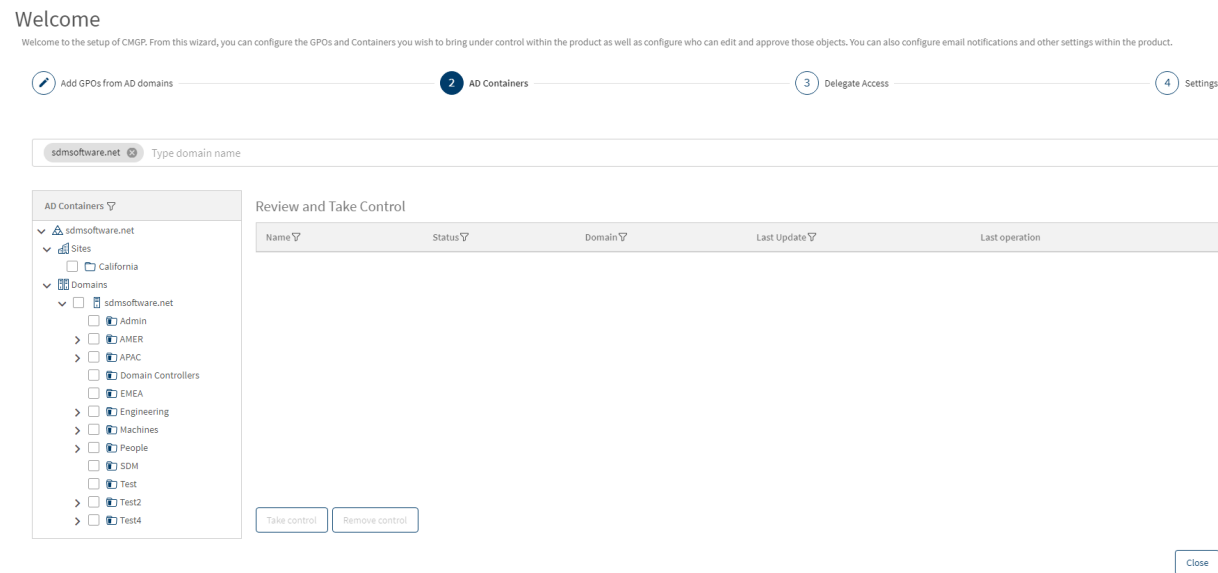


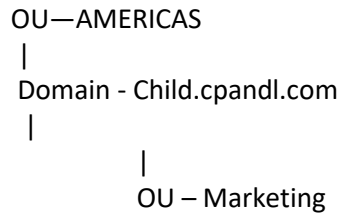
Figure 13 Selecting AD Containers to Take Control of

On the left-hand pane, you will notice a tree structure for the forest that you selected in the prior step. If you expand the tree from the top-level forest-name node, you will see two sub-trees—one for AD sites and one for domains, as shown in Figure 13 above.

If you have child domains added in Step 1, above, then those child domains will appear as sub-nodes to the root domain. For example, if I am managing two domains—cpandl.com and child.cpandl.com, then child will be shown as follows:

Cpandl.com

|



Select Sites, Domains and OUs that you wish to take under control. Similar to GPOs, there is a process that happens when you take control of a container. To start with, you will need to grant the CMGPI service account the **read and write permissions** rights over any sites, domains or OUs that you want to take control of. This can be done, again, with the **SetCMGPPermissions.exe** utility, or via AD Users and Computers (or by granting the service account privileged access by virtue of an existing privileged group).

The process of taking control of a container will result in a similar change in permissions to GPOs, but because the permission model on AD objects is different, the take control process differs as follows:

1. Built-in privileged groups such as Domain Admins, Enterprise Admins and LocalSystem are unchanged.
2. Any other users or groups that have write permissions on the gpLink and gpOptions attributes, will be set with Deny permissions to write to those attributes. If a principal has full control on a container object, they will be given Deny permissions on gpLink and gpOptions, but the Full Control ACE will be left as-is.

The bottom line here is that we want to prevent non-built-in privileged groups from being able to link, unlink and set link enforcement on any container under control by CMGPI.

To take control of containers, simply check the box next to the container (site, domain or OU) to place it in the Review and Take Control list, then press the Take Control button (see Figure 14). Note that you will need to select each OU in a nested hierarchy separately to take control of each. If you want to recursively take control of containers, see the **Register-CMObjects** PowerShell cmdlet found in the CMGPI PowerShell module, described in [Appendix C: The CMGPI PowerShell Module](#).

Welcome

Welcome to the setup of CMGP. From this wizard, you can configure the GPOs and Containers you wish to bring under control within the product as well as configure who can edit and approve those objects. You can also configure email notifications and other settings within the product.

Progress bar: 1 Add GPOs from AD domains, 2 AD Containers, 3 Delegate Access, 4 Settings

sdmsoftware.net Type domain name

AD Containers

- sdmsoftware.net
 - Sites
 - California
 - Domains
 - sdmsoftware.net
 - Admin
 - AMER
 - APAC
 - Domain Controllers
 - EMEA
 - Engineering
 - Servers
 - Workstations
 - Machines
 - People
 - SDM
 - Test

Review and Take Control

Name	Status	Domain	Last Update	Last operation
AMER	Controlled	sdmsoftware.net		Success
California	Not Controlled			
sdmsoftware.net	Not Controlled	sdmsoftware.net		
EMEA	Not Controlled	sdmsoftware.net		
Engineering	Not Controlled	sdmsoftware.net		
Servers	Not Controlled	sdmsoftware.net		
Workstations	Not Controlled	sdmsoftware.net		

Take control Remove control

Close

Figure 14 Taking control of AD containers

When you select the checkbox for a container, it's put into the Review and Take Control list, but when you un-check it, it's removed. If you come back to this screen, you will have to re-check the relevant containers to see their status and take or remove control.

Now that we've taken control of both GPOs and containers, we need to delegate access to those controlled objects. This can be done using Step 3—Delegate Access in the Welcome Wizard.

The Take Control Process for Intune Profiles

Once Intune support is enabled you will see all available configuration profiles appear in CMGPI, as shown here:

Welcome

Welcome to the setup of CMGP. From this wizard, you can configure the GPOs and Containers you wish to bring under control within the product as well as configure who can edit and approve those objects. You can also configure email notifications and other settings within the product.

Progress bar: 1 Add GPOs from AD domains, 2 AD Containers, 3 Intune Profiles, 4 Delegate Access, 5 Settings

Azure AD connected

Name	Platform	Type	Assigned	Modified Date	Status	Last operation
Android Enterprise - personal - Device restrictionsX	Android Enterprise	Template	No		Not Controlled	
Android Enterprise - personal - Trusted certificate	Android Enterprise	Template	No		Not Controlled	
Android Enterprise - Trusted certificate - 2	Android Enterprise	Template	No		Not Controlled	
b04d621b-733f-4222-b71f-7b3404964760	Android (AOSP)	Template	No		Not Controlled	
BaselineX	Windows 10 and later	Administrative Templates	Yes	4/20/23, 4:40 PM	Controlled	Success
bbd198de-6258-4aa8-9d5a-bf8c07076104	Windows 10 and later	Administrative Templates	No		Not Controlled	
Custom Attribute script	macOS	Custom attribute	No	4/20/23, 4:40 PM	Controlled	Success
iOS/iPadOS - Device restrictionsX	iOS/iPadOS	Template	Yes		Not Controlled	
iOS/iPadOS - Edition upgrade and mode switch	iOS/iPadOS	Template	No		Not Controlled	
iOS/iPadOS - Education	iOS/iPadOS	Template	No		Not Controlled	
iOS/iPadOS - PKCS certificate	iOS/iPadOS	Template	No		Not Controlled	

Take control Remove control

You can take control of any Intune Profiles that appear in the list. The process of taking control of an Intune profile involves adding a scope tag to that profile to restrict editing of that profile outside of

CMGPI. The scope tag that is added by CMGPI when a profile is taken under control is called **CMGPI_Controlled**.

Once an Intune Configuration Profile is taken control of, it appears as an object under control just as GPOs and containers do, and can be assigned editors and approvers.

*NOTE: CMGPI currently does not support creation of **new** Intune Configuration Profiles from within the platform.*

Delegate Access

The delegate access process is about adding users or groups of users as **editors** and **approvers** for a set of GPOs, containers or Intune Profiles.

Editor and Approver Capabilities

Editors have the following capabilities:

- Check out GPOs, containers or Intune profiles for change
- Edit GPOs or GPO permissions, link/unlink, enforce or enable/disable GPO links on containers and perform edit operations on Intune Configuration Profiles, as well as their assignments and scope tags
- Check in GPOs, containers and Intune Profiles after a change
- Discard a check out
- Request a rollback of a GPO, container or Intune Profile change
- View differences between current and prior versions of GPOs, containers and Intune Profiles

Approvers have the following capabilities:

- Approve GPO, container or Intune Profile changes
- Reject GPO, container or Intune Profile changes
- Cancel a GPO, container or Intune Profile approval
- Deploy immediately or schedule a GPO, container or Intune Profile change for deployment
- Cancel a scheduled GPO, container or Intune Profile scheduled deployment
- View differences between current and prior versions of GPOs, containers or Intune Profiles

To proceed, select Step 5--Delegate Access from the Welcome Wizard. You will see a list of the objects (GPOs and Containers) that you have delegated from Steps 1 & 2, along with two columns for selecting Approvers and Editors, as shown in Figure 15.

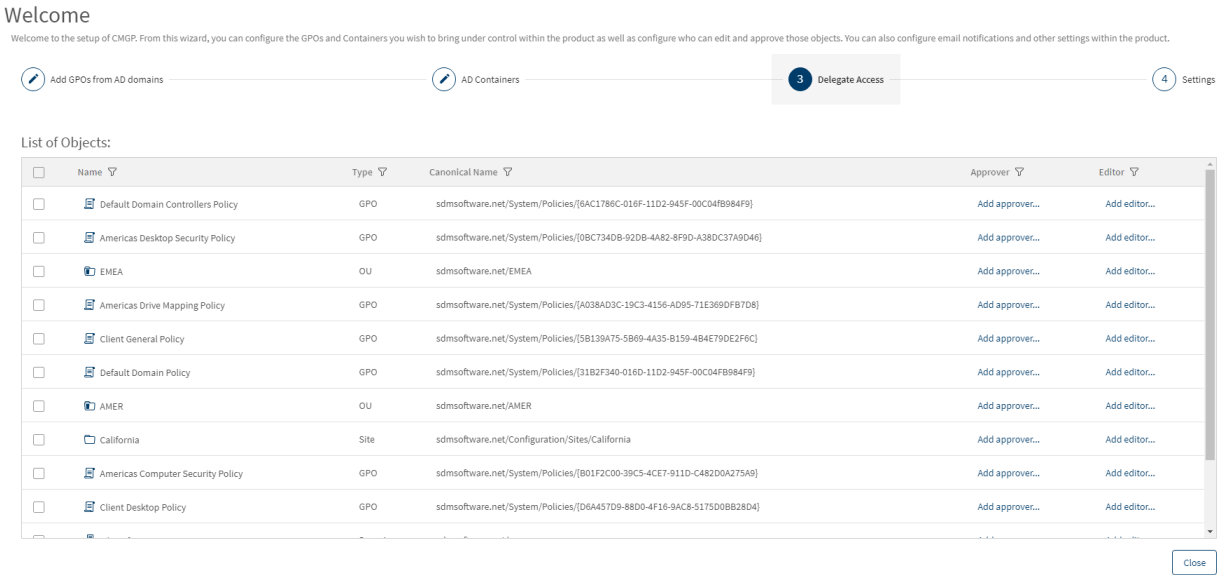


Figure 15 Delegating access to GPOs and Containers

You have two ways you can add editors and approvers. You can select all items from the checkbox at the upper left of the grid. When you do that, links are added to set the same editor and approver for the selected items, as shown here:

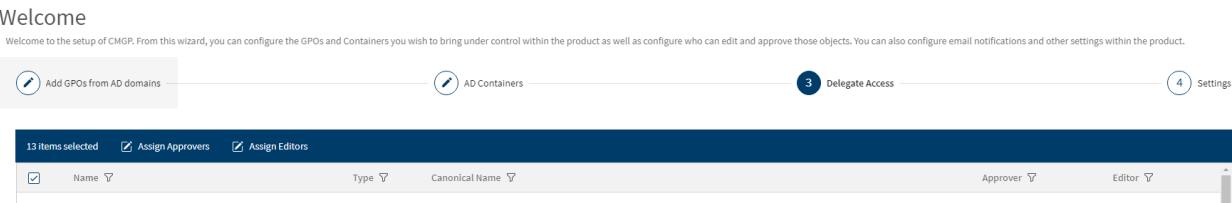


Figure 16

If you press the Assign Approvers or Assign Editors links, you can set the approvers or editors for all selected objects to the same value.

Alternatively, you can set approver and editor on individual objects by clicking the Add approver.. or Add editor... links in the Approver and Editor columns, as shown here:

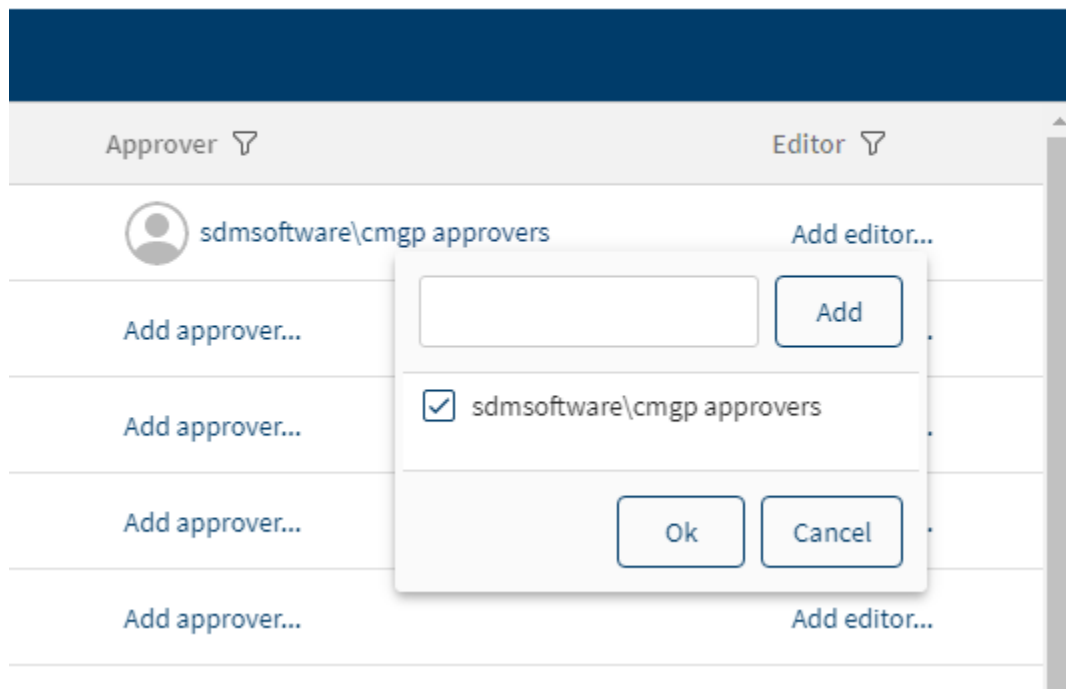


Figure 17

When entering an approver or editor, you will need to enter free text in the domain\user or group name format, as shown in Figure 17 above, where we've added the sdmsoftware\CMGPI approvers group as an approver for this object. Once the user or group name is entered, press the Add button to add the object and then press OK to commit the change. To remove a previously selected user or group, uncheck the box on the object and then press OK.

You can use either AD users or AD groups as editors or approvers. In the case of groups, the user's group membership will be evaluated at logon time and their managed objects calculated. Note that for Intune Profiles, even though you are entering an AD domain and user name as editor and approver, when it comes time to edit an Intune Profile, you'll be authenticating to Azure AD using the corresponding Azure AD credential.

You do not need to assign editors and approvers for all objects during this wizard step. Object delegation can be accomplished after the fact if you are a Product Administrator.

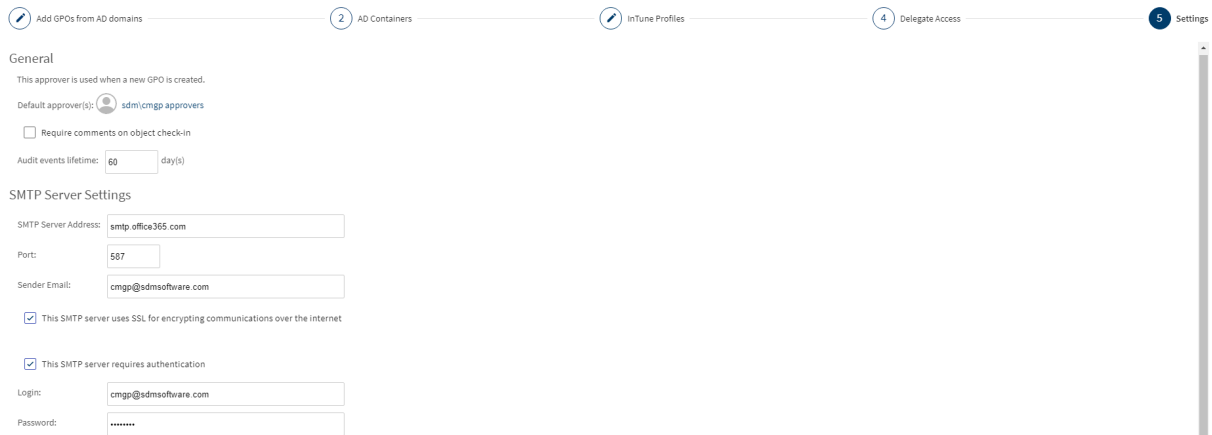
Once you have completed setting approvers and editors you can proceed to Step 5—Settings, in the Welcome Wizard.

Settings

The settings page within the Welcome Wizard allows you to configure a number of general product settings, as shown in Figure 18:

Welcome

Welcome to the setup of CMGPI. From this wizard, you can configure the GPOs and Containers you wish to bring under control within the product as well as configure who can edit and approve those objects. You can also configure email notifications and other settings within the product.



1 Add GPOs from AD domains 2 AD Containers 3 InTune Profiles 4 Delegate Access 5 Settings

General

This approver is used when a new GPO is created.

Default approver(s):

☐ Require comments on object check-in

Audit events lifetime: day(s)

SMTP Server Settings

SMTP Server Address:

Port:

Sender Email:

☒ This SMTP server uses SSL for encrypting communications over the internet

☒ This SMTP server requires authentication

Login:

Password:

Figure 18: Configuration for general product settings

These settings are described here:

- **Default Approvers:** This allows you to set one or more users or groups as default approvers, who are automatically assigned to GPOs newly created using CMGPI. In this case, a user or member of a default approver group will be able to approve a given GPO or container change for newly created GPOs. Be sure to click the Save button on the Settings page when you've added a default approver.
- **Require comments on object check-in:** If this box is checked then when an editor checks in an object change, they will be REQUIRED to enter text in the comment box and cannot skip over those comments.
- **Audit events lifetime:** This value, which defaults to 60 days, controls how long CMGPI audit events are kept in the system before they are purged. You can adjust this value up or down depending on your needs.
- **SMTP Server Settings:** CMGPI uses email to alert editors and approvers when certain events happen. To facilitate that, you will need to configure SMTP settings for your environment. The Sender email you enter is used to send a test email to the currently logged on user's email address (mail attribute on the user object in AD) that confirms that the settings are working, when you press the Test button. The sender email is also the source email from any alerts the product sends.

Make sure you press **Save** on the settings dialog to ensure that changes you entered here are saved correctly.

Press the Close button to close the Welcome Wizard. Once the settings are configured, you can proceed with using the product. Remember that you don't need to complete all steps of the Welcome Wizard prior to using the product.

Using the Product

Once the product is installed and configured, 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>. The ability to log in to CMGPI is governed by the roles that the product supports. We've already introduced the Editor and Approver roles, but the product contains a number of other roles as well, which are defined below.

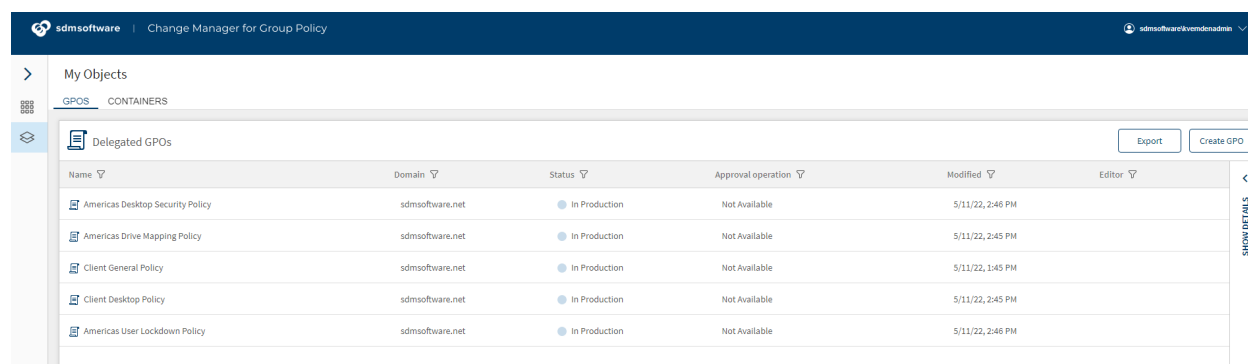
Note, currently CMGPI supports only using AD accounts to log in and grant access to product functionality. In order to support the Intune settings editing function, you will need to also have an Azure AD account with the required access (more on this in the section on editing Intune profiles.)

Product Roles

The Product Administrator role is the only role that can delegate Product Roles, including the roles defined here. 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 GPOs and containers, setting delegation on GPOs, containers and Intune profiles, configuring application settings, managing licensing and viewing statistics and audit events across all managed objects. The user who installs CMGPI is in the Product Administrators role by default but the role can be delegated to other users as well. NOTE that the one limitation Product Administrators have is that they are prevented from making themselves approvers for any GPO or container.

GPO Creator: While users who are in the Editors role can perform most tasks related to GPO management, the one thing they cannot do by default is create new GPOs. That job is reserved for members of the GPO Creator role, which allows members to create new GPOs. Those GPOs are still subject to approval-based workflow for deployment, but nonetheless, 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:



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	

Figure 19 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. The purpose of the break glass role is to allow you to temporarily bypass normal approval-based workflows when needing to make urgent changes to GPOs or container links. A user who is in the Break Glass role does not need to explicitly be made an editor or approver of a GPO or container. They can check out and edit any object under control by CMGPI and they can also approve and deploy those changes themselves. This removes any oversight from the object change 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. This is only provided to a Break Glass user and provides 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. The Auditor role has two main rights. Members of this role can see all objects that have been delegated in CMGPI, and what their current state is. They can also view differences in previous versions of the object. Their second main right is that they can view the [CMGPI Audit Log](#), which allows them to see what activities have occurred.

CMGPI Dashboard

When a user who is delegated as an approver or editor to either GPOs, containers or Intune Profiles logs into the CMGPI web application, they are immediately presented with a Dashboard showing high-level statistics for their role, as shown in Figure 20 below:

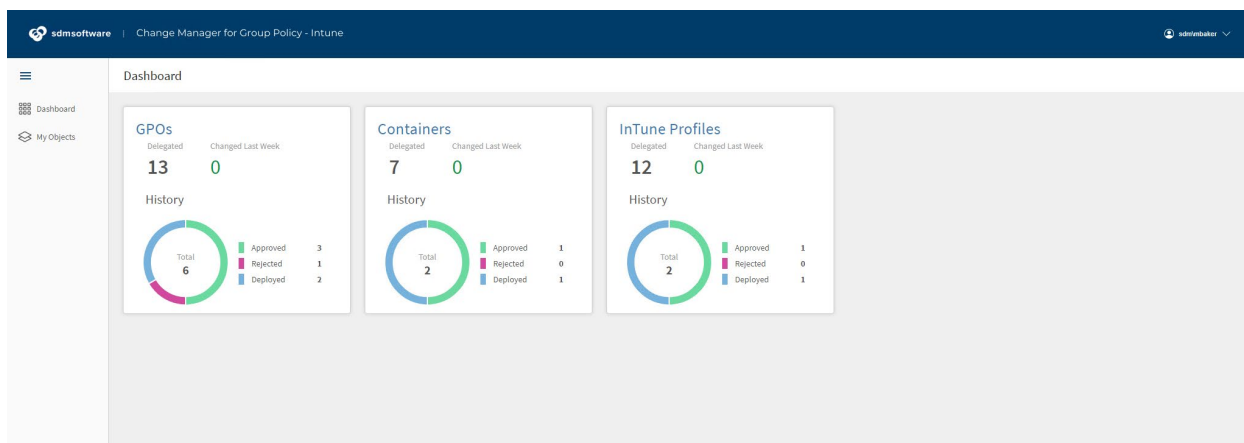


Figure 20 The CMGPI Dashboard

The dashboard is broken into three sections—the left-hand box provides statistics for GPOs, the middle box provides statistics for containers and the right-hand box provides statistics for Intune Configuration Profiles currently under control through the product. When a user in either the approver or editor roles logs in, they are seeing the statistics that are relevant to them. As an example, the GPOs, Delegated statistic shows how many GPOs are currently delegated to them, as either an editor or approver. The

Changed Last Week number shows the number of GPOs (or containers or Intune profiles) 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 or editor for. So, if I, as an editor of GPOs, log into CMGPI, I will see any GPOs (or containers or Intune profiles) that were approved, rejected or deployed, that I was the editor for, even though I was 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 facilitated by using the menu bar on the left-hand side of the product. The menu bar options change depending upon what role the logged in user is part of. As an example, a user who is an editor or approver will see two options on the left, as shown in Figure 21:

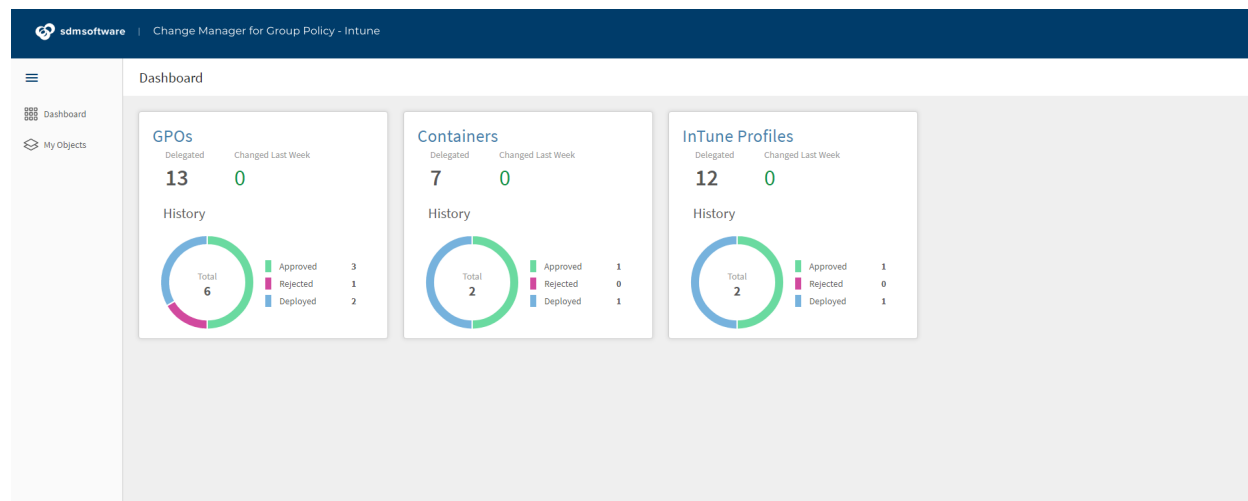


Figure 21 Viewing the CMGPI menu

By contrast, a product administrator, logging into the console, will see quite a few more options:

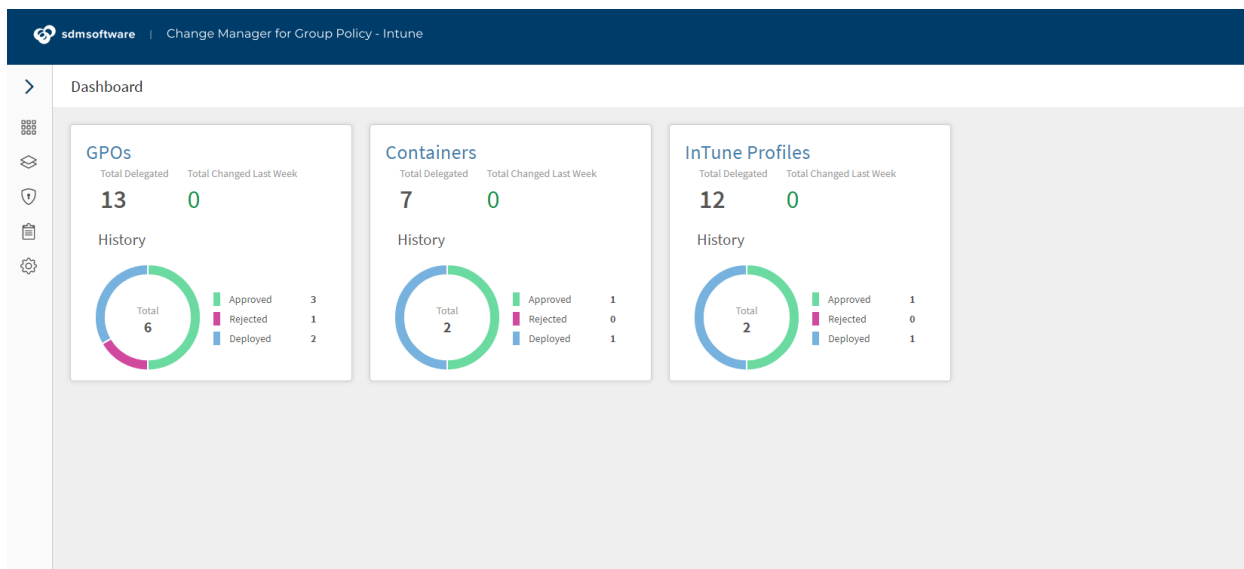


Figure 22 The full set of CMGPI menu options

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 or approver for. In the case of product administrator, break glass or auditor roles, all objects under control are shown here.
- **Delegation, Product Roles:** Allows the product administrator to delegate users to additional CMGPI [product roles](#).
- **Delegation, Objects:** Allows a product administrator to manage the delegation of GPOs, containers and Intune Profiles that are currently under control. This is where a product administrator can change which users and groups are editors or approvers of a GPO, container or Intune Profile.
- **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, require comments on check-in, audit events lifetime and SMTP settings.
- **Settings, Target DC:** This section allows you 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 additional GPOs, containers, or Intune Profiles that were not taken control of during the Welcome Wizard.
- **Settings, License:** Allows the product administrator to view and update the license that is in use by CMGPI.

The Change Control Process

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

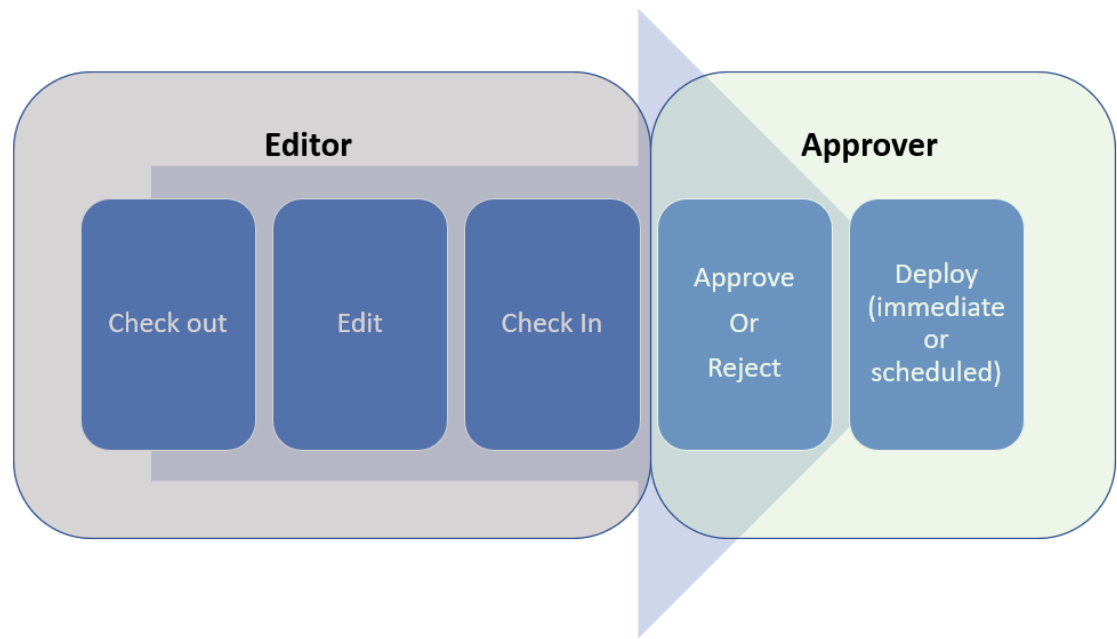


Figure 23 The CMGPI Change Workflow

As an editor, the starting point after logging in to the CMGPI console is the **My Objects** page, as shown in Figure 24:

sdmsoftware Change Manager for Group Policy - Intune				
My Objects				
GPOS CONTAINERS INTUNE PROFILES				
Delegated GPOs				
Export Create GPO				
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_GPPPlug	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

Figure 24 The My Objects page

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

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

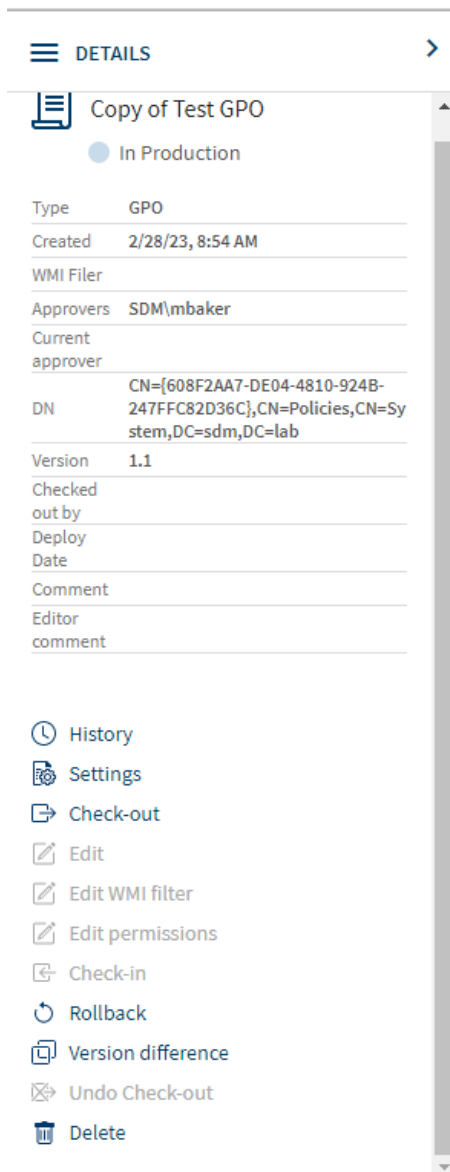


Figure 25 The Details Pane on an object

Actions that are currently available are shown as dark text and the 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 both GPOs and containers.

Editing GPOs

Once you press 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 also has the ability to check for changes that have happened to controlled GPOs, 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

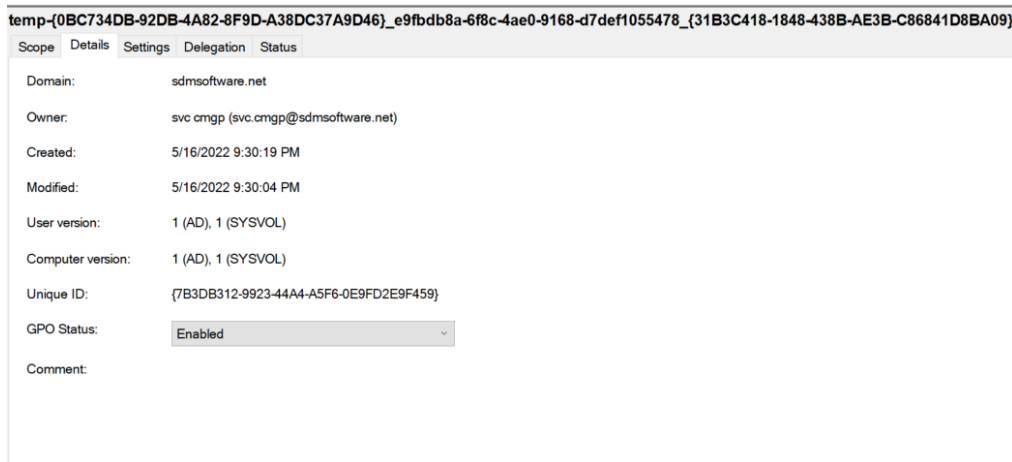
From this dialog, you can view the difference report to show the difference between what's currently in production and what CMGPI knows is the last known good version deployed. And you can choose how to handle it. The first option, "Roll-back the production version to the last controlled version," overwrites 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," then 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:** The history view allows you to see the history of what changes have been committed to the GPO since the product took control of it
- **Settings:** The settings report shows the current settings within the production GPO
- **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 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

NOTE: 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 have a very distinct naming structure, as shown here:



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 you 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. (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:

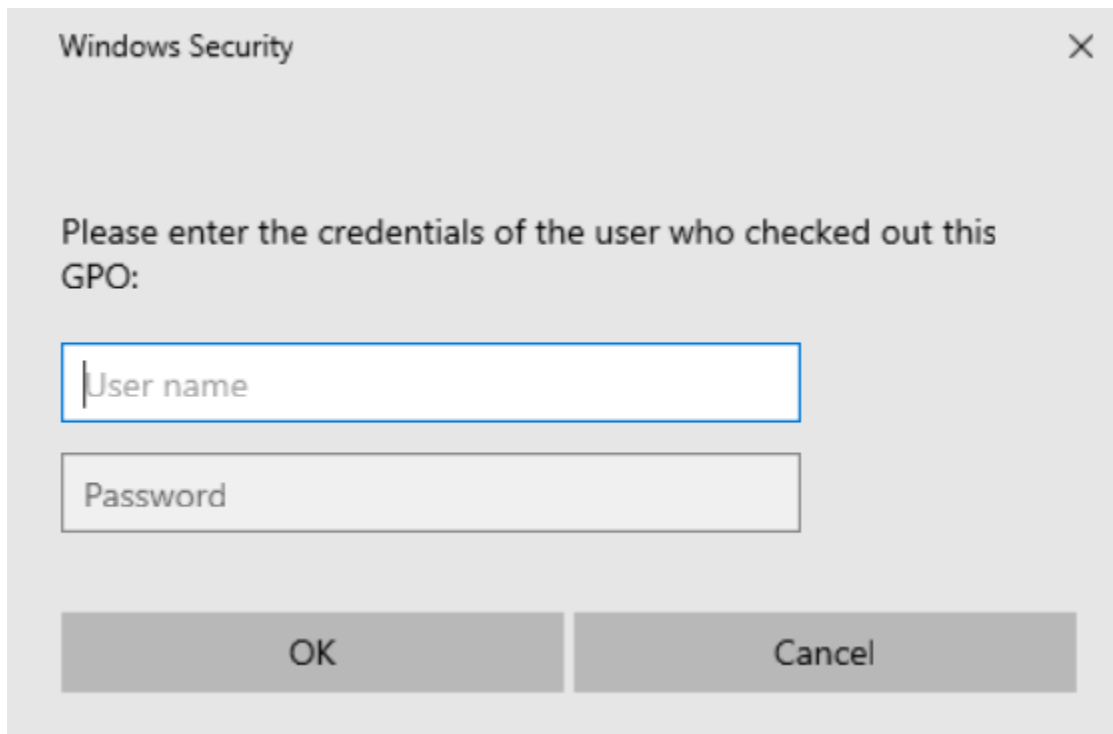


Figure 26 Entering credentials to launch the GP Editor

Once the 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, simply 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.

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 press the button, you have the option of creating a new, empty GPO, or you can create a copy of an existing GPO, in which 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, then it will be created and then automatically checked in, waiting for approval. Note that since you are creating a new GPO here, 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:

Delete



The delete operation will be queued for the approver of this GPO.

Comment to approver:

This GPO is no longer needed

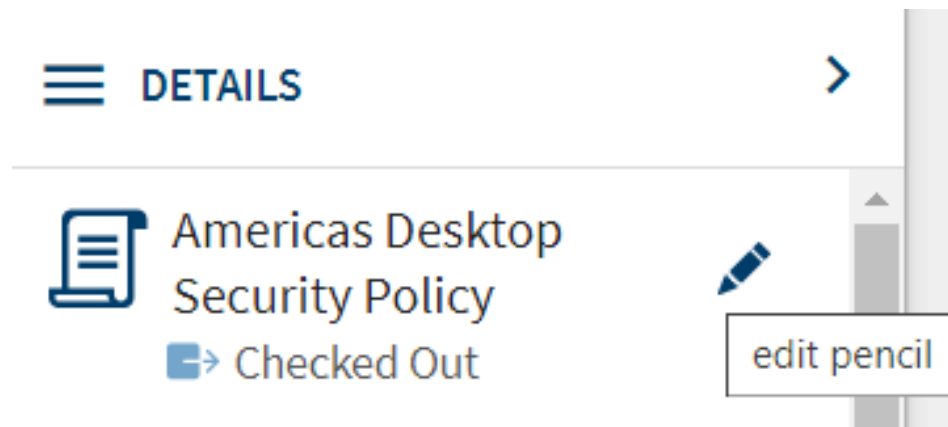
Submit

Cancel

When they submit the request, the GPO is then 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.

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 press the edit pencil, you can change the name of the GPO and press 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 given GPO as part of the change process, by selecting an existing WMI filter from the dropdown, as shown below, or choosing <None> to remove an existing WMI filter.

Edit WMI Filter



Test GPO

This GPO is linked to the following WMI filter:

Name:

Test OS

Ok

Cancel

Changing GPO Delegation

GPO delegation can also be changed as part of the change approval process. 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 in Figure 27 below:

Delegations

Americas Desktop Security Policy

Group and users:
Permissions:

Apply

Read

Deny apply

Add

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

Ok

Cancel

Figure 27 Modifying GPO Delegation

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

NOTE: 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

As 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. These comments are stored with the change through its lifetime and can be referenced when you view differences on a given GPO (see Figure 28 below) or from the **History** view on the Details pane.

SDM Software Change Manager for Group Policy/Intune® Installation & User Guide

Page | 39

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

Check-in

Americas Desktop Security Policy

Comment to Approver:

Made a change to Security Options for Change Ticket #33045


Ok Cancel

Figure 28 Comments recorded with a GPO change

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


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

Figure 29 Approver email notification

The approver can approve or reject this request by pressing the buttons in the email, which will direct them to the appropriate page in the CMGPI application. 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.


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. Pressing deploy 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

Figure 30 Scheduling a 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 both the editor and approver, indicating the status of the deployment. This applies to all types of deployments—GPOs, containers and Intune Profiles.

When an object is deployed, the 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 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. At that point, you can edit the container. Press 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 Admin and UNC hardening	sdm.lab	⋮

☒ Block inheritance

Figure 31 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 to link. Press the Add button to add the GPO to the link list. The GPO will be added to the end of the list.

*When you add a new GPO to the link list, it is added as a **DISABLED** link. Click the three dots to enable the link.*



Press OK when you're done editing the link list and then press 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. Note that changing Block Inheritance, when deployed, has an effect on what GPOs are inherited by a given container.



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 can then choose to deploy it immediately or on a schedule, as with GPO changes. The same options are available as shown in Figure 30 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 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 users or groups to those roles. However, when it comes time for an editor to actually edit a profile, they will authenticate to Azure AD (AAD) using their AAD credentials. For example, if you assign *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 to AAD in order to edit that profile.

Before they can do that, you will need to grant access to AAD 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 AAD security group called **CMGPI Intune Editors**. It also creates an AAD 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 AAD 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>
```

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

When you run the script, you’ll be prompted for your AAD credentials, which should have the ability to add a security group and custom role to your AAD 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

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 presses Edit on a profile, a new browser window is opened focused on the temporary Intune profile, as shown here:

The screenshot displays the Microsoft Intune admin center interface. The left-hand navigation pane includes links to Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'temp-TestSettingsCatalog_b24ecd05-7bee-480a-a126-5fbb2c860718' and identifies it as a 'Device configuration profile'. A 'Delete' button is visible. Below this, the 'Device and user check-in status' is shown with a bar chart indicating counts for Succeeded, Error, Conflict, Not applicable, and In Progress. A 'View report' button is present. Two informational boxes are shown: 'Device assignment status' (reporting on devices targeted by the policy) and 'Per setting status' (viewing configuration status for each setting). The 'Properties' section includes a 'Basics' tab with fields for Name, Description, and Platform. The 'Assignments' section has an 'Edit' link. Below, the 'Included groups' and 'Excluded groups' sections are shown, both currently displaying 'No results'.

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

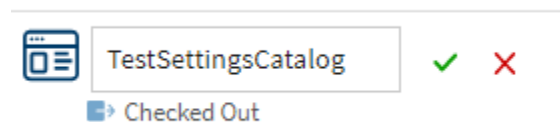
SDM Software Change Manager for Group Policy/Intune® Installation & User Guide

Page | 47

This will look 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 simply clicking the pencil icon on the name of the profile after it's been checked out:





Once you've adjusted the name as desired, 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, press the edit link next to the Scope Tags section on the details pane. Once you do that, the existing tags are presented and you can choose to add or remove tags from here. Note that 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 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 pressing the Edit link next to the Assignments section of the Details pane, which will bring up the dialog as shown here:

Assignments

Include groups ☒ Groups ☐ All users/devices

Type group or user name

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

Type group or user name

This dialog mimics the capabilities in Intune itself. Notably, you can both include and exclude groups, and that can include either AAD groups or users or all users/devices. If you are adding groups, you can start typing the name of the AAD 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 profiles 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, any profile changes that have been submitted. 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\kvmedenadmin
5/20/22, 5:09 PM	✓ Check-in	EMEA	sdmsoftware.net	Started	sdmsoftware\kvmedenadmin
5/20/22, 4:45 PM	➤ Check-out	EMEA	sdmsoftware.net	Success	sdmsoftware\kvmedenadmin
5/20/22, 4:45 PM	➤ Check-out	EMEA	sdmsoftware.net	Started	sdmsoftware\kvmedenadmin
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 Time: 5/20/22, 5:22 PM

Location: sdmsoftware.net

User: sdmsoftware\lgrangeradmin

Status: Success

Canonical Name: sdmsoftware.net/EMEA

Figure 32 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 also 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, you can 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 member of the Product Administrator role. A product administrator can see and manage licensing from the Settings, License page, as shown here:

☰

Dashboard

My Objects

Delegation

Product Roles

Objects

Audit log

Settings

General

Take Control

License

Settings • License

License Mode: Demo

Company:

Contact:

Time Remaining: 17 day(s)

Expiration Date:

License count: 0

License status: Valid

Activate a new license: Upload new license

Figure 33 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 pressing the “Upload new license” button and then 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> -domain <DNS Domain Name> <cmd> [option] [<cmd> [params] ...]
cmds are:
-GPOCreator
-GPOModify
-Container <Optional DN of parent container--OU or domain DN>
-Site <Optional DN of site or parent of all sites>
-Recurse
```

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 all GPOs in the specified domain.

SetCMGPPermissions.exe -trustee sdmsoftware\svc.CMGPI -domain sdmsoftware.net -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 used in conjunction with -Recurse, with all sites objects, as shown in the example here:

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

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:

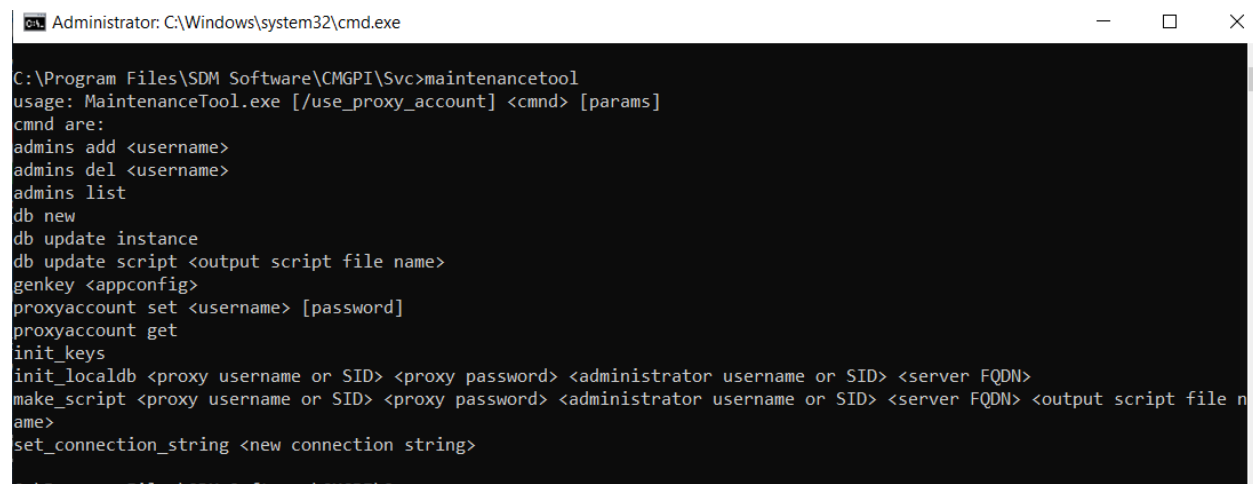
Setting Name	Description	Default Value
DefaultApprovers	Semi-colon separated list of the defined default approvers	Blank (unless set in the UI)
FrontendBaseURISettingName	Base URI used in all messages that reference the CMGPI front-end	URI used during setup
OperationsLogQueryLimit	Max count of audit log entries to retrieve	1000
ADGroupsCacheTTLSeconds	Time after which a user's group membership will be re-enumerated by CMGPI service	600
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	7200 (5 days)

	in and waiting for approval out will be flagged and an email reminder will be sent to the approval	
--	---	--

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 admin add mycompany\joeadmin

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

Maintenancetool proxyaccount set mycompany\svc_cmgp Passw0rd#!!

Show the current CMGP Service account

Maintenancetool proxyaccount get

Change the database connection string to point to a SQL Server instance called InstanceName running on port 50019 where the database name is CMGP

Maintenancetool set_connection_string ""Provider = MSOLEDBSQL.1;Data Source=cmgp.cpandl.com,50019\InstanceName;Initial Catalog=CMGP;Integrated Security=SSPI;"

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 67 cmdlets within a module called **SDM-CMGPI** 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

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 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 of 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 of CMGPI

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

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-CMEntities 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-CMEntities: 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-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-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-CMGPO: Creates a new GPO in CMGPI

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

Remove-CMGPO: Creates a GPO Deletion request

Rename-CMObject: Allows you to request a GPO rename

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

Set-CMDomainDC: Allows you to set a given domain controller as the preferred DC for a given domain under control in CMGPI

Set-CMEditorComment: Allows you to set a check-in comment on a GPO or container check-in

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

Set-CMEntityDescription: Allows you to set the description to a given checked out CMGPI managed Intune profile

Set-CMIntuneSettings: Allows you to disable or set 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: Used to set configurable options within CMGPI

Set-CMSMTPSettings: Can be used to set SMTP settings

Set-CMSystemDelegations: [Internal]

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

Test-CMSetup: Triggers Welcome wizard

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 want and need to be able to deploy the product with your own certificate. Doing so usually involves simply assigning your custom certificate with the IIS Administrator tool to the CMGPI web site, as shown here:

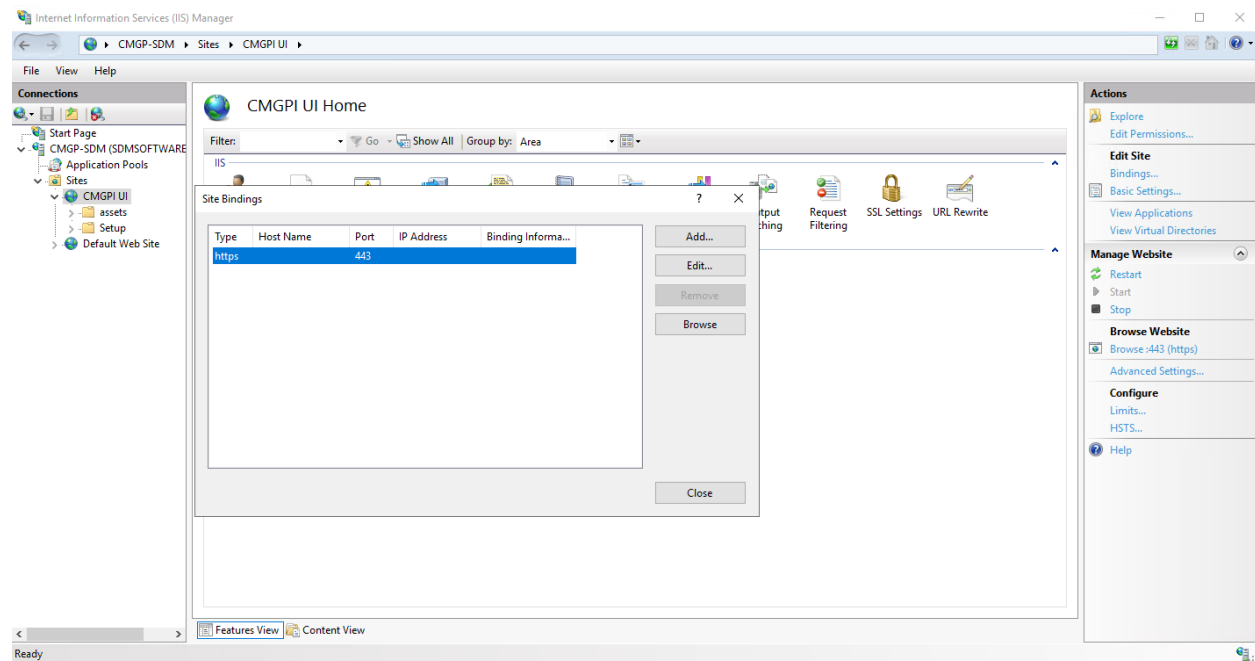


Figure 34 Configuring SSL binding for the CMGPI web application

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 CMGP 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 CMGP's configuration. We recommend you use this script when assigning a new certificate. The script should be run on the CMGPI web server and has the following options:

AddressHostname.ps1 -GetFrontentFqdn -BackendFqdn <string> [<CommonParameters>]: Returns the front end FQDN of the CMGP server for a given back end FQDN

AddressHostname.ps1 -GetBackendFqdn [<CommonParameters>]: Returns the current back end FQDN

AddressHostname.ps1 -SetFrontentFqdn -BackendFqdn <string> -FrontendFqdn <string> [<CommonParameters>]: Sets the front end FQDN for a given back end FQDN

AddressHostname.ps1 -SetBackendFqdn -BackendFqdn <string> [<CommonParameters>]: Sets the backend FQDN

AddressHostname.ps1 -GetFrontendCertificate [<CommonParameters>]: Returns the current SSL certificate thumbprint of the front end

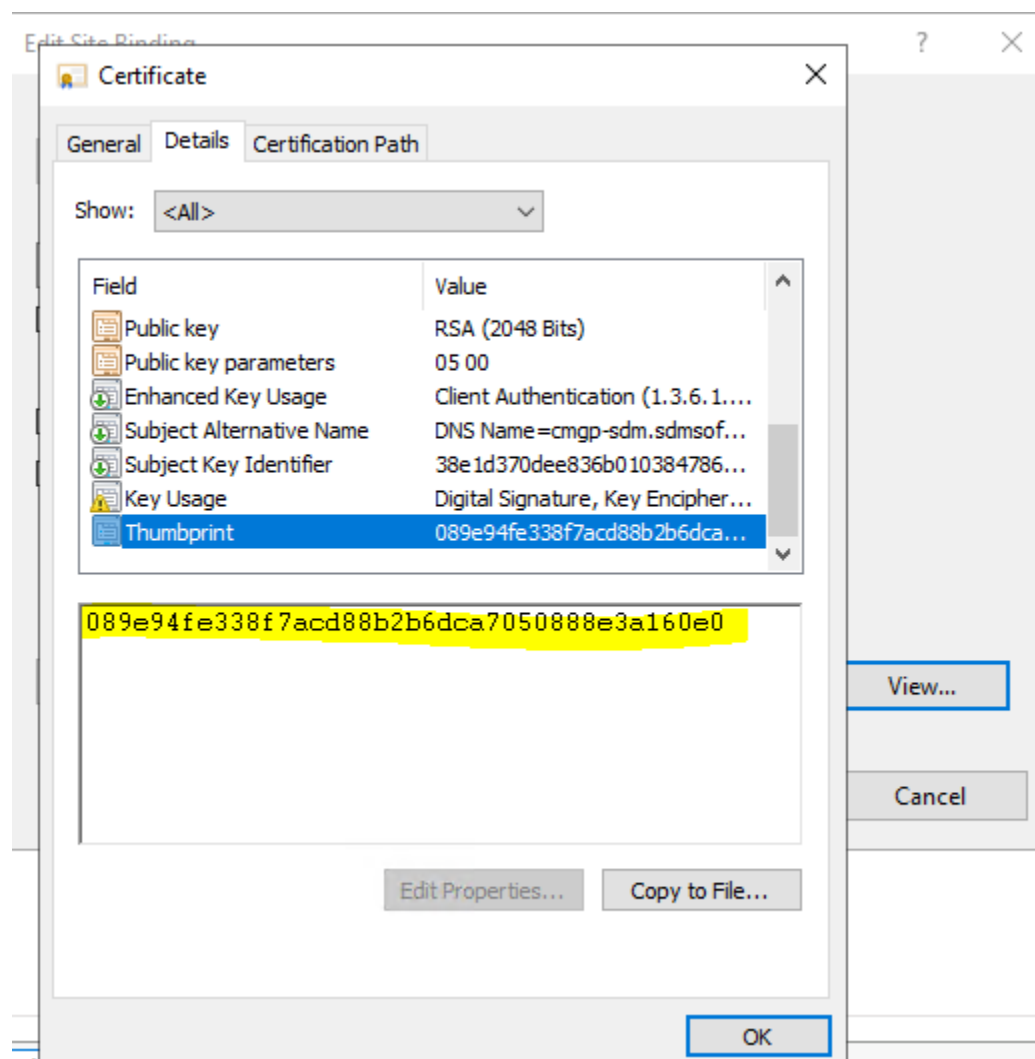
AddressHostname.ps1 -GetBackendCertificate [<CommonParameters>]: Returns the current SSL certificate thumbprint of the front end

AddressHostname.ps1 -SetFrontendCertificate -Thumbprint <string> -CertificateStoreName <string> [<CommonParameters>]: Sets the front end SSL certificate

AddressHostname.ps1 -SetBackendCertificate -Thumbprint <string> [<CommonParameters>]: Sets the back end SSL certificate

For commands above that require an SSL thumbprint , this *ChangeCertificate.ps1 <SSL Certificate thumbprint>*

Where the thumbprint you provide is taken from the properties of your SSL certificate. Which you can see 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 CMGP installation. You will need to set the certificate thumbprint for **both** the front end and back end of the CMGP server, as shown in steps 1 and 2 here:

1. Set the certificate for the front end

```
.\AddressHostname.ps1 -SetFrontendCertificate -Thumbprint  
'DDB44891BAF00C7E8DD072E945FEE837D34C05A8' -CertificateStoreName 'my'
```

2. Set certificate for the back end

```
.\AddressHostname.ps1 -SetBackendCertificate -Thumbprint  
'DDB44791BAF0EC7E3DD072E945FEE837D34C05A8'
```

Now let's assume you have the CMGP server hostname as cmgp.cpandl.com and you want to alias the hostname to gpochange.cpandl.com. Once you've set the SSL certificates for that hostname using steps 1 and 2 above, you'll need to also change the fully qualified domain names (FQDNs) of the front end and back end as well. Steps 3 and 4 below are examples of the syntax for that.

3. Set front end FQDN

```
.\AddressHostname.ps1 -SetFrontendFqdn -FrontendFqdn 'cmgp.cpandl.com' -BackendFqdn  
'gpochange.cpandl.com'
```

4. Set back end FQDN

```
.\AddressHostname.ps1 -SetBackendFqdn -BackendFqdn 'gpochange.cpandl.com'
```