



SDM Software Change Manager for Group Policy/Intune®

Version 1.9

Installation Guide

Revisions:

Document Version 1.0.....Feb 28,2025

Contents

CMGPI Architecture Overview	3
CMGPI Components	3
Network Requirements	4
Installation Requirements	4
Hardware	4
Software	4
Configuration/Security Rights Required	5
GPO Change Control Requirements	5
Intune Change Control Requirements	6
Entra ID SSO Requirements	7
Installation	7
Configuring the SQL Server Database	15
Configuring the Azure SQL Database	15
Migrating from one Azure SQL Database to another	17
Initial Configuration	18
Taking Control of GPOs	21
The Take Control Process for GPOs	22
The Take Control Process for AD Containers	24
The Take Control Process for Intune Profiles	27
Delegate Access	28
Enabling 3-level Approval in CMGPI	28
Editor, Approver and Deployer Capabilities	29
Settings	32
Configuring Intune Connectivity from the UI	33
Configuring Entra SSO from the UI	34
Configuring SSL on the CMGPI Server	37
Appendix A: Command-Line Installation Reference	38

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:

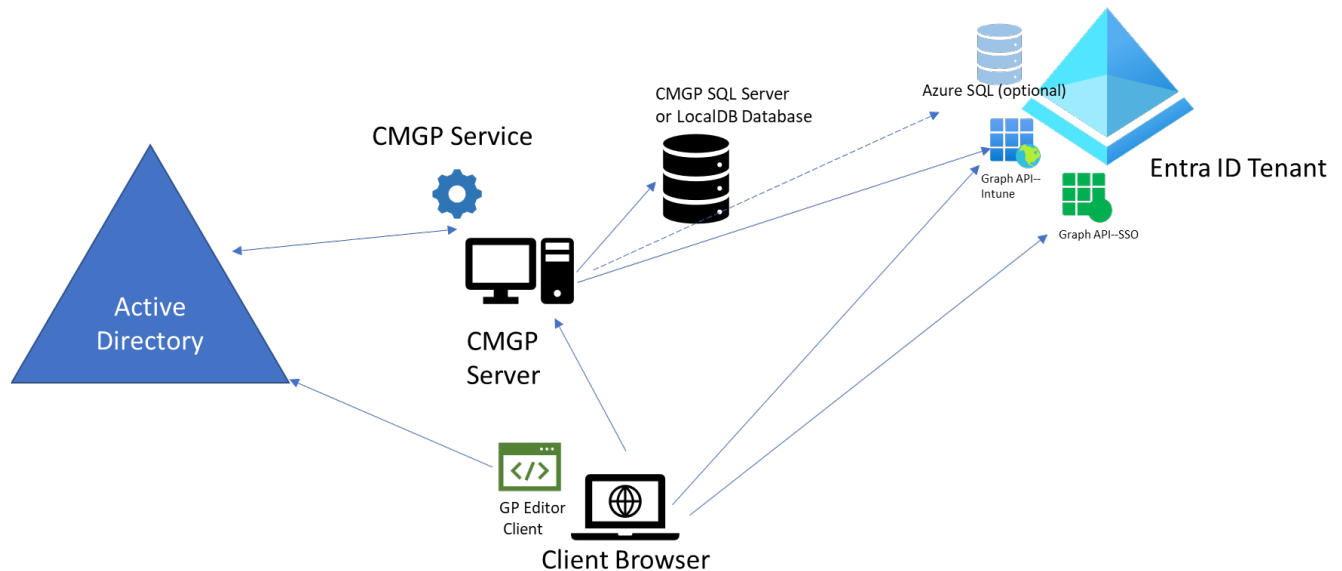


Figure 1: the CMGPI Architecture

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 (used for evaluation purposes only), 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.

Network Requirements

The following table enumerates the ports and protocols required for the CMGPI components listed above:

Source	Destination	Port(s)	Protocol
CMGPI Server	Active Directory (DC based on selection in the product)	LDAP (389), Kerberos (88), SMB (445), RPC Port Mapper (135), RPC Ports (49152-65535)	TCP
CMGPI Server	CMGPI Database (SQL Server)	1433 (or specified SQL client port)	TCP
CMGPI Server	CMGPI Database (Azure SQL --optional)	1433 (or specified SQL port running in Azure)	TCP
CMGPI Server	Graph API (for either Intune connectivity or SSO)	443	TCP
Client Browser	CMGPI Server	443 (by default)	TCP
Client Browser	Active Directory (uses DC Locator to select GPO) for GPO Editing only.	LDAP (389), Kerberos (88), SMB (445), RPC Port Mapper (135), RPC Ports (49152-65535)	TCP
Client Browser	Graph API (for Intune editing and for SSO)	443	TCP

Installation Requirements

The CMGPI installer provides a signed .exe 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 2016, 2019, 2022 or 2025 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) or, optionally Azure SQL)
- Chrome or Edge supported as Client Browser

*Ensure that the **ASP.Net** Windows feature is NOT enabled on the CMGPI server. This feature can be found in Server Manager, usually under the Web Server\Application Development section. This feature is known to cause issues with CMGPI web application behavior.*

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 for evaluation purposes)
- Microsoft IIS URL Rewrite Module 2
- Microsoft Application Request Routing 3.0

These components can be pre-installed if required. Occasionally security or anti-virus software will prevent the CMGPI installer from successfully installing for each of these components. If that is the case, we recommend pre-installing these packages prior to installing CMGPI.

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

GPO 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).

When using a gMSA account, you need to refer to the account with a \$ at the end of the username. For example: mydomain\gmsa\$.

The service account must have local administrator rights (i.e. a member of the local Administrators group) on the CMGPI server.

- Any user accessing the CMGPI server remotely needs the “**Access the Computer from the Network**” user right on the CMGPI server. The easiest way to accomplish this is to grant a group

access to this user right on the CMGPI server, and ensure all users who need to use CMGPI are in the group.

- 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.

If you are upgrading from a prior version of CMGPI and have deployed full SQL Server, you will need to provide the CMGPI service account with the db_DDLAdmin role for the upgrade or run the maintenancetool.exe utility 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. Now you can also pre-create the application registration and secrets ahead of time and configure those in the CMGPI UI. The following Graph API permissions 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 Entra ID tenant and you will need to have permissions to populate that group with members.

Entra ID SSO Requirements

If using the Entra ID SSO feature, you will need an enterprise application that has the following Graph API permissions:

- User.Read
- Directory.ReadAll
- GroupMember.ReadAll

Installation

The CMGPI installer is a signed .exe, called **CMGPI1.9Setup.exe**, 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. CMGPI makes your currently logged on user the first “Product Administrator” within CMGPI, able to configure and manage the application.

We do not recommend logging in and installing CMGPI with the account you’ve chosen as the CMGPI service account. This can result in unexpected behavior.

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

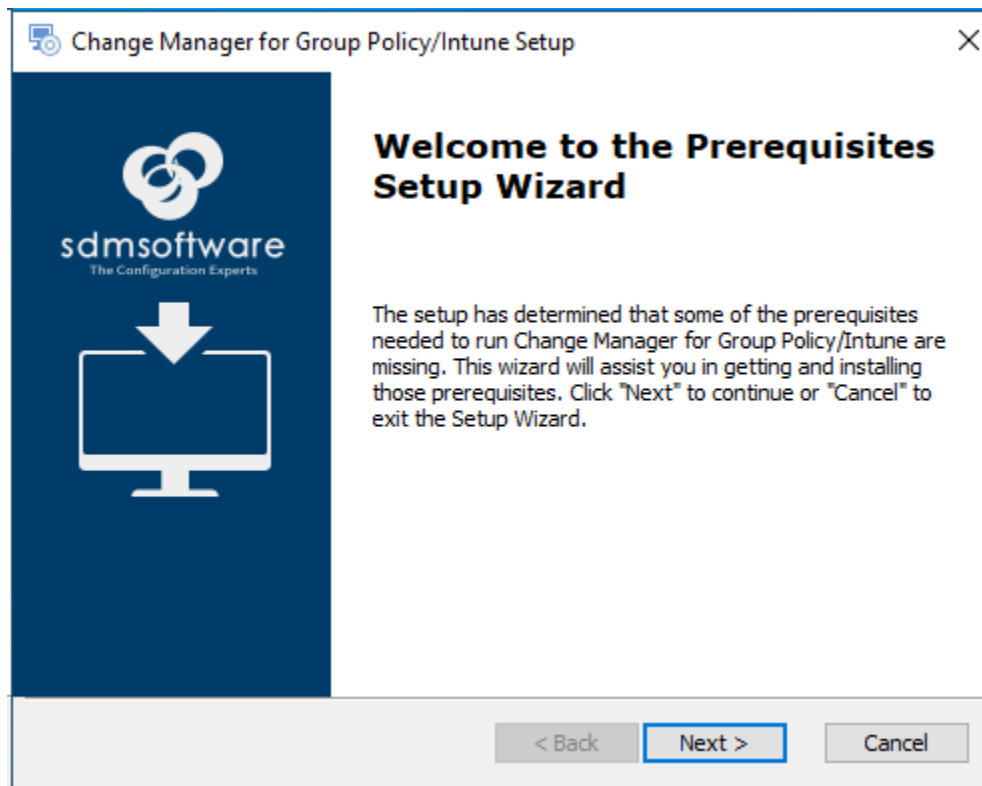


Figure 2

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

When you press the Next button, the dialog asks if you wish to install .Net Framework 4.7.2 (if it's not installed) and 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 if you are just evaluating CMGPI.**

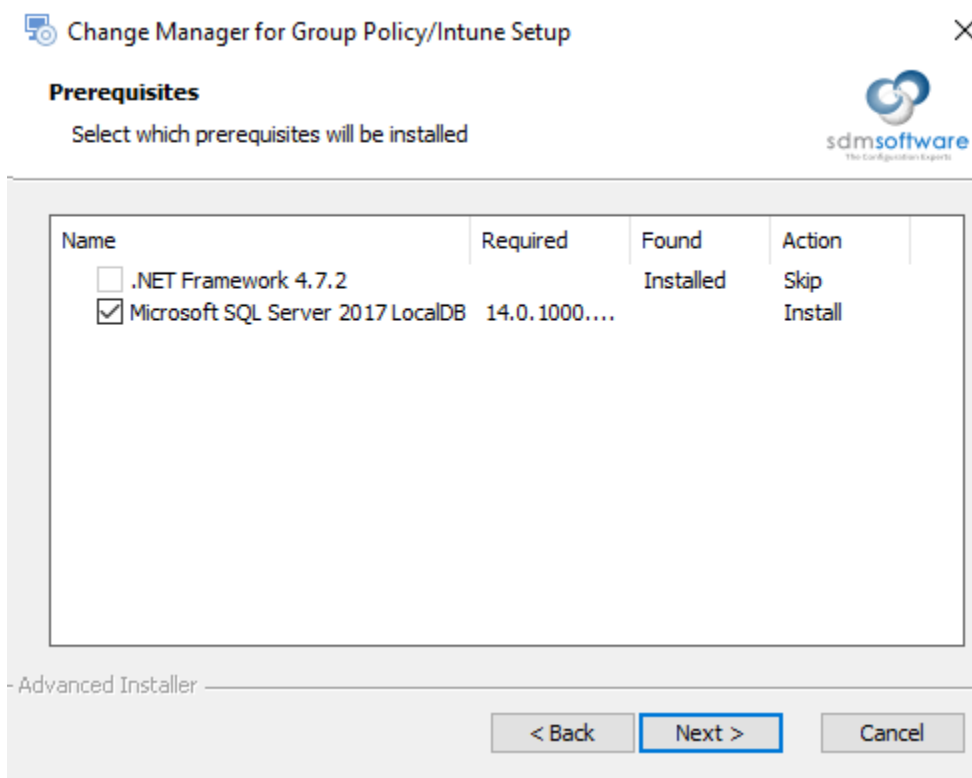


Figure 3

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. **If you are planning on installing CMGPI on a full SQL Server or Azure SQL database, there is no need to install this prerequisite.**

Once the LocalDB and/or .Net Framework installation completes, the CMGPI installer will continue. Press Next to accept the EULA. You will then need to provide the domain\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:
sdm\svc.cmgp

Password:
●●●●●●●●●●

-Advanced Installer

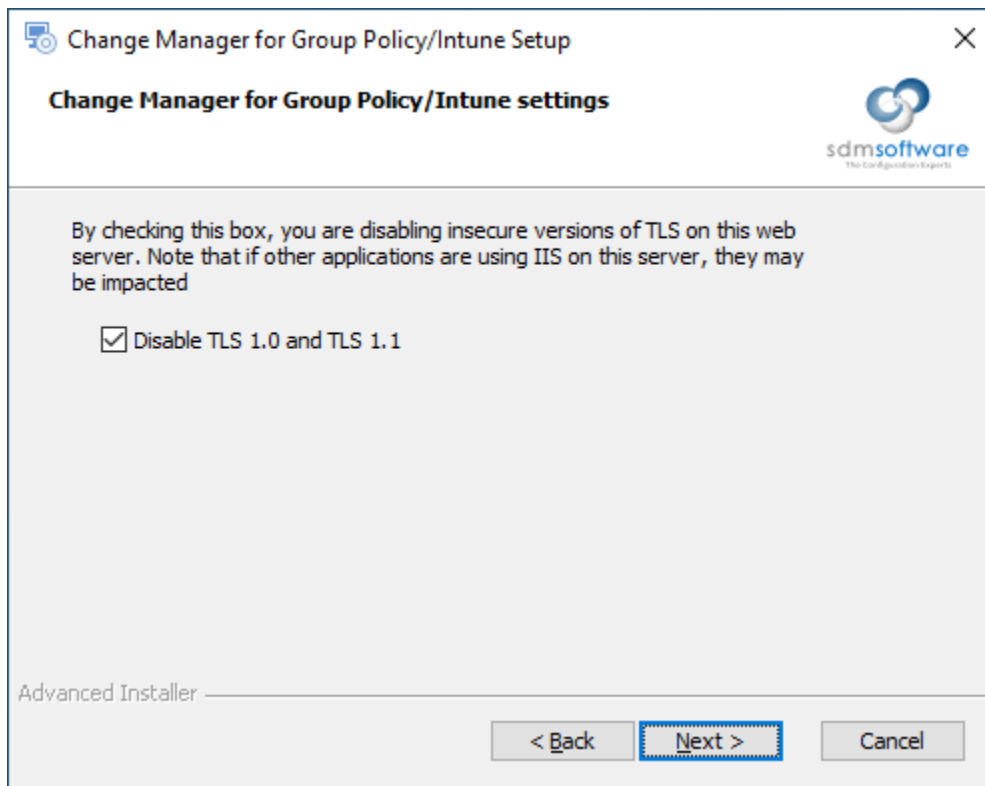
< Back Next > Cancel

Figure 4

If you are using a group Managed Service Account (gMSA) leave the password field blank here and enter the gMSA username with a \$ symbol at the end (e.g. mydomain\gMSAAccount\$).

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 (defaults to the C: volume but you can install on any volume), and on the following screen, you will need to choose whether you wish to disable insecure older versions of TLS on this server (the default is to disable them), as shown here:



On the next screen you'll need to choose whether you plan to use the SQL Server LocalDB instance on the server you're installing, a SQL Server installation separate from the CMGPI installer or Azure SQL, as shown in Figure 5.

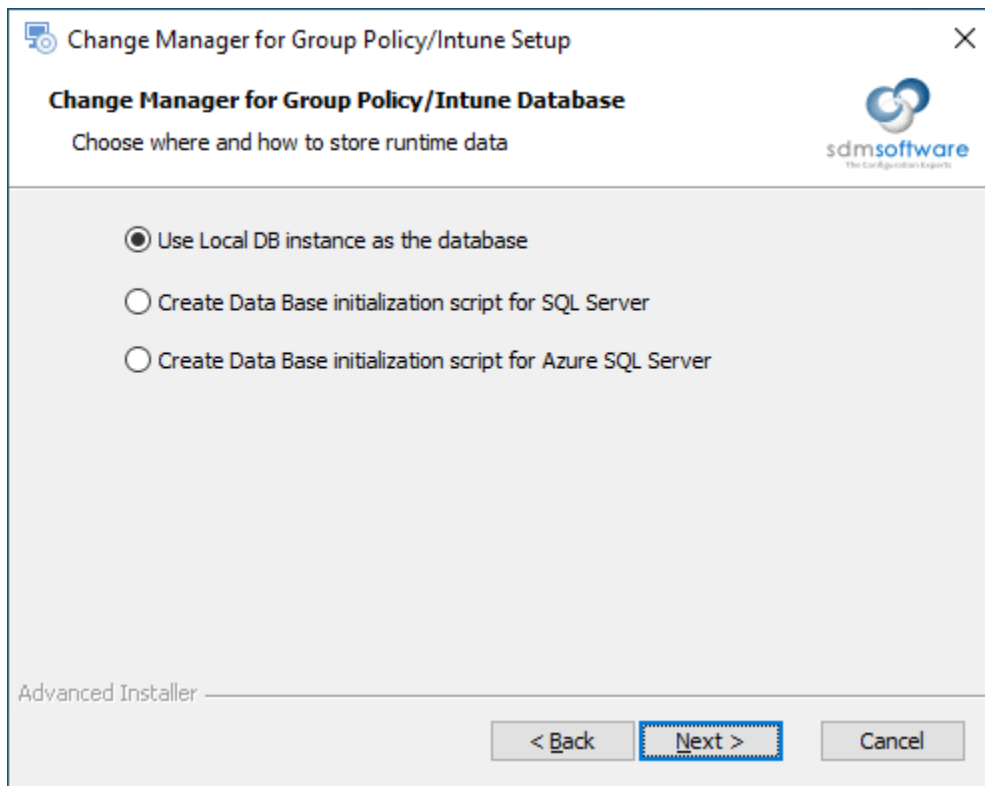




Figure 5

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 Server script that will open in your default text editor at the end of the CMGPI installer process. You can use this script within Microsoft SQL Server Management Studio to create the CMGPI database. The third option will generate a similar installation for an Azure SQL deployment. If you choose either the SQL Server or Azure SQL options, 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/Intune Setup** ✕

Configure SQL Server connection

Please enter information to connect SQL Server




SQL Server Instance:

Port:


Advanced Installer —

Or for Azure SQL:

 **Change Manager for Group Policy/Intune Setup** ✕

Configure SQL Server connection

Please enter information to connect SQL Server



SQL Server Instance:

Port:

Database:

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.

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.

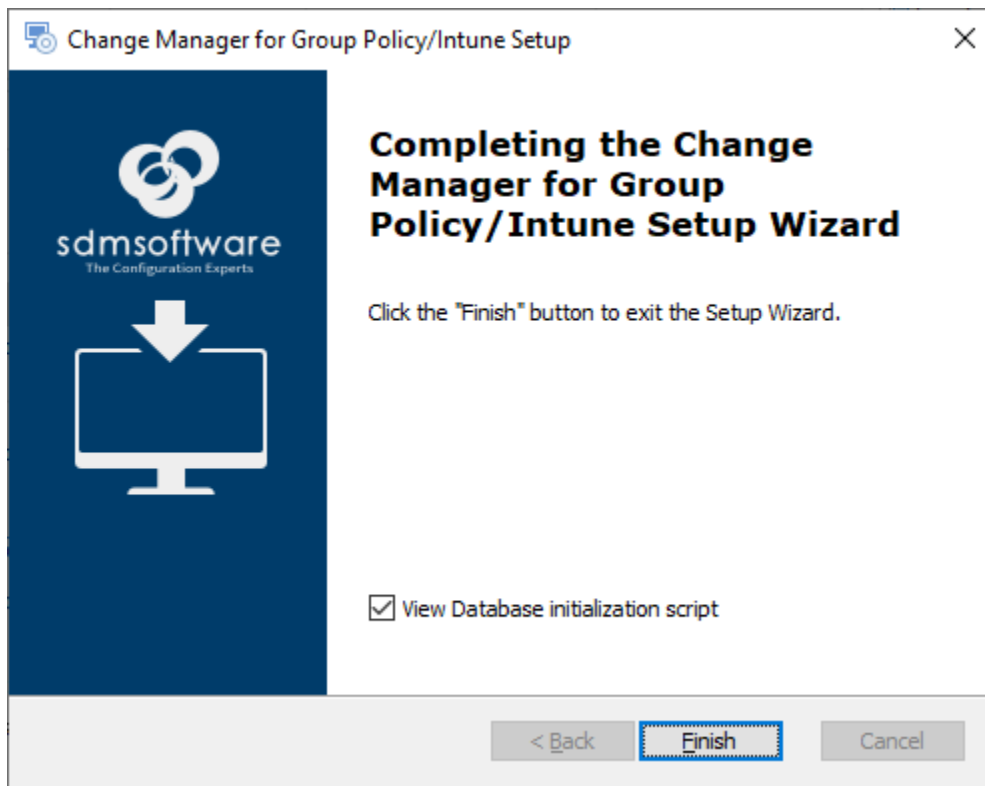
The installer will then complete the remainder of the installation, which includes adding required Windows Features and configuring IIS for the web application.

The CMGPI installer installs a self-signed SSL certificate that is used to protect the CMGPI web application, by default. To install your own certificate, you will be required to run a special PowerShell provided in the CMGPI installation called "addresshostname.ps1". Please refer to Appendix E in the CMGPI User Guide for usage.

During the installation process, two other prerequisite Microsoft packages are installed that require your attention to accept prompts— the Microsoft Application Request Routing 3.0 application and the Microsoft URL Rewrite Module 2 application. 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 web application.

Note also that if you chose to use the full SQL Server or Azure SQL setup option, the SQL creation script to create the CMGPI database (called CMGP-DB-Creation.sql) will open in Notepad once you select the Finish button on the installer for you to copy/paste into SQL Server Management Studio, as shown here:



In addition, the script itself is saved on the desktop of the installed server in case you need to retrieve it after Notepad closes. If you close Notepad, the CMGPI installer will end, but while Notepad is open, the installer will stay open as well.

Configuring the SQL Server Database

Copy the contents of the SQL Server creation script that appeared in Notepad after the installation completes, into a “New Query” in SQL Server Management Studio, connected to your database server and press “Execute.” The result is a new database called **CMGP**. Among other things, the script will grant your service account a login to the CMGPI database with db_datareader and db_datawriter permissions on the database itself.

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

Configuring the Azure SQL Database

Using Azure SQL as the database source requires that the database is already pre-created in Azure.

It is a prerequisite to first create the Azure SQL database in Azure prior to configuring CMGPI to use it.

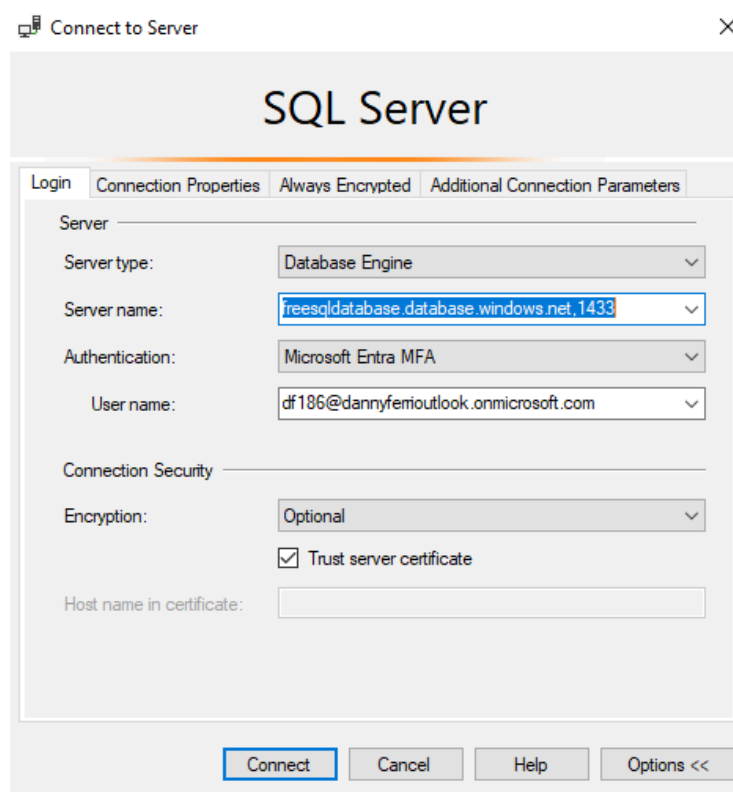
Before configuring the Azure SQL connection in CMGPI, use SQL Server Management Studio to verify access to the Azure SQL database you created. You may need to change the inbound port on the Network Security Group in Azure to allow public communication to the database.

Once successfully connected as the figure below shows, you need to run the “ConnectAzureSQL.ps1” script that is found by default in `c:\program files\sdm software\cmgpi\svc`. This script configures an Entra application registration that CMGPI will use to talk to the Azure SQL instance. This is required for the connectivity between the CMGPI server and the Azure SQL instance. This script requires two Microsoft PowerShell modules to be installed prior to running: **Az.Accounts** and **Az.Resources**. If your environment supports installing modules from the PowerShell Gallery, you can use the following command to install these two modules:

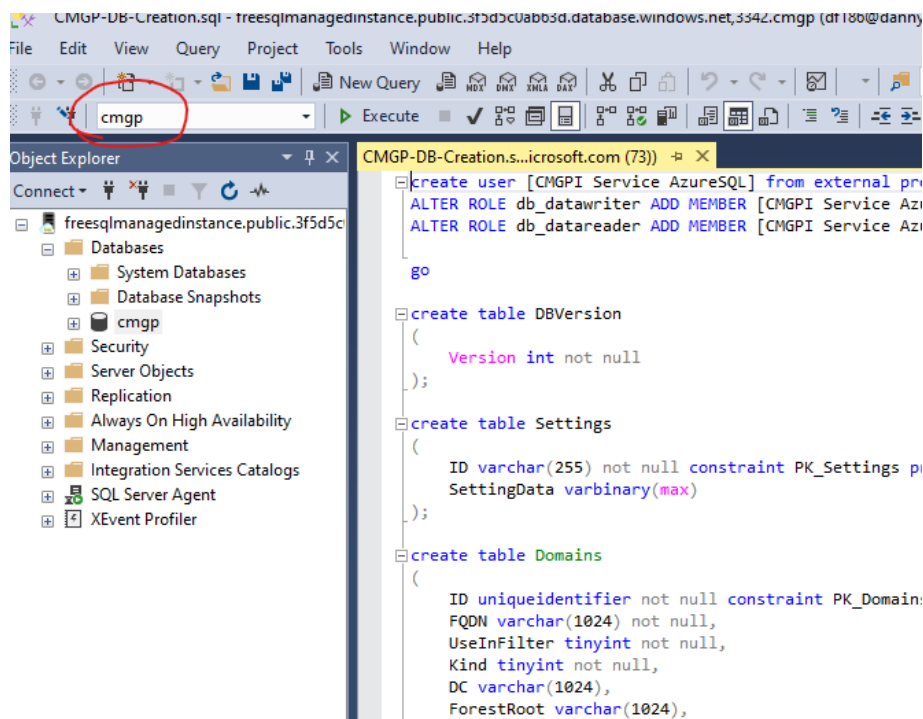
Install-Module Az.Accounts,Az.Resources

You’ll receive some prompts to confirm the installations but after they have run and installed successfully you’re ready to run ConnectAzureSQL.ps1. This script requires two parameters to run—your Entra ID “Tenant Id” and the Account ID of the user who has permissions in Entra to create application registration objects. Namely, you must provide the login ID of that account. The login ID is typically the user principal name (UPN) of the user, which is used to log into Entra.

Once the “ConnectAzureSQL.ps1” script has completed successfully, go to SQL Server Management Studio and connect to your Azure SQL Database as shown in the example below:



Ensure that you select your target database that you pre-created first before running the script that was saved to the desktop during the CMGPI installation.



This process supports both Azure SQL Database as well as Azure SQL Managed Instance. Depending on which Azure License you have, it may be necessary to grant Admin privileges to the database or database instance to the Entra application created by the ConnectAzureSQL.ps1 script above. For more information on how to do this, please see <https://learn.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?view=azuresql&tabs=azure-powershell>.

Migrating from one Azure SQL Database to another

If you are migrating your Azure SQL database to another Azure SQL database, this can be easily done using the "Maintenancetool.exe" utility found in c:\program files\sdm software\cmgpi\svc. This utility provides a number of functions but one of those is to change the connection string of the database that CMGPI is currently configured to use. Below is a sample command to do so:

MaintenanceTool.exe connection db set String: Server=tcp:publicdatabaseurl,port;Initial Catalog=databasename; Authentication=Active Directory Service Principal;Persist Security Info=False;Connect Timeout=30;Encrypt=True;TrustServerCertificate=False"

Once completed, remember to start the CMGPI Server service.

(Please see Appendix C: Modifying CMGPI Application Configuration in the CMGPI User Guide for more information on the MaintenanceTool utility.)

Initial Configuration

After installation, you'll need to log in to the CMGPI web user interface to configure the product.

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 targeted at CMGPI. Or, from a default installation, browsing to <https://<CMGPI Server Name>> should launch the application.

*CMGPI has been tested with current Chrome and Microsoft Edge browser versions.
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:

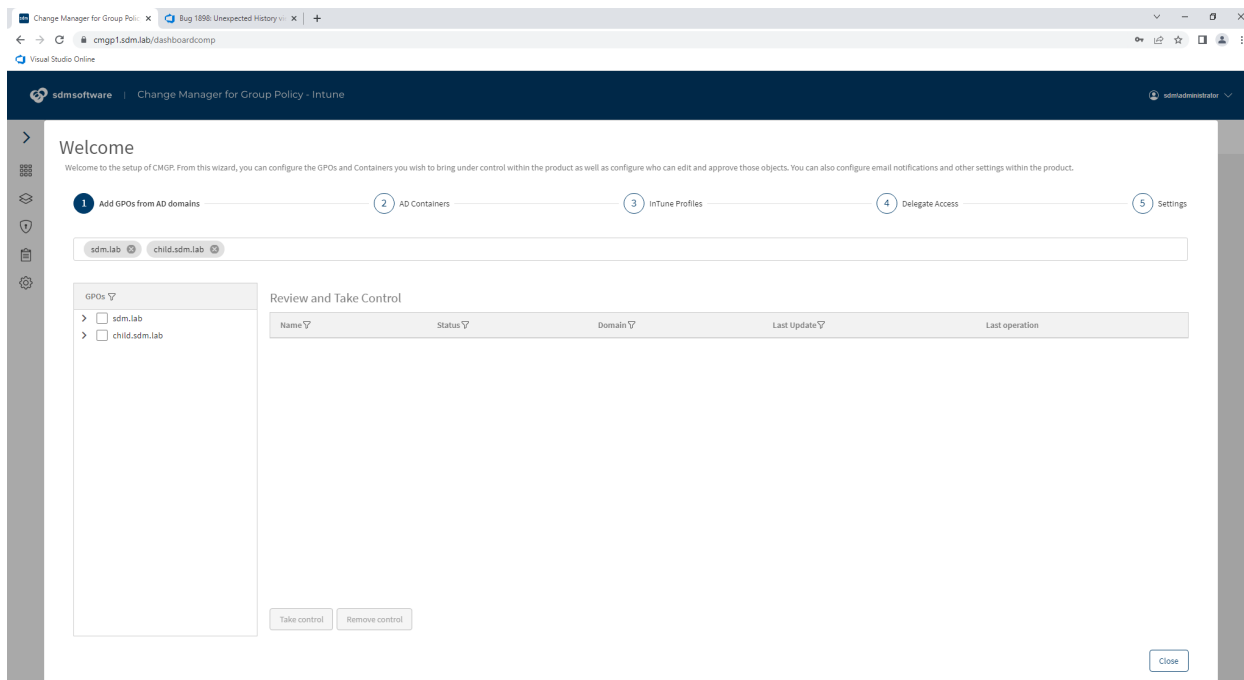


Figure 8: The CMGPI Welcome Wizard

The wizard provides you with a way of setting up the initial product configuration.

If you don't want to use the wizard, you can safely close it at this point and then set all the individual options in the product from the main Settings menu.

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, domains, 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 script needs to have been run prior to using this wizard or you will have needed to configure Intune connectivity from the Settings menu. Without this, 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. You can also do this from the Delegation, Objects menu
- **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** in the **CMGPI User Guide** for more details) 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. Note that the connection to Intune must be in place before you can take control of Intune Configuration Profiles. You can either do this using the provided ConnectIntune.ps1 script (described in Appendix F of the CMGPI User Guide) or from the Settings\Intune menu when logged in as a Product Administrator.

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, including child domains or domains in other domain trees. They are not added automatically, as is shown in Figure 9 below:

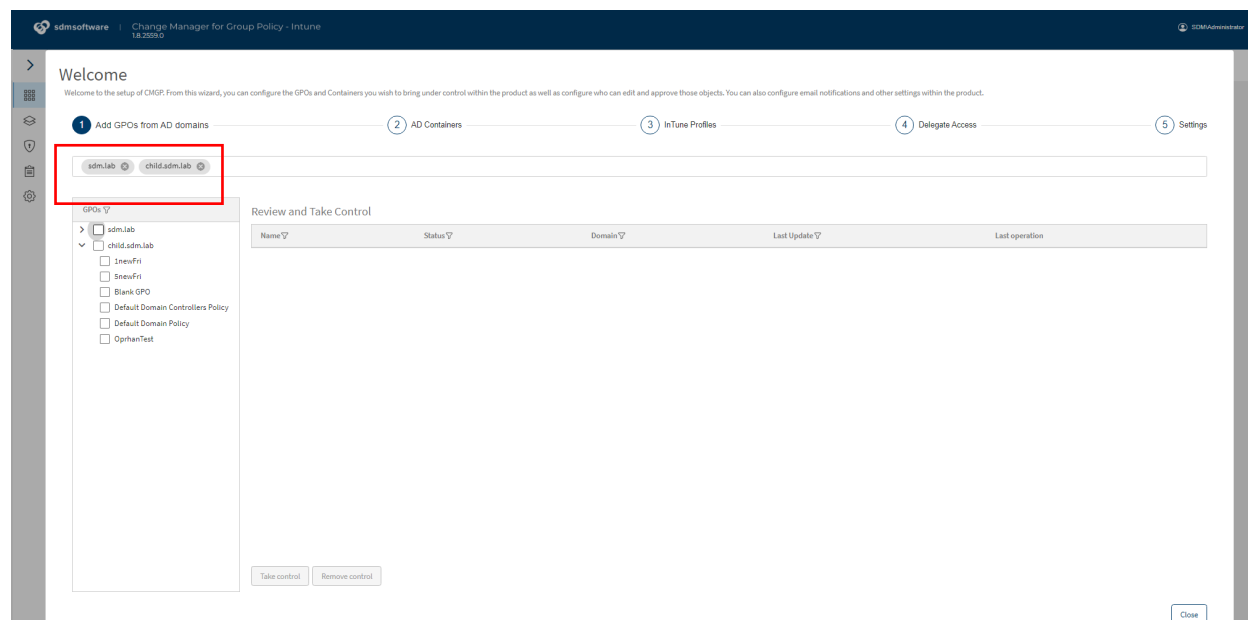


Figure 9 Adding domains to manage in CMGPI

Once you add a DNS domain name and press Enter, 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**

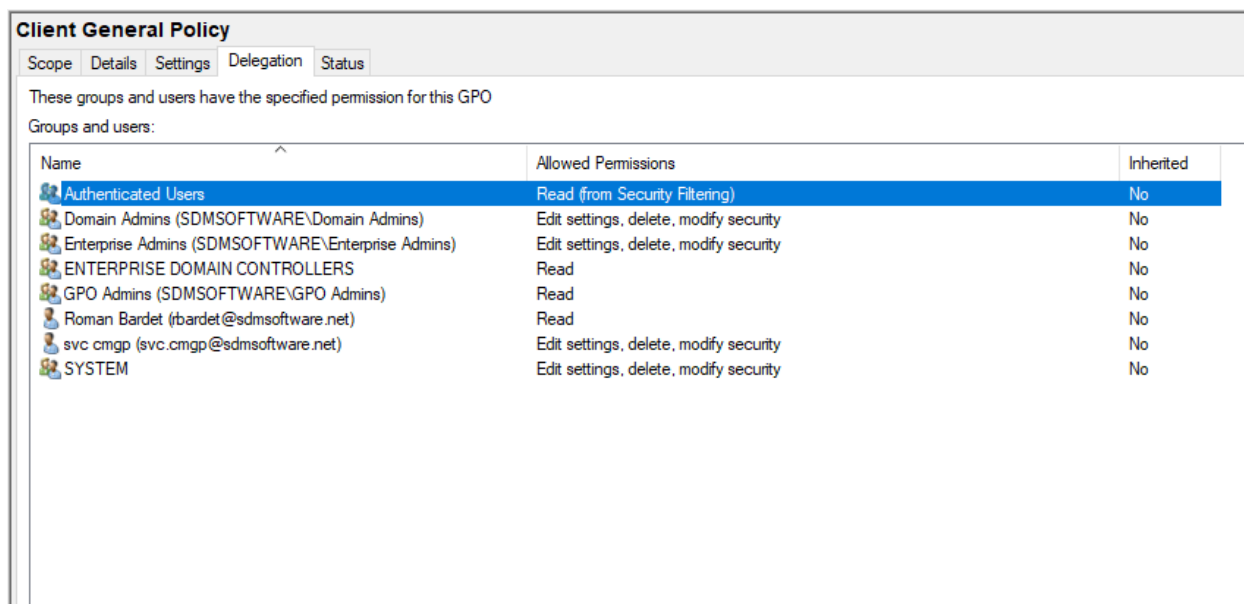
These three Access Control Entries (ACEs) will remain after a Take Control operation is performed. However, if a "discretionary" user principal was added to the GPO's delegation that grants either "Edit Settings" or "Edit Settings, Delete, Modify Security" permissions on that GPO, that user principal's 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 one or more GPOs.

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



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 below.

*The Take Control process can take a while as CMGPI is performing a set of tasks such as backing up the GPO, indexing its settings for our settings search feature and related tasks. We **don't** recommend taking control of 100s of GPOs at once, but rather to perform the operation in batches to limit the time that the product is busy performing the Take Control operation.*

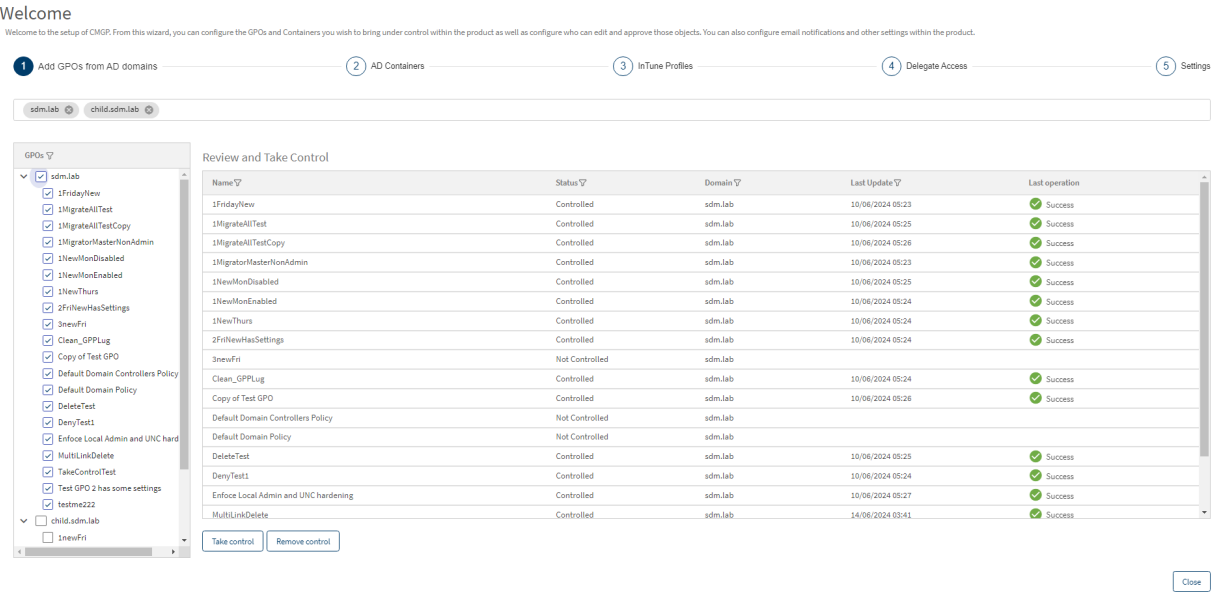


Figure 12 Taking control of GPOs

Any issues that appear will be shown as either “Warning” or “Failed” in the Last Operation column. You can click on the status to see more details of the problem. Note that “Warnings” usually don’t prevent the take control operation but may provide useful information. For example, if we encounter a GPO with orphaned SIDs in its delegation list, we will declare that as a warning for you to be aware of.

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:

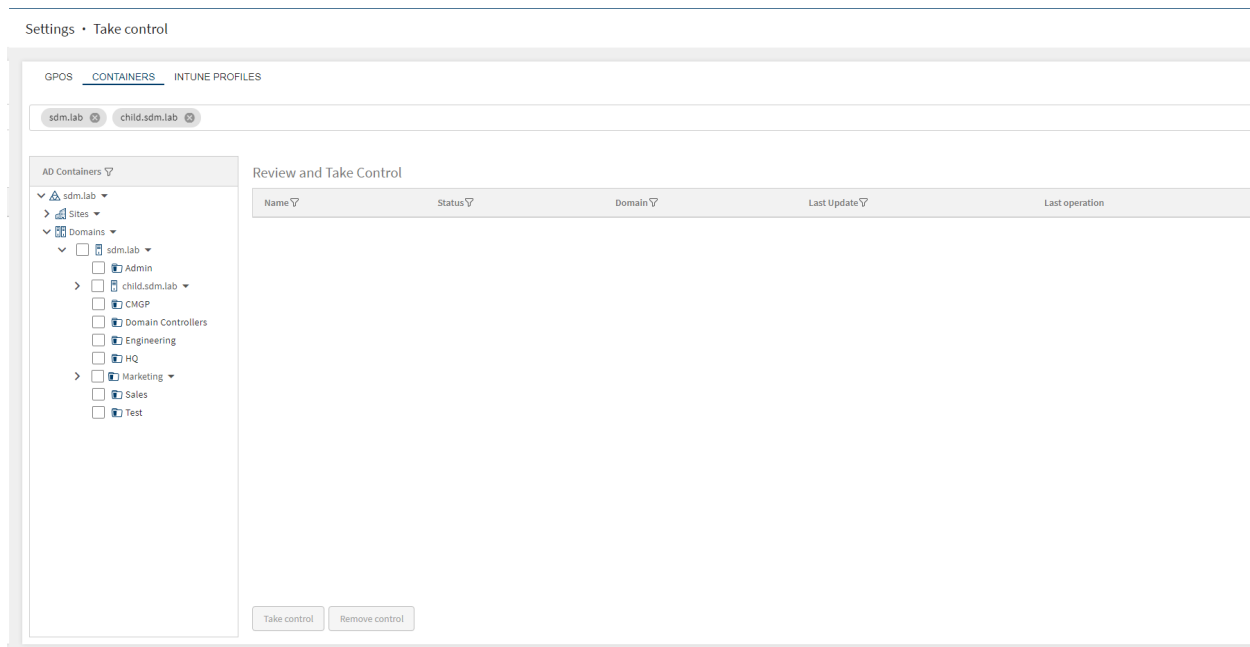


Figure 13 Selecting AD Containers to Take Control of

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:

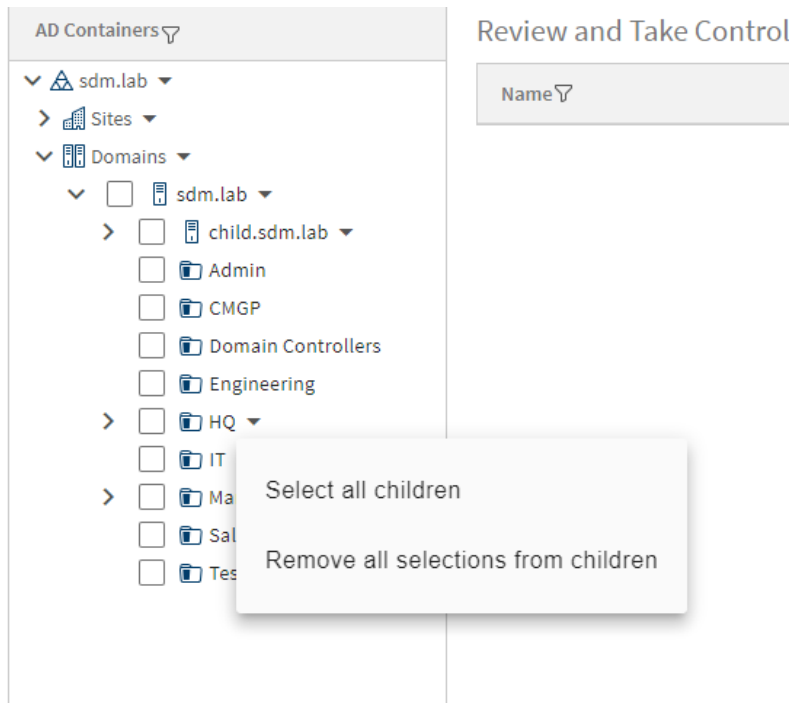
Cpandl.com

```

|
OU—AMERICAS
|
Domain - Child.cpandl.com
|
|
|
OU – Marketing

```

Select Sites, Domains and OUs that you wish to take under control by checking the boxes next to each node in the tree. Note that some nodes—those with child nodes underneath, contain an arrow (▼) symbol next to the name of the container. If you select that symbol, you'll have the option of selecting all child nodes underneath the parent or excluding all child nodes, as shown here:



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).

GPOS CONTAINERS INTUNE PROFILES

sdm.lab child.sdm.lab

AD Containers ▾

- sdm.lab ▾
 - Sites ▾
 - Marin
 - NewYark
 - Domains ▾
 - sdm.lab ▾
 - Admin
 - child.sdm.lab ▾
 - Domain Controllers
 - Regional
 - Sales
 - CMGP
 - Domain Controllers
 - Engineering
 - HQ
 - Marketing ▾
 - Sales
 - Test

Review and Take Control

Operation in progress. 6 of 12 objects completed

Name ▾	Status ▾	Domain ▾	Last Update ▾	Last operation
Marin	Controlled			Success
NewYark	Controlled			Success
sdm.lab		sdm.lab		
child.sdm.lab		child.sdm.lab		
Regional		child.sdm.lab		
Users	Controlled	child.sdm.lab		Success
Sales	Controlled	child.sdm.lab		Success
Engineering	Controlled	sdm.lab		Success
HQ		sdm.lab		
Marketing		sdm.lab		
Users		sdm.lab		
Sales	Controlled	sdm.lab		Success

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 uncheck 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.

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.

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

Entra ID connected

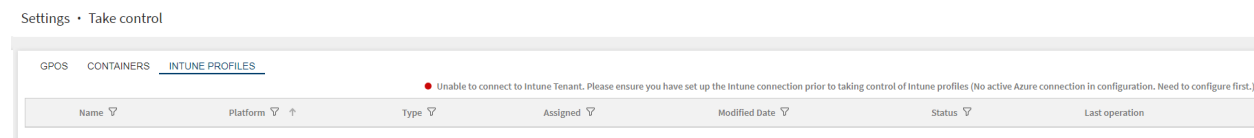
<input type="checkbox"/>	Name ▾	Platform ▾	Type ▾	Assigned ▾	Modified Date ▾	Status ▾	Last operation
<input type="checkbox"/>	1bedafad-973d-48d9-aa62-10414fad54b	macOS	Shell script	No		Not Controlled	
<input type="checkbox"/>	1fb8deaa-e47c-4abd-ac45-d8bd29381b3	Windows 10 and later	PowerShell script	No		Not Controlled	
<input type="checkbox"/>	257afaf8d-9ed9-45ca-ad4c-1bd33baf9f16	macOS	Shell script	No		Not Controlled	
<input type="checkbox"/>	57cd4e12-d961-4a73-870d-01591cd96d6f	Windows 10 and later	Administrative Templates	No		Not Controlled	
<input type="checkbox"/>	5ed96253-e32c-4093-9034-e1037586cfe9	Android (AOSP)	Template	No		Not Controlled	
<input type="checkbox"/>	60c2482c-c785-4f62-98cf-ec23e23f1d76	Windows 10 and later	Administrative Templates	No		Not Controlled	
<input type="checkbox"/>	62bab183-f9f1-433b-b449-7b2446478a8	Android (AOSP)	Template	No		Not Controlled	
<input type="checkbox"/>	6383e6d9-3f8f-4c0f-b311-7b0600340939	Windows 10 and later	Administrative Templates	No		Not Controlled	
<input type="checkbox"/>	6552f639-f7c4-4f8b-8530-df1c2ff03110	iOS/iPadOS	Settings Catalog	No		Not Controlled	
<input type="checkbox"/>	6da5530b-a83b-40e1-4b59-98889860748d	iOS/iPadOS	Settings Catalog	No		Not Controlled	
<input type="checkbox"/>	778d9a57-5b05-43c1-b146-98e2cc8da123	Windows 10 and later	Administrative Templates	No		Not Controlled	
<input type="checkbox"/>	8bda6036-b086-4347-87d6-c5cd5f2559f	Windows 10 and later	PowerShell script	No		Not Controlled	
<input type="checkbox"/>	8d98e20b-e14d-44c8-b711-0e60c4096a46	iOS/iPadOS	Settings Catalog	No		Not Controlled	

Take control Remove control

Close

Prior to configuring Intune support, either through the included PowerShell script or via the Settings, Intune dialog, you will see the following when you try to take control of Intune profiles—this is perfectly normal until that configuration is complete. Note that once you configure the connection to Intune,

there may be a delay in populating this screen while CMGPI is querying Intune via the Microsoft Graph API. This should take no more than a few minutes.



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.

*CMGPI currently does not support creation of **new** Intune Configuration Profiles from within the platform. This is planned for an upcoming release.*

Now that we've taken control of both GPOs, containers and Intune Profiles, we need to delegate access to those controlled objects. This can be done using Step 4—Delegate Access in the Welcome Wizard or from the Delegation, Objects menu after the wizard has closed.

Delegate Access

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

Enabling 3-level Approval in CMGPI

Note that starting in version 1.9, CMGPI supports 3 levels of approval for changes: Editor, Approver and Deployer. The new Deployer role separates what was previously combined in the Approver role. It means that you can have 3 distinct levels of approval for edit, approving and finally, deploying object changes. This 3-level approval is **not** enabled in the product by default. You can enable it using the following steps:

1. Open an elevated command prompt on the CMGPI server, running an AD account with the product administrator role.
2. Change directories to: C:\Program Files\SDM Software\CMGPI\Svc
3. Run the following command: **maintenancetool deployer_role enable**
4. Once that succeeds run **maintenancetool deployer_role check** to ensure it's enabled

Note that this operation is a one-time, one-way process. Once enabled, it cannot be disabled. Also, once it's enabled all objects under control by CMGPI will need to specify an editor, approver and deployer role.

Editor, Approver and Deployer Capabilities

Editors have the following capabilities:

- Check out GPOs, containers or Intune profiles for change
- View the history of a GPO, container or Intune profile and view their current settings
- 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
- Search for settings within any GPO or Intune profile under control by CMGPI
- Check in GPOs, containers and Intune Profiles after a change
- Undo 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
- Delete a GPO

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
- View the history of a GPO, container or Intune profile and view their current settings
- Search for settings within any GPO or Intune profile under control by CMGPI
- View differences between current and prior versions of GPOs, containers or Intune Profiles

Deployers have the following capabilities:

- View the history of a GPO, container or Intune profile and view their current settings
- Search for settings within any GPO or Intune profile under control by CMGPI
- View differences between current and prior versions of GPOs, containers or Intune Profiles
- Deploy immediately or schedule a GPO, container or Intune Profile change for deployment
- Cancel a scheduled GPO, container or Intune Profile scheduled deployment

To proceed, select Step 4--Delegate Access from the Welcome Wizard or Delegation, Objects from the product main menu. You will see a list of the objects (GPOs, Containers, and Intune Profiles) that you have delegated from Steps 1, 2 & 3, along with three columns for selecting Approvers Editors and Deployers, as shown in Figure 15.

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.



List of Objects:

<input type="checkbox"/>	Name ▾	Type ▾	Canonical Name ▾	Approver(s) ▾	Editor(s) ▾	Deployer(s) ▾
<input type="checkbox"/>	Regional	OU	child.sdm.lab/Regional	sdm\mbaker	Add users or groups...	sdm\test2
<input type="checkbox"/>	DarrenTestSettingsCatalog	Intune Profile	Windows 10 and later/Settings Catalog/DarrenTestSettingsCatalog	sdm\mbaker	Add users or groups...	sdm\test2
<input type="checkbox"/>	Marin	Site	sdm.lab/Configuration/Sites/Marin	sdm\mbaker	Add users or groups...	sdm\test2
<input type="checkbox"/>	Sales	OU	child.sdm.lab/Sales	sdm\mbaker	Add users or groups...	sdm\test2

Figure 15 Delegating access to GPOs and Containers

You have two ways you can add editors, approvers and deployers. 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:

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 Intune Profiles 4 Delegate Access 5 Settings

3 Items selected <input checked="" type="checkbox"/> Assign Approvers <input checked="" type="checkbox"/> Assign Editors <input checked="" type="checkbox"/> Assign Deployers						
<input type="checkbox"/>	Name ▾	Type ▾	Canonical Name ▾	Approver(s) ▾	Editor(s) ▾	Deployer(s) ▾
<input checked="" type="checkbox"/>	Regional	OU	child.sdm.lab/Regional	sdm\mbaker	Add users or groups...	sdm\test2
<input checked="" type="checkbox"/>	DarrenTestSettingsCatalog	Intune Profile	Windows 10 and later/Settings Catalog/DarrenTestSettingsCatalog	sdm\mbaker	Add users or groups...	sdm\test2
<input checked="" type="checkbox"/>	Marin	Site	sdm.lab/Configuration/Sites/Marin	sdm\mbaker	Add users or groups...	sdm\test2

Figure 16

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

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

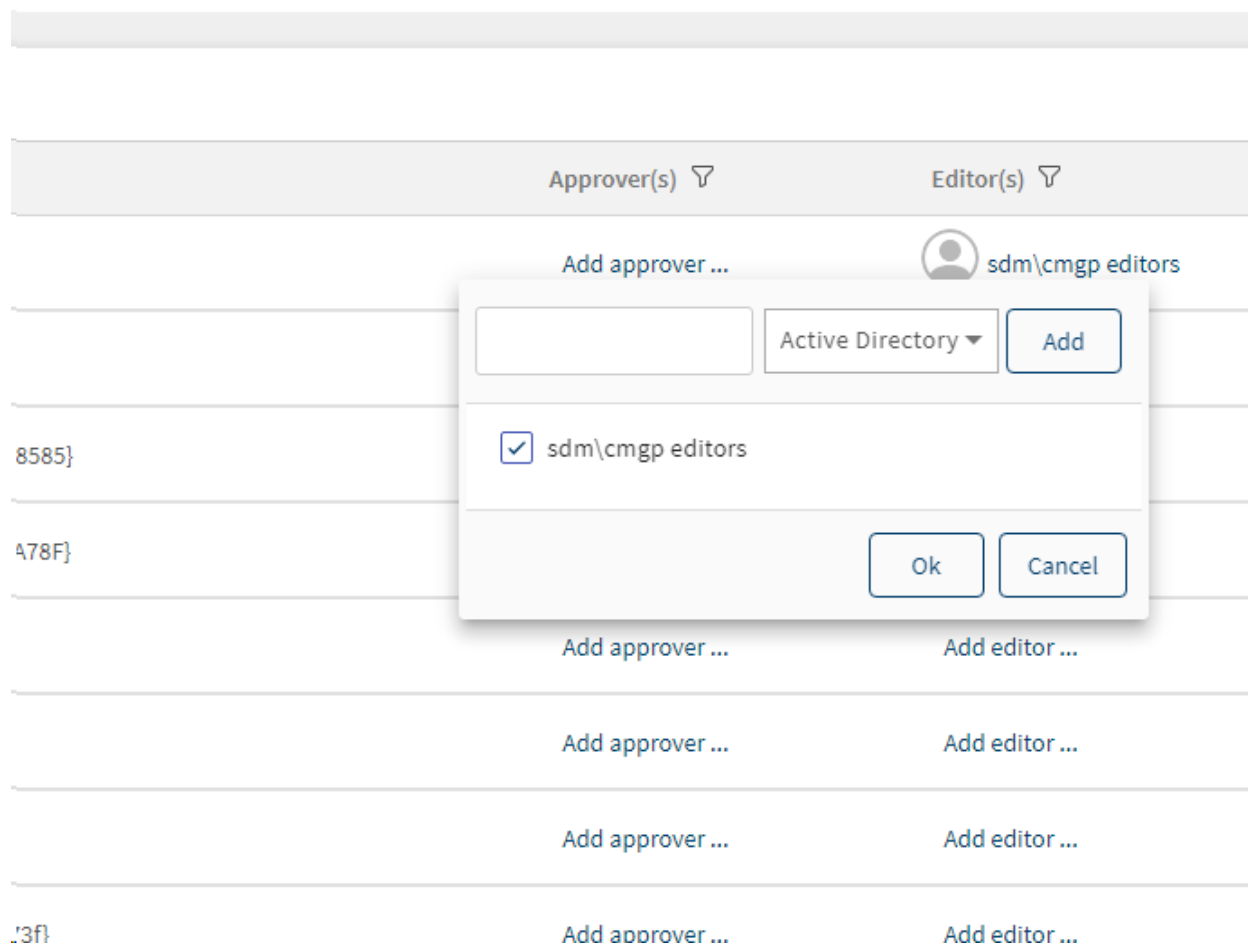


Figure 17

When entering a deployer, 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 SDM\CMGPI editors group as an approver for this object. As you're typing into the box, you will get hints as the system looks up users or groups that exist in AD or Entra ID. You can select these hints to ensure you've selected the correct object. Note that if you've configured Entra ID SSO (see [Configuring Entra SSO from the UI](#) below) you will have an extra drop-down to choose whether you want to add an AD or Entra ID user or group here. Once the user or group name is entered, press the Add button to add the object and then press OK to check that you've entered the object correctly, and 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 user or groups as editors, approvers and deployers or, if Entra ID SSO is enabled, then Entra users or groups. In the case of groups, the user's group membership will be evaluated at logon time and their managed objects calculated. For Intune Profiles, even when you are entering an AD domain and user name as

editor and approver, when it comes time to edit an Intune Profile, you'll always be authenticating to Entra ID using the corresponding synchronized Entra ID credential.

You do not need to assign editors, approvers and deployers 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 deployers, 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 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 Intune Profiles 4 Delegate Access 5 Settings

Default approver(s): sdm\cmgp approvers

Default deployer(s): sdm\cmgp deployers

☐ Require comments on object check-in

☐ Select to enforce naming conventions for GPOs

GPO naming rule:

Audit events lifetime: 60 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 that are newly created using CMGPI. In this case, a user or member of a default approver group will be able to approve a given GPO change for newly created GPOs.
- **Default Deployers:** This allows you to set one or more users or groups as default deployers who are automatically assigned to GPOs that are newly created using CMGPI. In this case, a user or member of the default deployer group will be able to deploy a given GPO change for newly created GPOs.

- **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.
- **Select to enforce naming conventions for GPOs:** If this box is checked, you can provide a naming standard to enforce on GPOs whenever a new GPO is created or an existing GPO is renamed. This naming standard expects a regular expression (regex) to enforce the naming standard.
- **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.

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.

Configuring Intune Connectivity from the UI

You can configure connectivity to manage Intune configuration profiles right from the CMGPI UI. A Product Administrator can configure this connectivity from the Settings, Intune menu option, as shown in the figure below:

sdmsoftware | Change Manager for Group Policy - Intune 1.8.2559.0

Settings • InTune connection settings

Enter InTune connection settings

☐ Enable InTune connection

Directory (tenant) ID:

Primary Domain name:

Application (client) ID:

Secret:

Secret ID:

Secret expiration date: 6/11/2024, 14:16:36

Figure 19 Configuring Intune Connectivity

Before you can enable Intune connectivity from this screen, you will need to create an application registration object within your Entra ID Portal. This object will need the Graph API permissions described above in the section on [Intune Change Control Requirements](#). Once you define the correct permissions and provide admin consent for the application, you'll need to enter the relevant details in the screen above, including your Entra ID tenant ID, the primary domain name of the tenant, the application registration's client ID and the secret ID and secret value of the secret you created on the application. When you press the **Test** button, the connection to Intune will be validated (and the secret expiration date will be updated to reflect to actual secret expiration). Make sure to press the **Save** button to save the configuration. Ensure that the Save button changes its status to greyed out, which confirms that the configuration was saved. This may take a few seconds. Once the configuration is saved, if you navigate to Settings, Take Control and choose the Intune Profile tab, you should see Intune profiles populate in the list. This could take a few minutes to populate from your tenant.

Configuring Entra SSO from the UI

CMPGI supports Single Sign On (SSO) using Entra ID users and groups. This means that you can now configure both global product roles and object-specific editor and approver roles with Entra ID users or groups instead of AD ones. If you choose to enable Entra ID SSO, you can still use AD users and groups as

well, but you may find that this gets confusing. We recommend choosing one or the other for delegating access to the product. In order to configure Entra ID SSO support, you have two options, similar to Intune. CMGPI provides a PowerShell script, found in C:\Program Files\SDM Software\CMGPI\Svc on the CMGPI server called **ConnectEntraID.ps1**. This script creates the required Enterprise Application and associated secret to enable SSO connectivity within CMGPI. More details of running the script can be found in Appendix G of the CMGPI User Guide.

The other way to configure SSO is to do it through the CMGPI UI, from the Settings, SSO menu, as shown in the figure below:

sdmsoftware | Change Manager for Group Policy - Intune 1.8.2559.0

Settings • SSO

Select identity provider for SSO configuration.

Identity provider: Entra ID

Enter the following data for in the providers website.

Application (client) ID: 7e9f6e26-8ec

Directory (tenant) ID: 0c1894d05b3

Secret:

Secret Id: 07d9dfa3-a2...07

Secret expiration date: 6/10/2026, 17:00:00

Redirect URI: https://cmgp1.sdm.lab/

Test Save

Figure 20 Configuring SSO in CMGPI

In order to use this screen, you will need to have pre-created an enterprise application in your Entra ID tenant, with a defined secret. Note that the redirect URL should generally point to the CMGPI URL itself.

Once you've configured SSO settings, you can **Test** the connectivity to ensure it works, and **Save** the connection information, which will update the Secret expiration date in the UI above. Once you've configured SSO, the next time you log into the CMGPI web application, you'll see the following new option:




Change Manager for Group Policy - Intune

Domain\user name

Password

Sign in

 Sign in with Windows Authentication


 Sign in with Entra ID

Figure 21 CMGPI configured with Entra ID SSO

You'll need to assign global or per-object roles to Entra ID users before they can log in using their Entra ID credentials, but once you've done so, press the "Sign in with Entra ID" button and the familiar Azure sign-on prompt will appear and allow you to enter your Entra ID user name and password.

Configuring SSL on the CMGPI Server

When you install CMGPI, it installs a self-signed certificate for the web server. The CMGPI service itself also uses the certificate to secure communication to it. So when you have to change the SSL certificate for the application, you need to change it for both the web server and the CMGPI service. In order to facilitate this, we've provided a PowerShell script called **AddressHostname.ps1** to perform the operation. **Appendix E** in the **CMGPI User Guide** details how to use the script to perform this operation.

Appendix A: Command-Line Installation Reference

This section provides detailed command-line instructions for installing CMGPI silently. This installation method is intended for advanced users already familiar with the product and who want to automate the setup.

Before initiating the command-line installation, ensure the target server meets [software and hardware requirements](#).

Note: We recommend using the Command Prompt (CMD) for executing product installation rather than a PowerShell session.

To automate installation of CMGPI with MS SQL Database:

1. Extract the contents of the CMGPI bundle to a desired location on the target server:

```
CMGPI.exe /extract c:\temp
```

2. Install the following modules from the unpacked bundle:

- Microsoft Application Request Routing 3.0

```
msiexec /i c:\temp\requestRouter_amd64.msi /qn /l*x c:\temp\request_router_installation.log
```

- IIS URL Rewrite Module 2

```
msiexec /i rewrite_amd64_en-US.msi /qn /l*x c:\temp\rewrite_module_installation.log
```

3. Run the CMGPI installer with the following parameters:

```
msiexec /i c:\temp\CMGPI.msi ^
```

```
USER_NAME="<proxy account user name>" USER_PASSWORD="<proxy account password>" ^
```

```
RADIOBUTTONGROUP_DBOPTIONS_PROP="<create data base initialization script for SQL server>" ^
```

```
DB_GEN_SCRIPT_FILE_NAME="c:\temp\cmgpi_create_db.sql" ^
```

```
SQL_SERVER_INSTANCE_PROP="<name of the SQL server instance>" ^
```

```
SQL_SERVER_PORT_PROP=1433 ^
```

```
SKIP_IIS_REWRITE_MODULE=1 SKIP_REQ_ROUTER_MODULE=1 ^
```

```
USE_SETTINGS_BACKUP=false ^
```

```
/qn /l*x c:\temp\cmgpi_installation.log
```

Note: If you are using a group Managed Service Account (gMSA) leave the password field blank here and enter the gMSA username with a \$ symbol at the end (e.g. *mydomain\gMSAAccount\$*).

4. Use SQL Server Management Studio to execute the SQL script located at *c:\temp\cmgpi_create_db.sql* (requires the user account with the *database admin* role). This script will create the SQL database for CMGPI.

5. Start the CMGPISvc service:

```
sc start CMGPISvc
```

To automate installation of CMGPI with Azure SQL Database:

1. Extract the contents of the CMGPI bundle to a desired location on the target server:

```
CMGPI.exe /extract c:\temp
```

2. Install the following modules from the unpacked bundle:

- Microsoft Application Request Routing 3.0

```
msiexec /i c:\temp\requestRouter_amd64.msi /qn /! *x c:\temp\request_router_installation.log
```

- IIS URL Rewrite Module 2

```
msiexec /i rewrite_amd64_en-US.msi /qn /! *x c:\temp\rewrite_module_installation.log
```

3. Run the CMGPI installer with the following parameters:

```
msiexec /i c:\temp\CMGPI.msi ^
```

```
USER_NAME="<proxy account user name>" USER_PASSWORD="<proxy account password>" ^
```

```
RADIOBUTTONGROUP_DBOPTIONS_PROP="<create data base initialization script for Azure SQL server>" ^
```

```
DB_GEN_SCRIPT_FILE_NAME="c:\temp\cmgpi_create_db.sql" ^
```

```
SQL_SERVER_INSTANCE_PROP="<name of the Azure SQL Server instance >" ^
```

```
SQL_SERVER_PORT_PROP=1433 ^
```

```
SKIP_IIS_REWRITE_MODULE=1 SKIP_REQ_ROUTER_MODULE=1 ^
```

```
USE_SETTINGS_BACKUP=false ^
```

```
/qn /! *x c:\temp\cmgpi_installation.log
```

Note: If you are using a group Managed Service Account (gMSA) leave the password field blank and enter the gMSA username with a \$ symbol at the end (e.g. *mydomain\gMSAAccount\$*).

4. Configure the necessary credentials for accessing the Azure SQL database using the MaintenanceTool utility:

```
cd "C:\Program Files\SDM Software\CMGPI\Svc"
```

```
MaintenanceTool.exe connection azure set "<tenant id>" "<primary domain name>"  
"<application (client) id>" "<application secret>" "<application secret id>"
```

Please see Appendix C: Modifying CMGPI Application Configuration in the CMGPI User Guide for more information on the MaintenanceTool utility.

5. Execute the Azure SQL script located at *c:\temp\cmgpi_create_db.sql* using the MaintenanceTool utility. This script will create the Azure SQL database for CMGPI.

MaintenanceTool.exe db new "c:\temp\cmgpi_create_db.sql"

6. Start the CMGPISvc service:

sc start CMGPISvc