



SDM Software Change Manager for Group Policy

Version 1.0

Installation & User Guide

Revisions:

1.1.....May 31, 2022

1.0.....May 23, 2022

Contents

Overview	4
CMGP Architecture Overview.....	4
CMGP Components.....	4
Installation Requirements.....	5
Hardware	5
Software	5
Configuration/Security Rights Required.....	5
Installation.....	6
SQL Server Configuration.....	12
Initial Configuration.....	12
Taking Control of GPOs	14
The Take Control Process for GPOs.....	15
The Take Control Process for AD Containers.....	18
Delegate Access.....	20
Editor and Approver Capabilities.....	20
Settings.....	22
Using the Product.....	23
Product Roles	24
Product Administrator.....	24
GPO Creator.....	24
Break Glass.....	24
Auditor.....	25
CMGP Dashboard.....	25
CMGP Navigation.....	26
The Change Control Process	28
Editing GPOs.....	30
Editing Containers.....	38
Audit Log.....	41
Licensing.....	41

Appendix A: Using the SetCMGPPermissions.exe to grant initial permissions required by CMGP	43
Appendix B: Customizable settings within CMGP	45
Appendix C: The CMGP PowerShell Module	46

Overview

SDM Software's Change Manager for Group Policy (CMGP) brings modern Group Policy change management processes to all organizations that leverage GP to configure and secure their Windows systems. Change Manager for GP provides web-based workflow to allow you to delegate control of GPO editing and GPO linking to appropriate personnel to ensure the security and integrity of your Group Policy environment. CMGP can be installed and made functional within minutes of downloading. In this document, we'll describe the requirements to install, configure and use the CMGP product, as well some best practices for doing so.

CMGP Architecture Overview

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

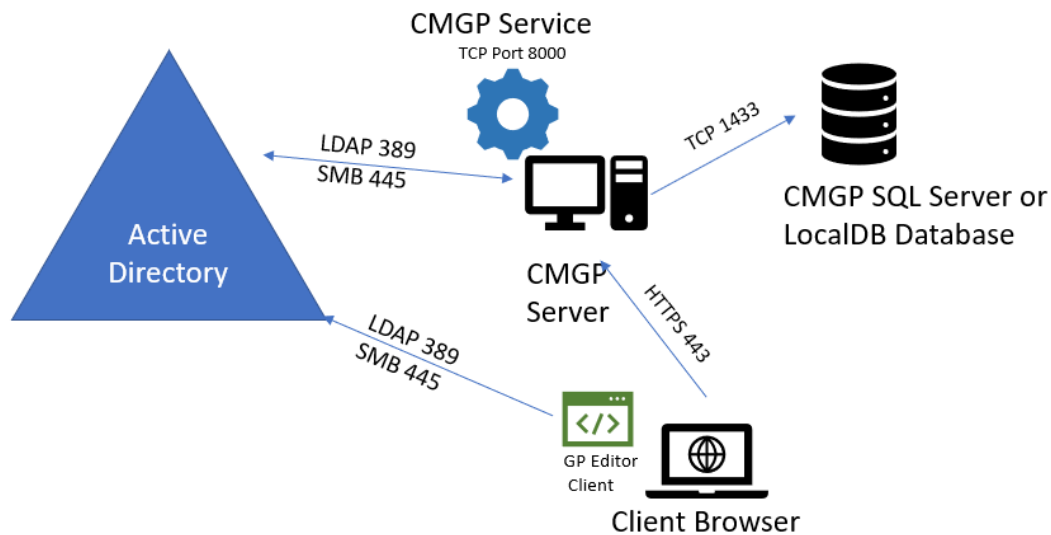


Figure 1: the CMGP Architecture

CMGP Components

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

- **CMGP Server:** The main application server for CMGP, which is composed of the CMGP web application, running on IIS and the **CMGP Service**, running as a Windows service.
- **CMGP Database:** This is the database store for CMGP. It can be co-located on the CMGP 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:** CMGP is a web-based app, supporting either Chrome or Microsoft Edge browsers. In order to edit GPOs, you will need 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 CMGP.

Installation Requirements

The CMGP installer provides a signed .msi file that will install aspects of the CMGP architecture needed for the CMGP server and database, as shown in Figure 1. There are several hardware, software and security configuration requirements for a successful CMGP 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 CMGP application server (more vCPU and memory allows for more concurrent users)

Software

- Windows Server 2012-R2, 2016, 2019 or 2022 required (CMGP should not be installed on a Domain Controller)
- .Net Framework 4.6 or greater
- Microsoft Group Policy Management Console (GPMC) feature installed
- 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 CMGP 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 CMGP installation)
- Microsoft IIS URL Rewrite Module 2

Configuration/Security Rights Required

- Service account for the CMGP application server. Service account can be either a regular AD account or a group Managed Service Account (gMSA). **Service account must have local administrator rights (i.e. a member of the local Administrators) on the CMGP server.**
- The CMGP 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 CMGP.) Here is the summary of permissions required in AD by the CMGP 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 CMGP 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 CMGP service account requires read and write access to the CMGP database.
- Any user who will be editing GPOs from the CMGP 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.

Installation

The CMGP installer is a signed .msiMSI 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 CMGP 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:

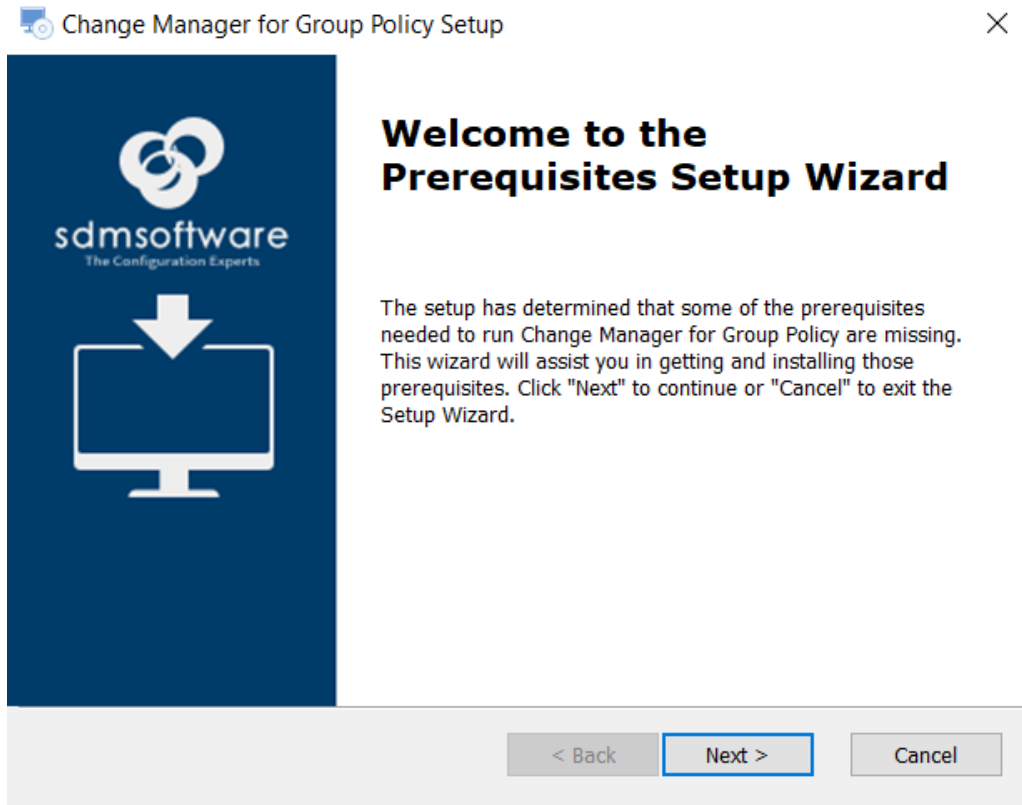


Figure 2

This only appears if you are indeed missing prerequisites that are required for CMGP 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 CMGP installation. This would be the case for small environments, or if you are just evaluating CMGP.

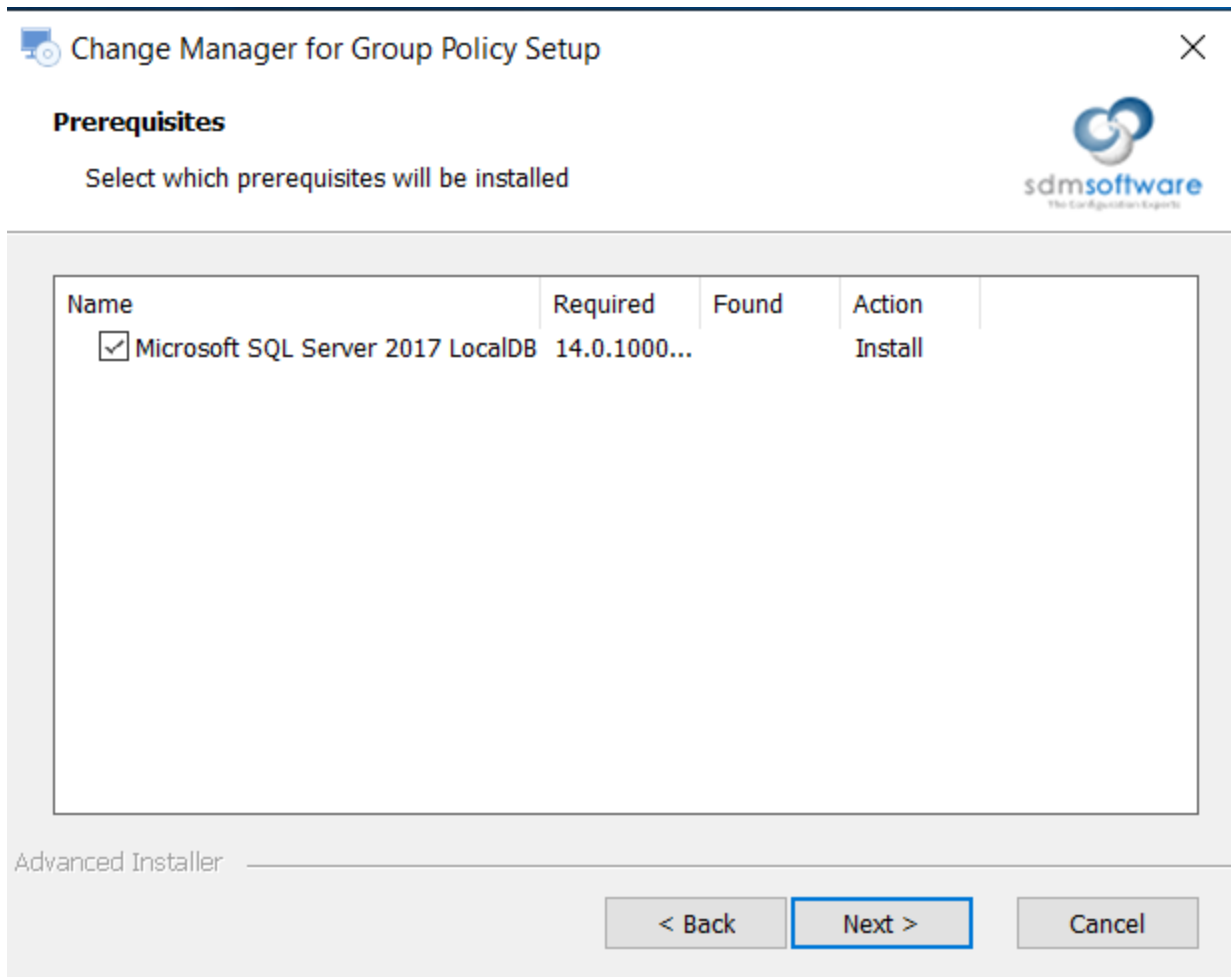


Figure 3

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 CMGP installation.

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

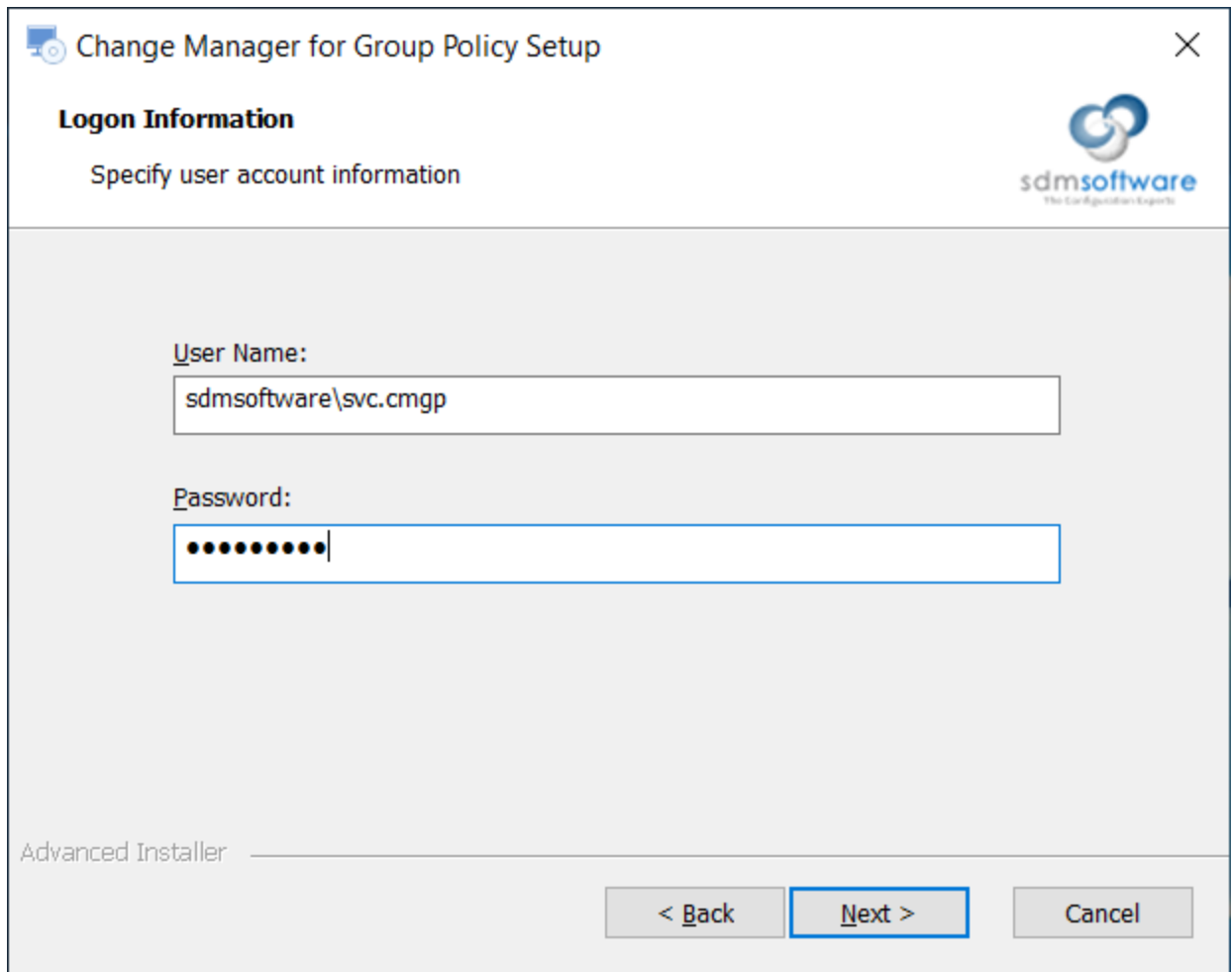


Figure 4

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 CMGP installer, as shown in Figure 5.

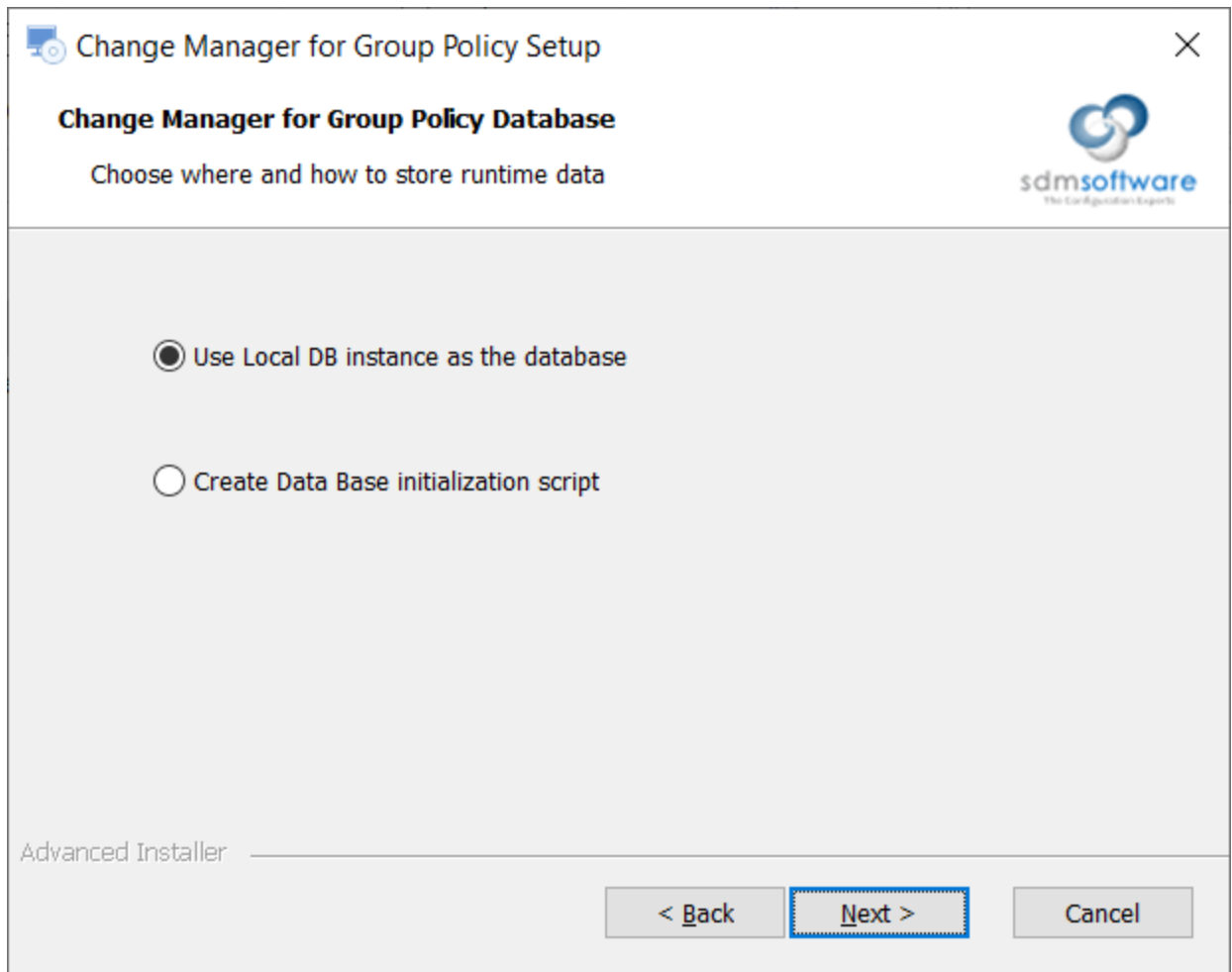


Figure 5

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 CMGP installer process, that you can use within Microsoft SQL Server Management Studio to create the CMGP 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:

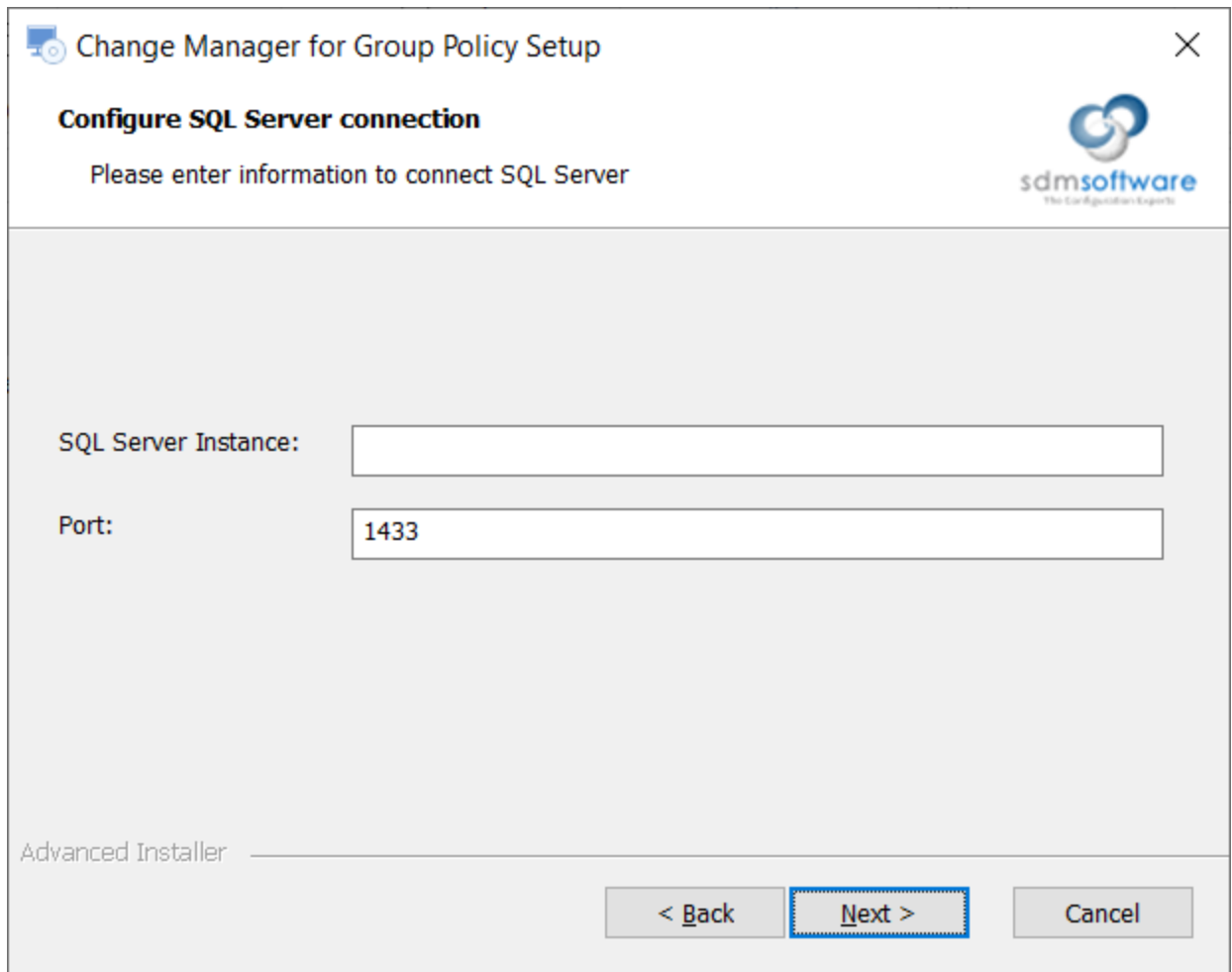


Figure 6

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 CMGP Service from the services control panel applet after the CMGP 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 CMGP installer installed a self-signed SSL certificate that is used to protect the CMGP 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 CMGP 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 CMGP 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 CMGP 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 **CMGP** and will grant your service account a login to the CMGP 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 CMGP server called "**SDM Software CMGP Service.**"

Initial Configuration

After installation, you'll need to log in to the CMGP web user interface to configure the product. To log into the product, double-click the "SDM Software Change Manager for Group Policy" web shortcut that was installed on the CMGP server desktop, to launch a browser target at CMGP. Or, from a default installation, browsing to <https://<CMGP Server Name>> should launch the application.

Note that CMGP has been tested with Chrome and Microsoft Edge browser. 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 CMGP product. You'll need to log in using domain-based credentials in the form of <domain\username> as shown in Figure 7 below:



Change Manager for Group Policy

Domain\user name

Password

Sign in

Figure 7

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

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.

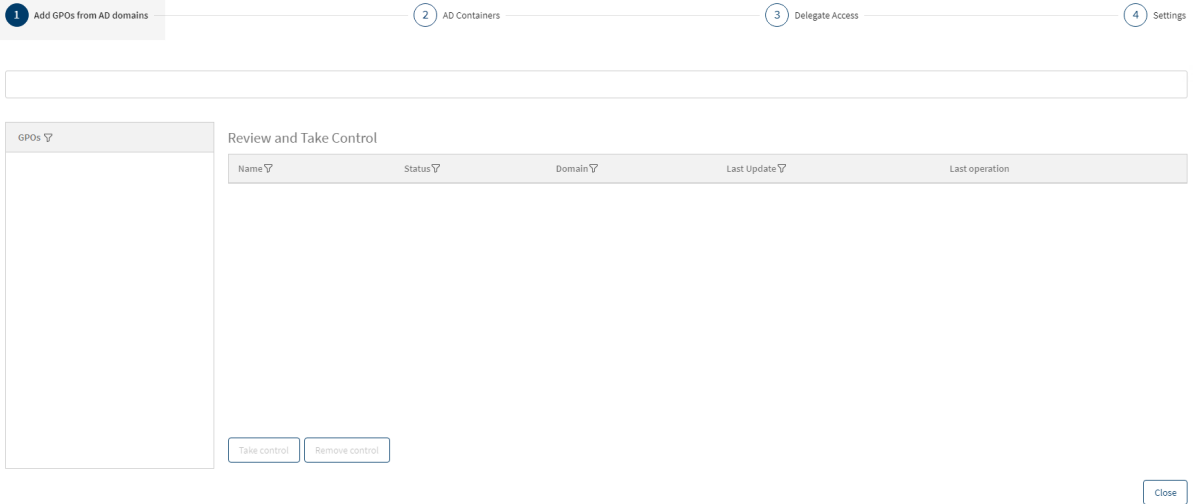


Figure 8: The CMGP Welcome Wizard

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

- **Add GPOs from AD Domains:** Allows you to take control of GPOs to be placed into change control within CMGP
- **AD Containers:** Allows you to take control of AD containers (sites, domain, or Organizational Units (OUs)) to be placed into change control within CMGP
- **Delegate Access:** Allows you to assign “editors” and “approvers” within CMGP 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 CMGP (see [Appendix A: Using the SetCMGPPermissions.exe to grant initial permissions required by CMGP](#)) or, if you don’t need to use a least privileged approach, you can place the CMGP 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.

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 or domains you wish to manage within CMGP. In the text box below step 1, enter the DNS name of any domain you wish to manage using CMGP. 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:

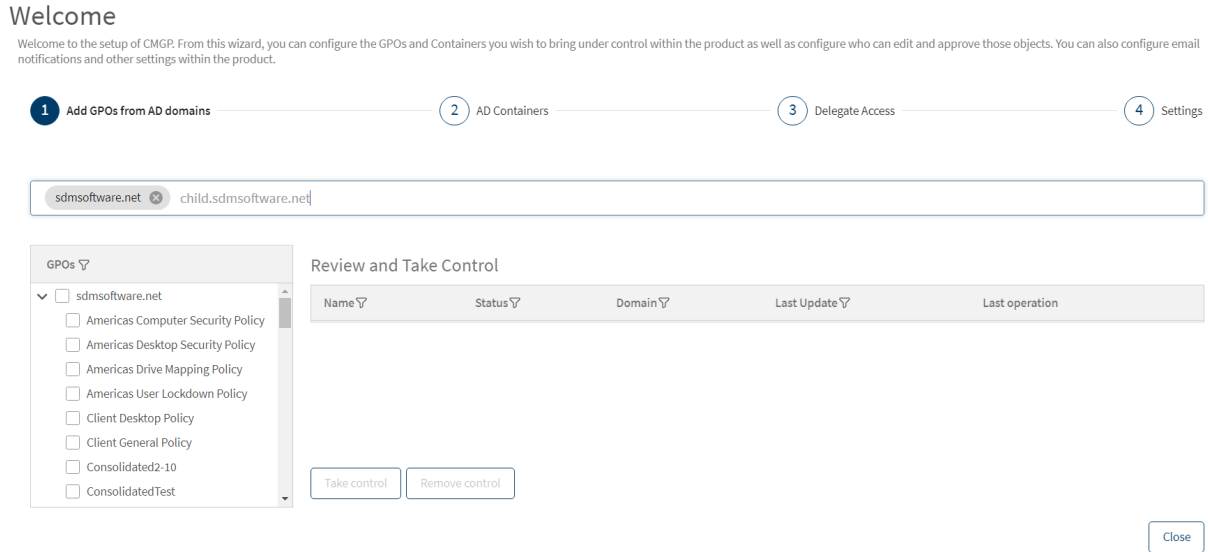


Figure 9 Adding domains to manage in CMGP

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 CMGP is a mechanism by which the permissions of that GPO are altered by the CMGP 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, those user principals 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@sdmsoftware.net)	Edit settings	No
svc cmgp (svc.cmgp@sdmsoftware.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 CMGP service account, in this example called svc.cmgp, 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@sdmssoftware.net)	Read	No
svc cmgp (svc.cmgp@sdmssoftware.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 CMGP.

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

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

sdmssoftware.net Type domain name

GPOs

- 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	sdmssoftware.net		Success
Americas Desktop Security Policy	Controlled	sdmssoftware.net		Success
Americas Drive Mapping Policy	Controlled	sdmssoftware.net		Success
Americas User Lockdown Policy	Controlled	sdmssoftware.net		Success
Default Domain Controllers Policy	Controlled	sdmssoftware.net		Success
Default Domain Policy	Controlled	sdmssoftware.net		Success
Client Desktop Policy	Controlled	sdmssoftware.net		Success
Client General Policy	Controlled	sdmssoftware.net		Success

Take control Remove control

Close

Figure 12 Taking control of GPOs

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:

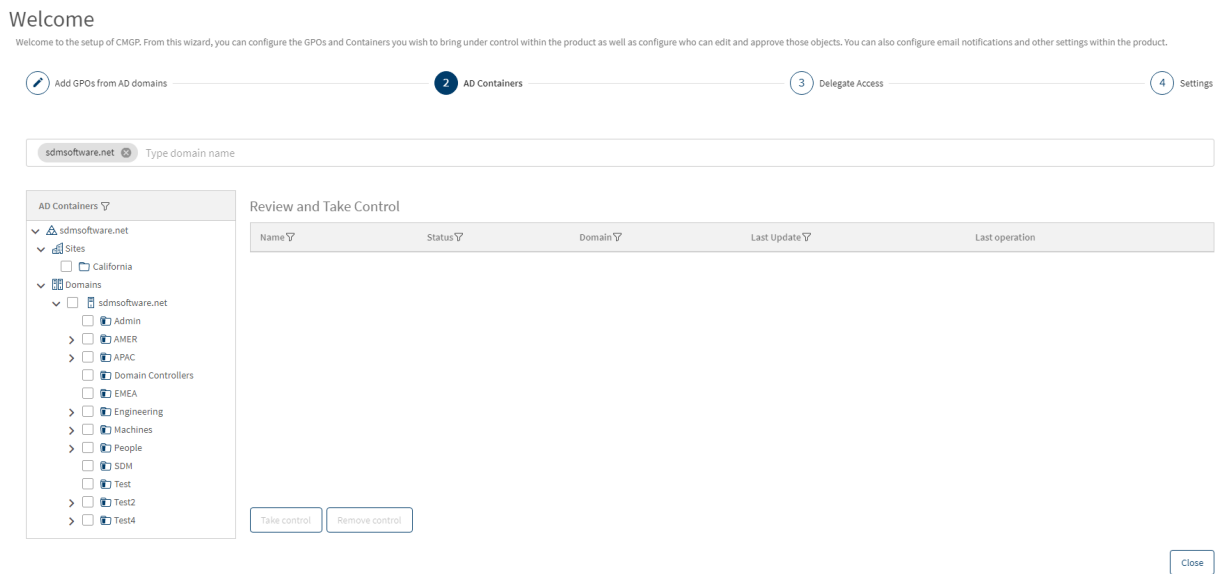
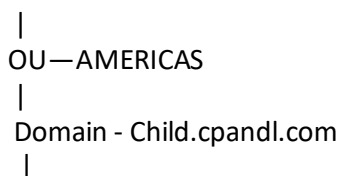


Figure 13 Selecting AD Containers to Take Control of

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



OU – Marketing

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 CMGP 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 CMGP.

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 CMGP PowerShell module, described in [Appendix C: The CMGP PowerShell Module](#).

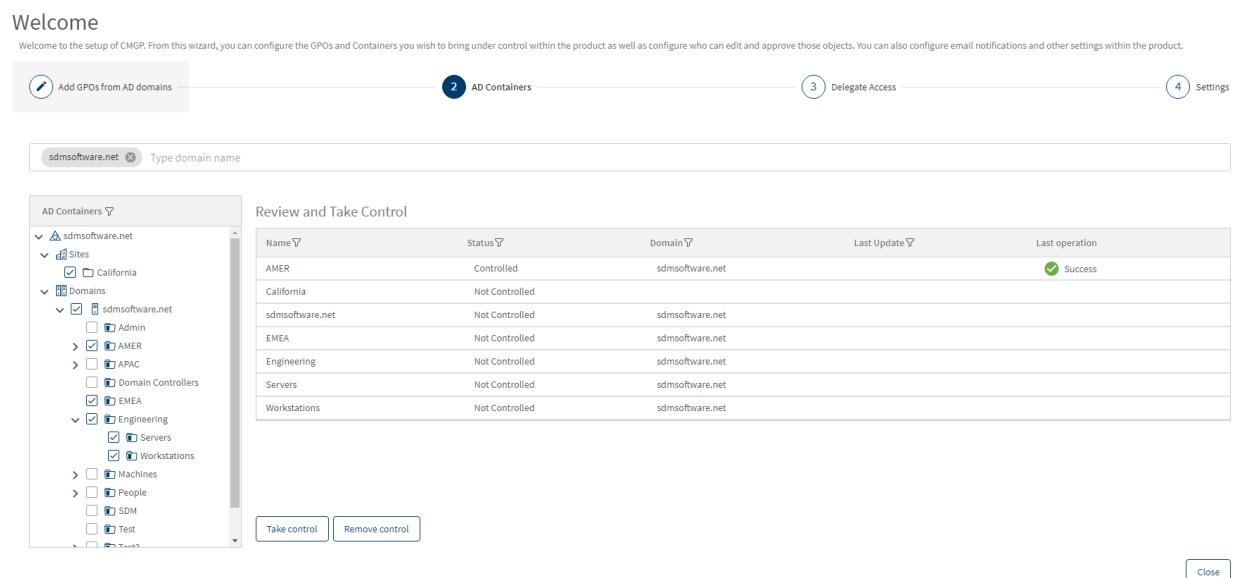


Figure 14 Taking control of AD containers

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.

Delegate Access

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

Editor and Approver Capabilities

Editors have the following capabilities:

- Check out GPOs or containers for change
- Edit GPOs or GPO permissions and link/unlink, enforce or enable/disable GPO links on containers
- Check in GPOs or containers after a change
- Discard a check out
- Request a rollback of a GPO or container change
- View differences between current and prior versions of GPOs or containers

Approvers have the following capabilities:

- Approve GPO or container changes
- Reject GPO or container changes
- Deploy immediately or schedule a GPO or container change for deployment
- View differences between current and prior versions of GPOs or containers

To proceed, select Step 3—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.

Welcome

Welcome to the setup of CMGR. 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.

<input type="checkbox"/>	Name ▾	Type ▾	Canonical Name ▾	Approver ▾	Editor ▾
<input type="checkbox"/>	Default Domain Controllers Policy	GPO	sdmsoftware.net/System/Policies/{6AC1786C-016F-11D2-945F-00C04FB984F9}	Add approver...	Add editor...
<input type="checkbox"/>	Americas Desktop Security Policy	GPO	sdmsoftware.net/System/Policies/{08C734DB-92DB-4A82-8F9D-A38DC37A9046}	Add approver...	Add editor...
<input type="checkbox"/>	EMEA	OU	sdmsoftware.net/EMEA	Add approver...	Add editor...
<input type="checkbox"/>	Americas Drive Mapping Policy	GPO	sdmsoftware.net/System/Policies/{A038AD3C-19C3-4156-AD95-71E369DFB7D8}	Add approver...	Add editor...
<input type="checkbox"/>	Client General Policy	GPO	sdmsoftware.net/System/Policies/{5B139A75-5B69-4A35-B159-4B4E79DE2F6C}	Add approver...	Add editor...
<input type="checkbox"/>	Default Domain Policy	GPO	sdmsoftware.net/System/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}	Add approver...	Add editor...
<input type="checkbox"/>	AMER	OU	sdmsoftware.net/AMER	Add approver...	Add editor...
<input type="checkbox"/>	California	Site	sdmsoftware.net/Configuration/Sites/California	Add approver...	Add editor...
<input type="checkbox"/>	Americas Computer Security Policy	GPO	sdmsoftware.net/System/Policies/{B01F2C00-39C5-4CE7-911D-C482D0A275A9}	Add approver...	Add editor...
<input type="checkbox"/>	Client Desktop Policy	GPO	sdmsoftware.net/System/Policies/{D6A457D9-88D0-4F16-9AC8-5175D0B828D4}	Add approver...	Add editor...

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:

Welcome

Welcome to the setup of CMGR. 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.

<input checked="" type="checkbox"/>	Name ▾	Type ▾	Canonical Name ▾	Approver ▾	Editor ▾
-------------------------------------	--------	--------	------------------	------------	----------

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:

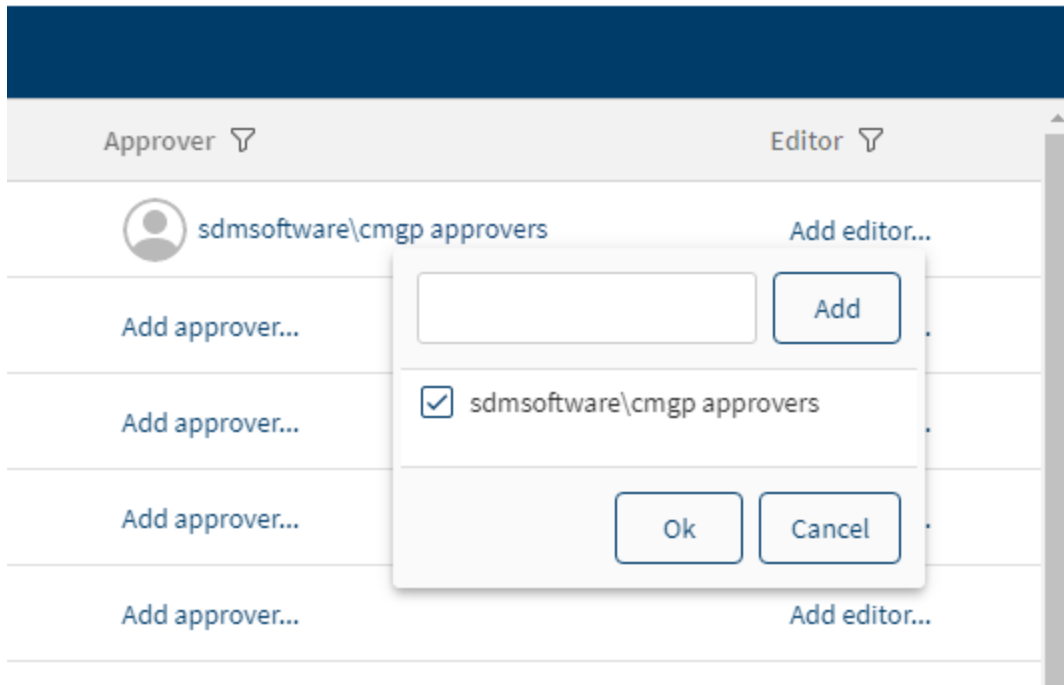


Figure 17

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\cmgp 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.

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 4—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.

General

This approver is used when a new GPO is created.

Default approver(s): Add users or groups...

Audit events lifetime: 60 day(s)

SMTP Server Settings

SMTP Server Address:

Port: 465

Sender Email:

You must enter a value

This SMTP server uses SSL for encrypting communications over the internet

This SMTP server requires authentication

Login:

Password:

Test Save

Close

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 CMGP. 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.
- **Audit events lifetime:** This value, which defaults to 60 days, controls how long CMGP 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:** CMGP 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 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.

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 environment. 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 CMGP is governed by the roles that the product

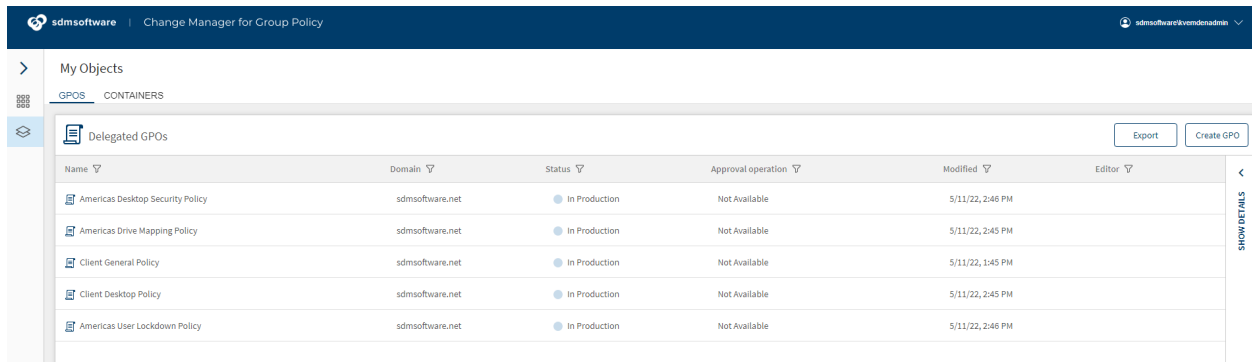
supports. We've already introduced the Editor and Approver roles, but the product contains a number of other roles as well, which are defined below.

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 CMGP menu under **Delegation, Product Roles**.

Product Administrator: Anyone with this role can control all aspects of CMGP configuration, including logging in to the console, taking control of GPOs and containers, setting delegation on GPOs and containers, configuring application settings, managing licensing and viewing statistics and audit events across all managed objects. The user who installs CMGP 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 CMGP. 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 CMGP and they can also approve and deploy those changes themselves. This removes any oversight from the GPO or container change process. The main purpose of this role is to allow temporary, urgent changes to occur without the overhead of an approval process.

Auditor: The Auditor role allows read-only access to certain aspects of CMGP. The Auditor role has two main rights. Members of this role can see all objects that have been delegated in CMGP, 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 [CMGP Audit Log](#), which allows them to see what activities have occurred.

CMGP Dashboard

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

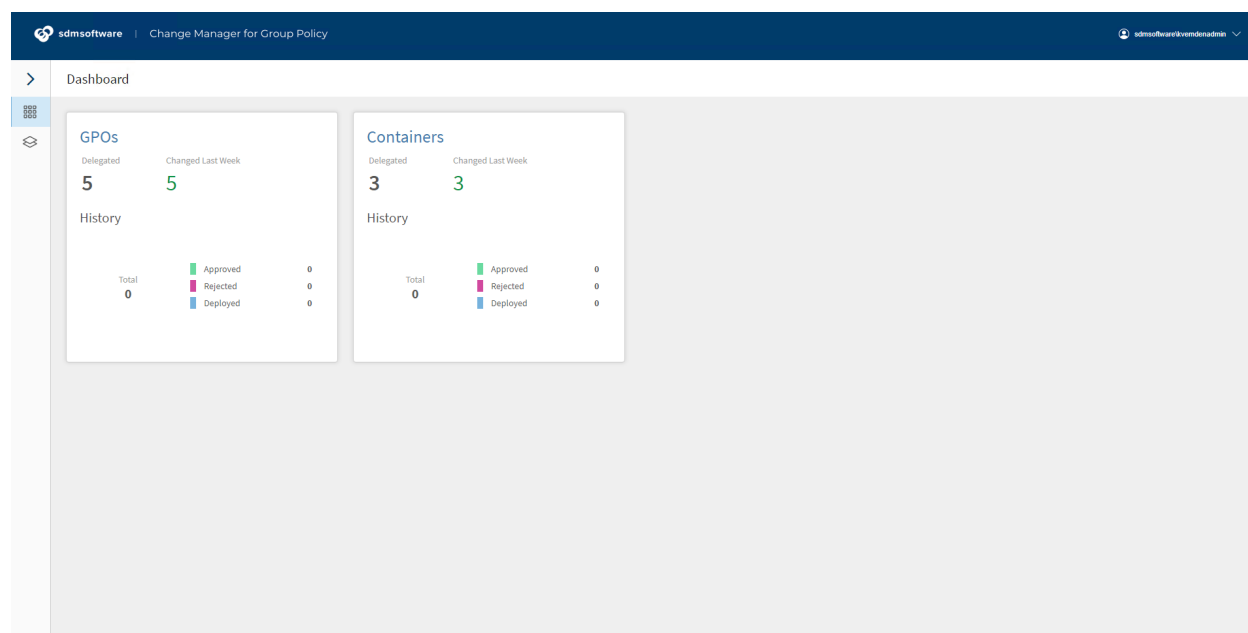


Figure 20 The CMG Dashboard

The dashboard is broken into two sections—the left-hand box provides statistics for GPOs and the right-hand box provides statistics for containers. 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) 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 CMGP, I will see any GPOs (or containers) 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.

CMGP Navigation

Navigating around CMGP 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, as shown in Figure 21:

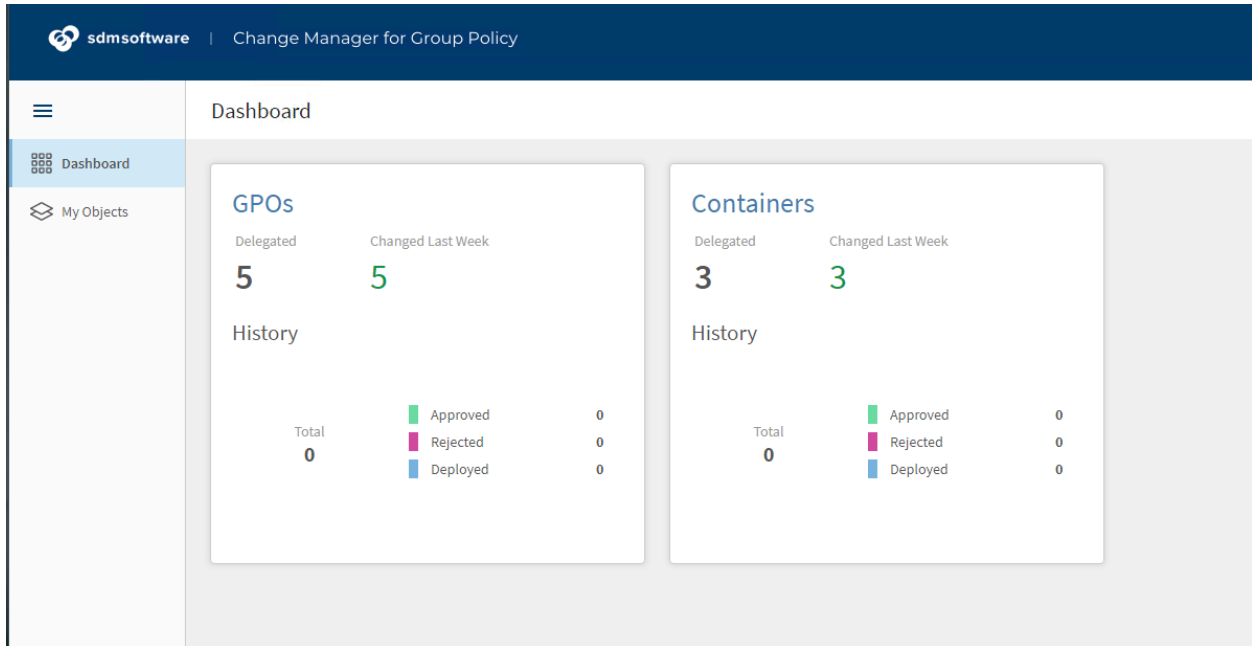


Figure 21 Viewing the CMGP menu

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

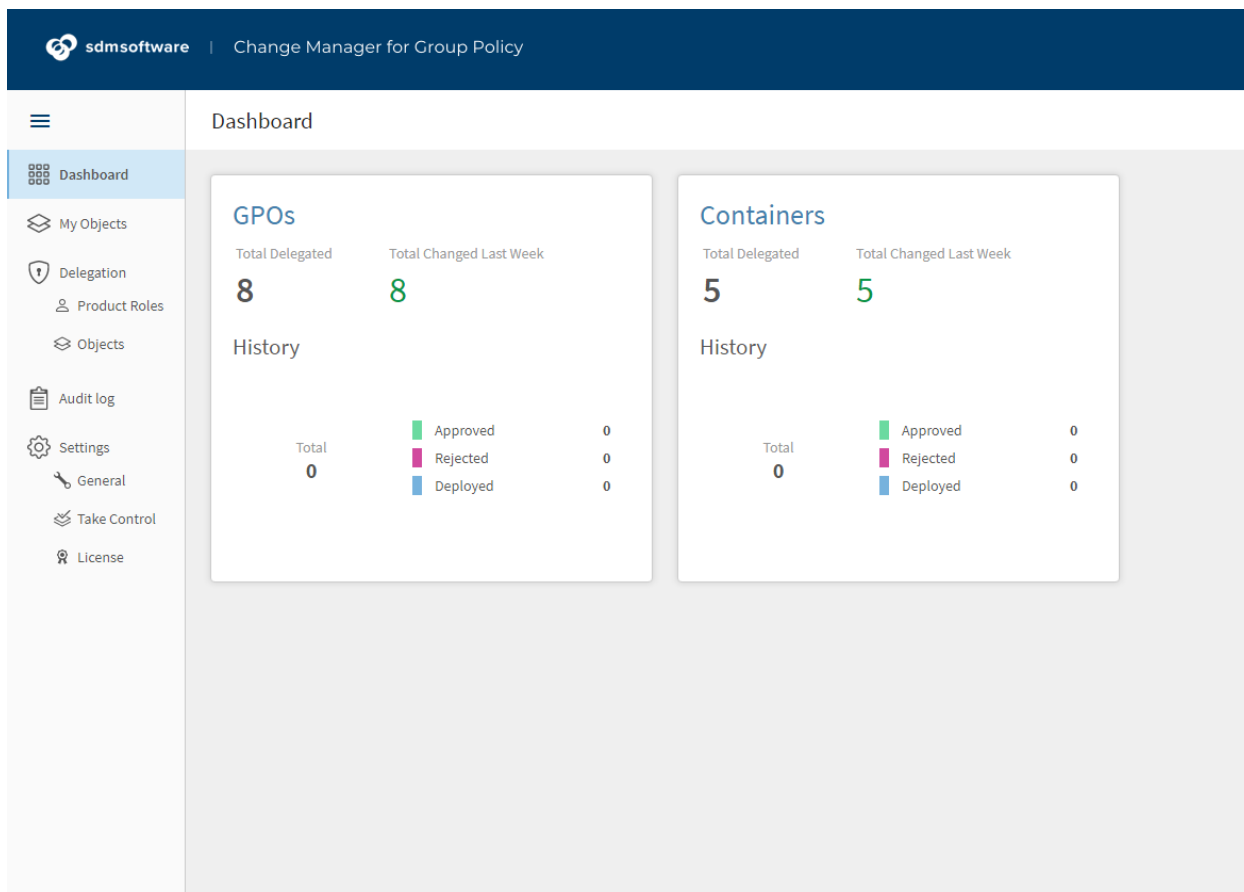


Figure 22 The full set of CMGP menu options

Each menu option is described here:

- **Dashboard:** Displays the CMGP dashboard page
- **My Objects:** Shows the list of GPOs and containers 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 CMGP [product roles](#).
- **Delegation, Objects:** Allows a product administrator to manage the delegation of GPOs and containers that are currently under control. This is where a product administrator can change which users and groups are editors or approvers of a GPO or container.
- **Audit Log:** Provides the product administrator or auditor with access to the audit log—which is a record of all activities performed within CMGP.
- **Settings, General:** Allows the product administrator to configure default approvers, audit events lifetime and SMTP settings.

- **Settings, Take Control:** Allows the product administrator to take control of additional GPOs or container objects 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 CMGP.

The Change Control Process

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

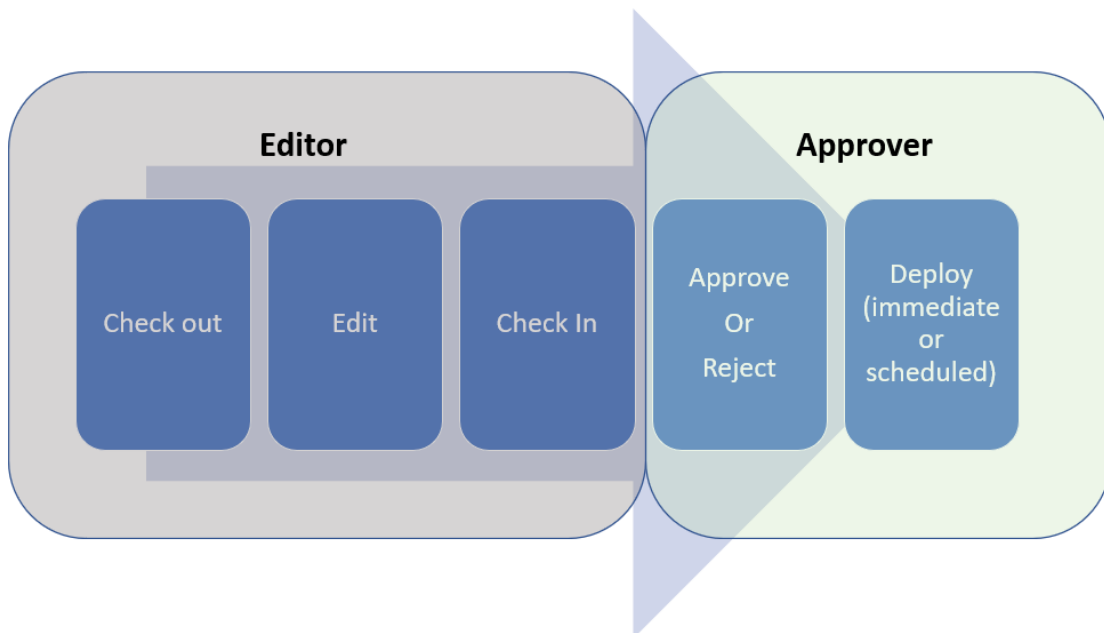


Figure 23 The CMGP Change Workflow

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

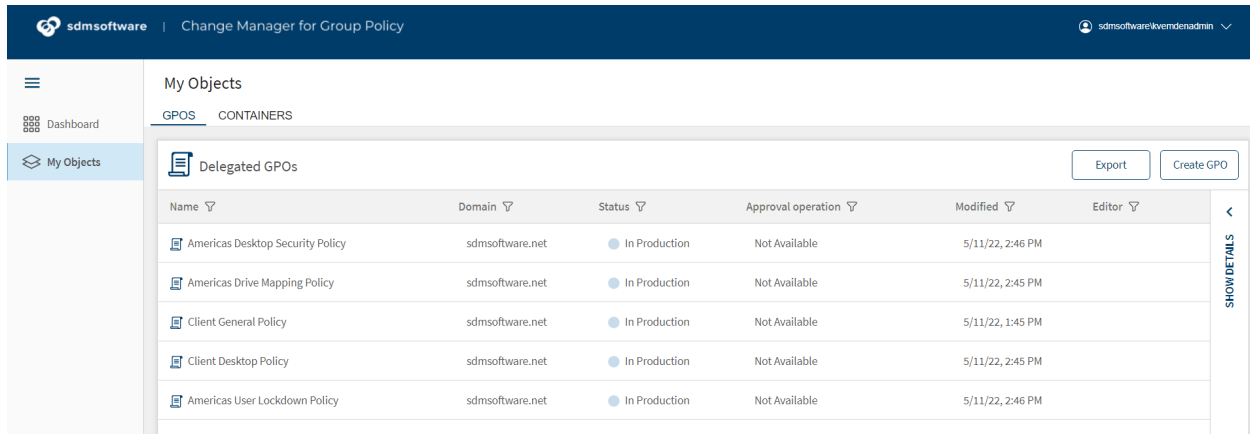



Figure 24 The My Objects page

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

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

 Americas Desktop Security Policy
● In Production

Type	GPO
Created	9/12/17, 2:58 PM
Approvers	SDMSOFTWARE\Tier 2 GPO Approvers
Current approver	
DN	CN={0BC734DB-92DB-4A82-8F9D-A38DC37A9D46},CN=Policies,CN=System,DC=sdmsoftware,DC=net
Version	1.0
Checked out by	
Deploy Date	
Comment	
Editor comment	

Linked to:

- sdmsoftware.net/Test4/Computers
- sdmsoftware.net/Machines
- sdmsoftware.net/AMER/Clients






-  Check-out
-  Edit
-  Edit permissions
-  Check-in
-  Rollback

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

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

Handling Out-of-Band Changes

CMGP also has the ability to check for changes that have happened to controlled GPOs or containers 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 CMGP 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 CMGP. 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 CMGP 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 can now perform the following actions:

- **Edit:** Launch the GPO Editor against the checked out 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 CMGP, when you check out a GPO, a temporary copy of that GPO is created in AD. These copies are only manageable by the CMGP service account and have a very distinct naming structure, as shown here:

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

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

They should not be removed or modified manually. CMGP 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 CMGP is run on a given Windows machine. This application can be pre-installed using the link from the CMGP home page (for CMGP 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 CMGP 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 first time through, the following message will appear:

Open Change Manager ...cy GPMC Driver?

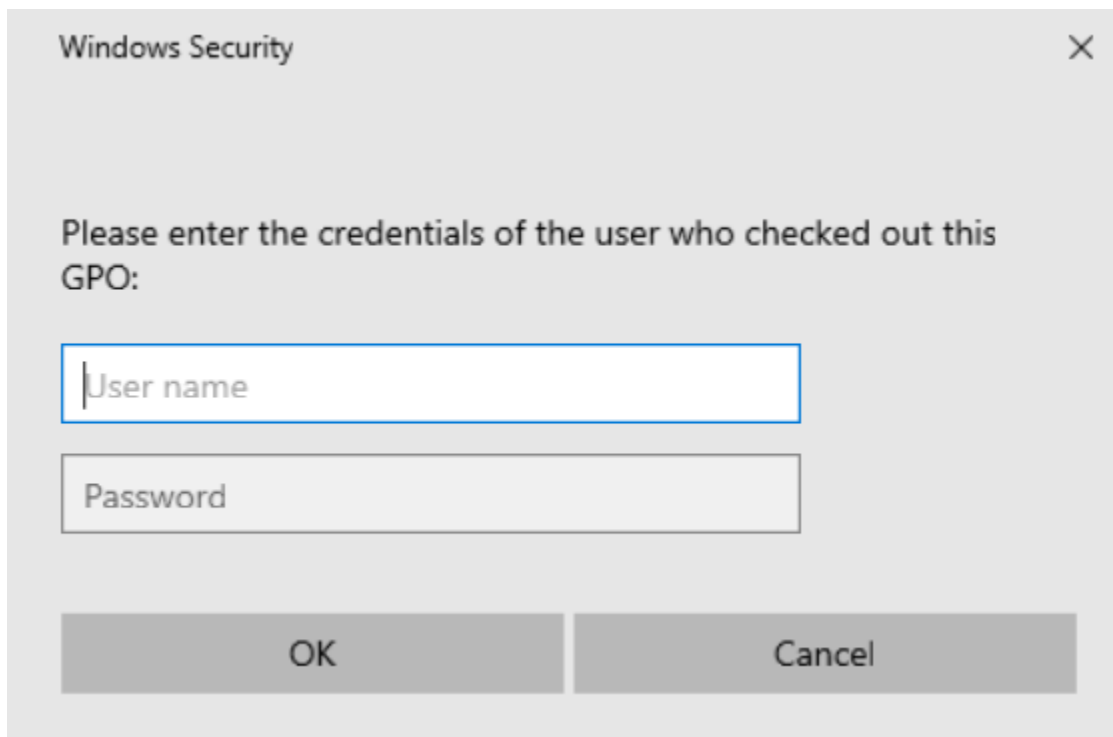
https://cmgp-sdm.sdmsoftware.net wants to open this application.

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:



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

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.

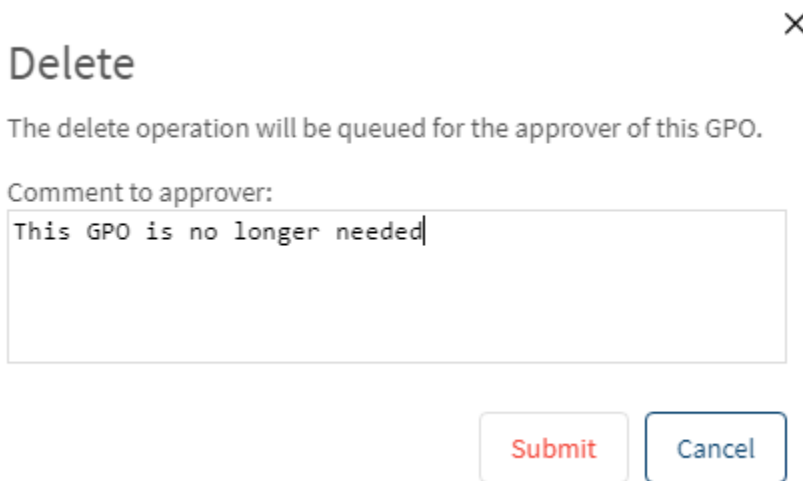
After a change has been made, it is not yet deployed (or even approved). You can make other changes to a GPO while it's checked out. For instance, you can rename a GPO, and you can edit delegation on a GPO.

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 X

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

Comment to approver:

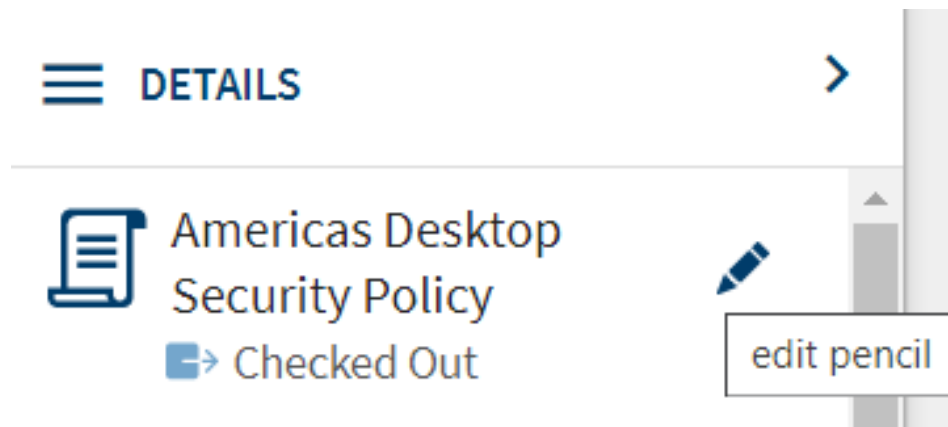
This GPO is no longer needed

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.

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 CMGP and will need to go through the same approval-based workflow as any other GPO change.

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:

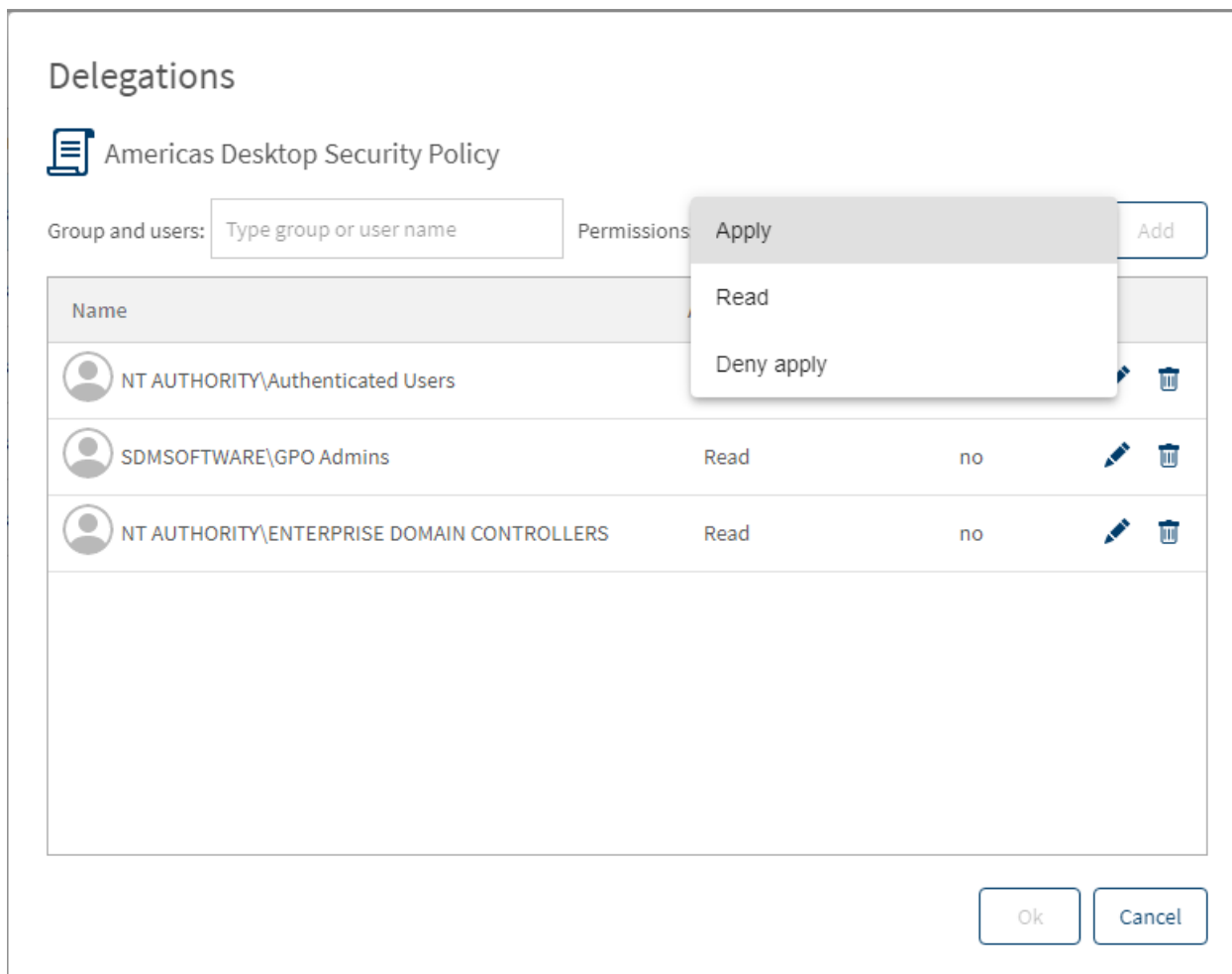


Figure 27 Modifying GPO Delegation

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

NOTE: CMGP 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 CMGP.

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).

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:

Your action is needed

 Darren Mar-Elia
To: Darren Mar-Elia

 Americas Drive Mapping Policy
Waiting Approval

Reply Reply All Forward

Fri 5/20/2022 4:00 PM

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 CMGP 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.

Once the approver has logged in and approved the outstanding change, the state of the GPO now 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

Roll back to production version if scheduled deployment fails.

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, CMGP will take the last known-good backup of the object being changed and apply it to production.

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 or container has been checked in by an editor, but has not been approved within **5 days**, that object is marked as “Overdue for Approval” in CMGP. This interval can be adjusted using the CMGP PowerShell cmdlet `Set-CMSettings`, and the option is described in [Appendix B: Customizable settings within CMGP](#).*

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
  sdmsoftware.net/Test GPO	sdmsoftware.net 
  sdmsoftware.net/Americas Computer Security Policy	sdmsoftware.net 

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.



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 CMGP application.

Once the link change is approved, the approver can then choose to deploy it immediately or on a schedule, as with GPO changes. In fact, 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 or containers, an approver can choose to cancel a deployment by selecting the “Cancel Deployment” option on the object from the Details pane.

Audit Log

All activities performed within CMGP 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\kvemdenadmin
5/20/22, 5:09 PM	Check-in	EMEA	sdmsoftware.net	Started	sdmsoftware\kvemdenadmin
5/20/22, 4:45 PM	Check-out	EMEA	sdmsoftware.net	Success	sdmsoftware\kvemdenadmin
5/20/22, 4:45 PM	Check-out	EMEA	sdmsoftware.net	Started	sdmsoftware\kvemdenadmin
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 CMGP 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 CMGP, you can use the PowerShell cmdlet **Get-CMEvents**, to get a list of audit events.

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:

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 CMGP 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 browse 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 CMGP license, contact support@sdmssoftware.com to get more details.

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

A prerequisite for using CMGP 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 CMGP service account the ability to modify the permissions of GPOs and AD containers. For GPOs, this amounts to granting the CMGP service account the “Edit settings, delete and modify security” permission on GPOs that are managed by CMGP. For AD containers (AD sites, domains and OUs) the permission required by the CMGP 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.

CMGP provides a command-line utility called **SetCMGPPermissions.exe** that sets the correct permissions on GPOs and containers that are required for CMGP 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 CMGP, 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] ...]
cmnds 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 CMGP 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 CMGP service account GPO creator rights on the domain. This is required to ensure that CMGP functions properly.

```
SetCMGPPermissions.exe -trustee sdmsoftware\svc.cmgp -domain sdmsoftware.net -GPOCreator
```

- **GPOModify:** Grants the CMGP service account modify rights over all GPOs in the specified domain.

SetCMGPPermissions.exe -trustee sdmsoftware\svc.cmgp -domain sdmsoftware.net -GPOModify

- **Container:** Grants the CMGP 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.cmgp -domain sdmsoftware.net -Container "OU=Machines,DC=sdmsoftware,DC=net" -Recurse

- **Site:** Grants the CMGP 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.cmgp -domain sdmsoftware.net -Site "CN=Sites,CN=Configuration,DC=sdmsoftware,DC=net" -Recurse

Appendix B: Customizable settings within CMGP

There are a number of settings that can be configured within CMGP, 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 CMGP. The settings can be retrieved and set using two PowerShell cmdlets from the CMGP PowerShell Module (called SDM-CMGP). 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 CMGP 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 CMGP service	600
EventsTTLDays	Duration after which CMGP audit logs will be purged	60
LocksTTLMinutes	Timeout after which any object locked by CMGP 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)
MaxDurationInApprovalStateMinutes	Timeout after which unapproved changes will be marked as "overdue for approval"	7200

Appendix C: The CMGP PowerShell Module

CMGP provides a separate PowerShell module, which can be installed by using the **CMGP-PSSetup.exe** installer file that ships in the CMGP download. The CMGP PowerShell module provides a set of 49 cmdlets within a module called **SDM-CMGP** that allows you to automate many aspects of CMGP operation and management.

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

```
Connect-CMServer -Server <FQDN of CMGP 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 CMGP cmdlet to see a more detailed description of each cmdlet:

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

Approve-CMObject: Allows a user in the CMGP 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 CMGP. 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 CMGP 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 CMGP

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

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

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

Get-CMDelegated: Returns the list of GPOs or containers that have been delegated within CMGP

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

Get-CMEvents: Retrieves events from the CMGP 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 CMGP

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

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

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 CMGP

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

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

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

Get-CMSystemDelegations: [Internal]
Get-CMUserContext: Retrieves the roles a given user has defined in CMGP
Get-CMUserPhoto: Retrieves any photo that is associated with a user defined to a role in CMGP
Grant-CMRole: Lets you assign a user to a particular role in CMGP
New-CMGPO: Creates a new GPO in CMGP
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-CMObjects: Allows you to take control of multiple GPOs or Containers
Remove-CMDomain: Removes an AD domain that is currently defined within CMGP
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-CMEditorComment: Allows you to set a check-in comment on a GPO or container check-in
Set-CMRoles: Provides an alternate way to set multiple role assignments in CMGP
Set-CMSSettings: Used to set configurable options within CMGP
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 CMGP SMTP settings
Unregister-CMContainer: Removes control of a controlled container in CMGP
Unregister-CMGPO: Removes control of a controlled GPO in CMGP
Unregister-CMObjects: Allows for multiple removal of control operations on GPOs or containers in a single command
Use-CMLicense: Allows you to activate a CMGP license