Managing Group Policy Securely with Admin Tiering & Change Control

Secure management of your Group Policy Environment

SDM Software, Inc.

October 2022

Contents

Overview

Group Policy remains a powerful tool for configuring Windows systems in many enterprises. But that power also makes it a target of attackers, looking to compromise an environment, or worse yet, spread ransomware or other types of malware. Indeed, as far back as 2017, our founder, Darren Mar-Elia (aka "GPOGuy") wrote a blog post entitled "Group Policy as Malware Delivery System" (see https://sdmsoftware.com/security-related/group-policy-malware-delivery-system/) that describes how an attacker hijacked a GPO to spread malware to all client systems in an environment. For these reasons, it's incredibly important to protect your Group Policy infrastructure the same way you might protect Active Directory itself from these attacks. In this whitepaper, we'll lay out a strategy created by Darren for protecting your Group Policy investment, and describe how SDM Software's Change Manager for Group Policy can simplify its implementation.

Admin Tiering Defined

Admin tiering is a concept that Microsoft introduced back in 2014, as a way of segregating areas of concern within a corporate network. They introduced three tiers—Tier 0 for Active Directory (AD) Domain Controllers (the most prized resource), Tier 1 for Windows servers and Tier 2 for Windows workstations. The idea was to prevent ease of lateral movement via credential theft, by controlling who could log into a given tier, as shown in Figure 1 below.

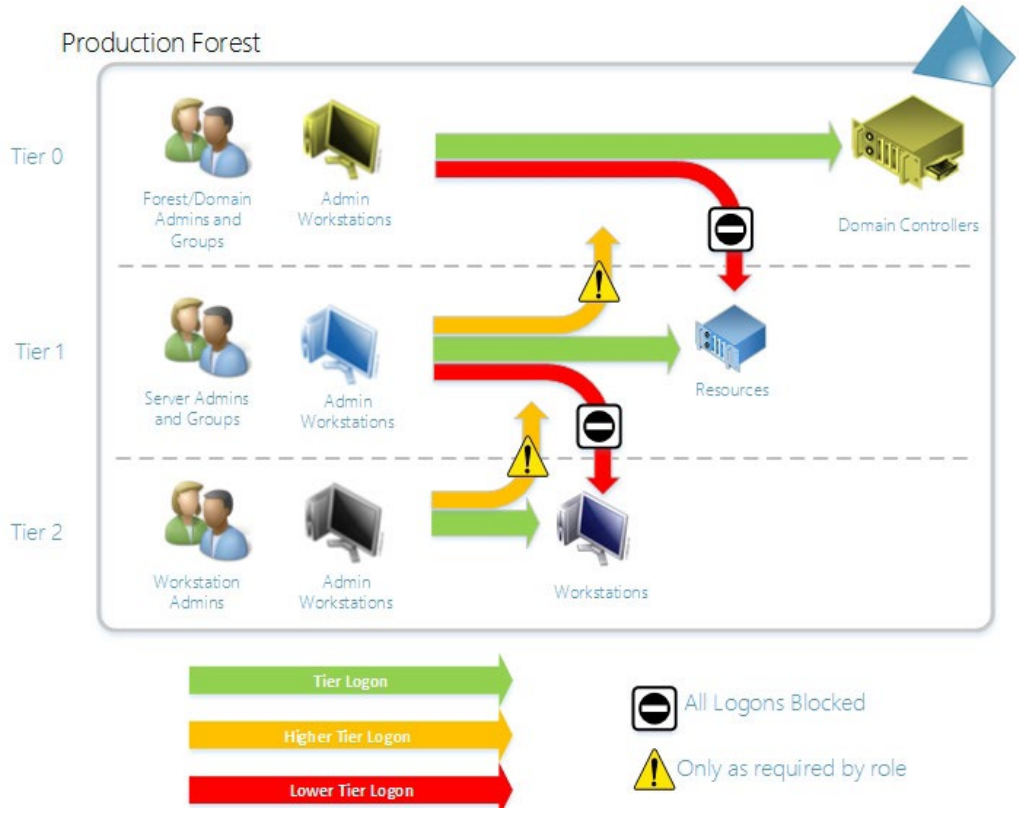

Figure 1 The Admin Tiering Model (Copyright Microsoft, 2014)

But the value of admin tiering applies equally well to Group Policy management, albeit using slightly different definitions. The goal of this whitepaper is to lay out how you can apply these principles of admin tiering to your Group Policy environment to ensure that a compromise of one tier of Group Policy does not easily lead to a total compromise of your entire environment.

But why is this important, you might ask. Well, there are many ways in which Group Policy can be abused to compromise an environment. Many attackers have used Group Policy to distribute malware, execute payloads or even exfiltrate data. In addition, if "Tier 0 GPOs" are compromised, it is relatively easy to "coerce" a GPO to grant the attacker Tier 0 (i.e. Domain Admin) access to AD. Once that happens, all bets are off in terms of protecting the environment.

Admin Tiering for Group Policy

As mentioned, admin tiering can provide protection from credential theft by segregating which administrators can log in to systems in particular tiers. A workstation admin account should not be able to log in to a domain controller. Likewise, an admin account that manages domain controllers should not be logging in to workstations, which are relatively easily compromised by attackers through phishing and other campaigns. If an attacker compromises a workstation where a Tier 0 administrator account has logged in, it is relatively easy for that attacker to get access to that Tier 0 account's credentials in memory using well known tools such as **mimikatz**, and then use those credentials to compromise AD.

But how does this process apply to Group Policy? Basically by applying the same tiering model for AD described above, to how GPOs apply in your environment. The first thing to note is that managing GPOs securely is basically an **AD security problem**. Namely, how do you delegate control to your GP environment to ensure that it's not abused. And when it comes to delegation, there are two main areas you need to be concerned about:

1. **Delegation on GPOs themselves**
2. **Delegation of containers where GPOs are linked**

The ability to edit a GPO gives the editor full control to add or remove any settings they want to. The ability to link a GPO to a container allows a user to apply a given GPO to whatever targets (users or computers) they wish, within AD.

Remember that GPOs can be linked to AD site objects, the AD domain object within a given domain, and any OU within that domain.

Both of these delegations can be applied to the admin tiering model, as shown in the table below:

Table 1: GPO Management Admin Tiering

Tier	GPO Delegation	Container Delegation
0	Any GPOs that are processed by **domain controllers**, including those linked at the AD site,	Any containers for which, when GPOs are linked to them, they are processed by Domain Controllers. This includes any

	domain or Domain Controllers OU level.	AD sites that contain DCs, the domain object, which is processed by all computers and users in the domain, and the Domain Controllers OU, which is where DC machine accounts typically reside.
1	Any GPOs that are processed by **Windows servers**, or users that log in to Windows servers**.** These would include any GPOs linked to OUs that only contain server machine accounts, or OUs that contain server administrator accounts.	Any containers that contain or are processed by server machine accounts, including OUs or AD sites that include subnets where server machine accounts reside, and OUs that contain server administrator user accounts.
2	Any GPOs that are processed by **Windows workstations.** These would include any GPOs linked to OUs that only contain workstation machine accounts, or OUs that contain workstation user accounts.	Any containers that contain or are processed by workstation machine accounts, including OUs or AD sites that include subnets where workstation machine accounts reside, and OUs that contain workstation user accounts.

Caveats

Table 1 above provides some general guidance on how to think about GPO administrative tiering, but there are some challenges you'll need to consider:

1. A GPO linked at the domain level could easily apply to all three tiers. And, depending upon security group filtering or WMI filtering on that GPO, it might only apply to a subset of tiers. That said, you have to assume that if a GPO linked to the domain is editable by a particular administrator, that it could be specifically targeted to domain controllers by that administrator, if that account is compromised. Therefore, all GPOs linked at the domain level should be considered **Tier 0**.
2. A given OU might contain both server and workstation machine accounts, or both workstation and server user accounts. The best solution is to separate machine accounts and user accounts by their form factor, but if you can't do that, then treat these mixed OUs as **Tier 1**, because you want to take the most secure posture possible.
3. Once you classify a GPO as Tier 0, 1 or 2, it's important to not allow linking of GPOs to containers outside of their tiers. Since there is no easy way to natively enforce what GPOs can be linked to which containers, you'll need to enforce this through your **GPO change control process**.

Implementing GPO Management Tiering

Now that we've defined what GPO tiering looks like, how do you implement it? The bottom line is that native Group Policy and AD delegation can provide the key towards enforcing GPO management tiering,

just as native AD delegation and user rights support the implementation of AD administrative tiering. Let's start first with GPO delegation. Say we need to define Tier 0 GPOs and containers. Figure 2 defines an AD domain that has GPOs linked to the domain, Domain Controllers OU and AD site level:

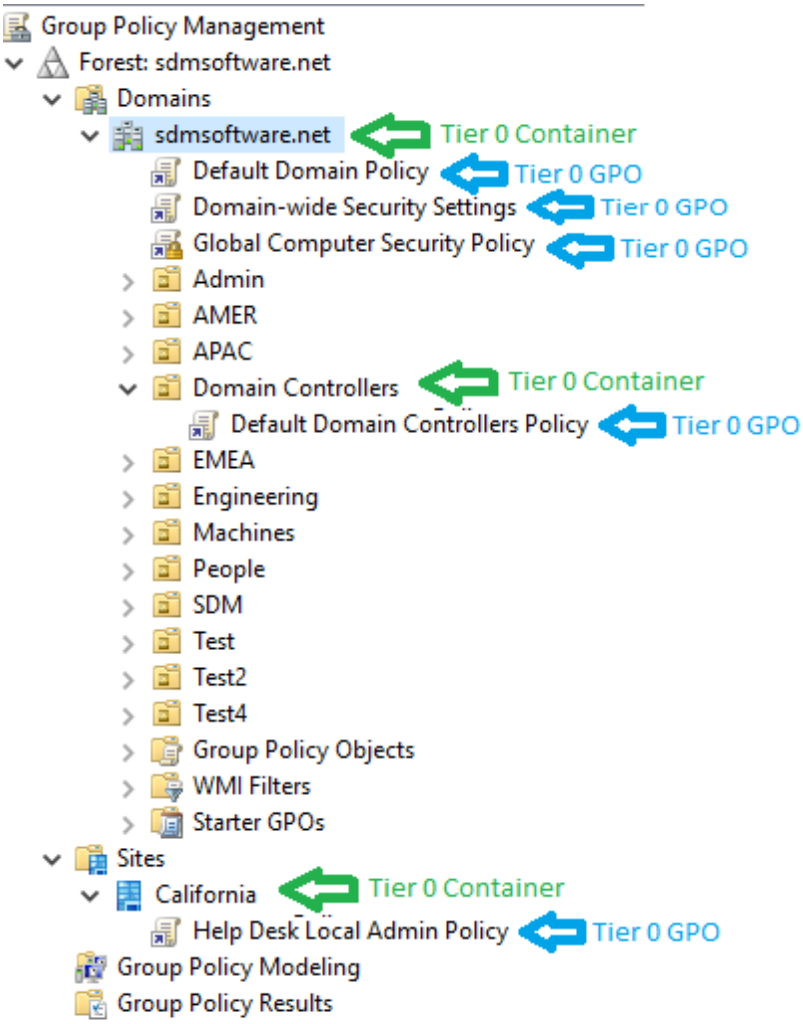

Figure 2 : Defining Tier 0 GPOs and Containers

As you can see in the figure above, the **sdmsoftware.net** domain object, the **Domain Controllers** OU, and the "**California" AD site (which contains domain controllers)** (shown in green) are all Tier 0 containers, because they can contain linked GPOs that are processed by domain controllers. Likewise, there are a number of GPOs linked to these containers (shown in blue). These GPOs are considered Tier 0 as well.

Container Delegation

Now let's look at how we can protect them. Let's start by focusing on the containers. Enforcing GPO tiering on a container is about controlling who can link GPOs to that container, or affect GPO processing by having the ability to set the "Block Inheritance" flag on that container. Natively in AD, there are two

permissions that control the linking of GPOs and the setting of Block Inheritance on a container. They are the **gPLink** and **gPOptions** attributes, and any security principal that has **write** permissions for these attributes on a container can link and set the flag on that container. You can easily set these permissions from within GPMC by selecting the container and then the **Delegation** tab. Make sure that "Link GPOs" is selected from the permission drop-down, and then Add your Tier 0 resource. The best practice here is to use an AD security group to grant the various tiering accesses in your environment, as shown in Figure 3 below:

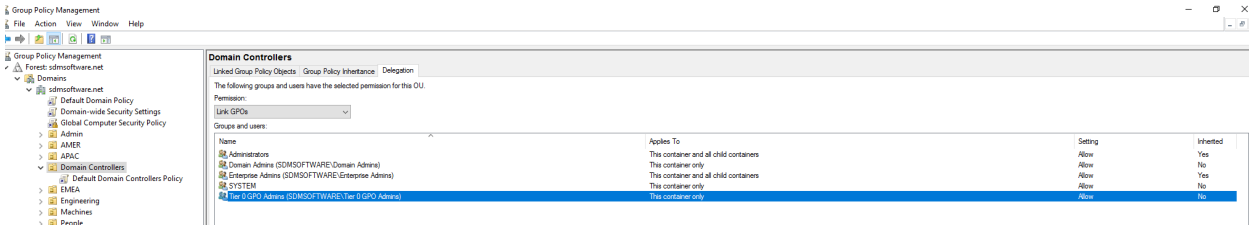

Figure 3 Enforcing Tier 0 delegation on a container

By default, Windows adds the domain local Administrators, Domain Admins, Enterprise Admins and System account to the delegation for linking of containers. You can choose to remove these groups/accounts if you want to have total control over who can link to your Tier 0 containers, or you can put these groups into your "Tier 0 Admins" group to incorporate them. Of course, you'll want to remove any other non-privileged accounts that should not have linking of Tier 0 containers at this stage, as well. The goal here is to ensure that you can control who is linking GPOs to your critical containers. Again, this is where a GP change control process that incorporates linking delegation can come in handy.

You can repeat this process for all of your Tier 1 and Tier 2 containers. The key is to first identify these objects and then classify them by tiers, then apply appropriate delegation, and most importantly, remove any delegations that do not respect the tiering model.

GPO Delegation

Delegating control of GPOs is very similar to that of containers and can also best be accomplished using GPMC. The security model for GPO delegation is a bit different than for containers, but nonetheless what you are after is to allow anyone within the tier to "edit" a GPO and not allow anyone outside of the tier. For example, in the figure below, we've allowed the "Tier 0 GPO Admins" the ability to "Edit Settings" on the Default Domain Controllers Policy GPO:

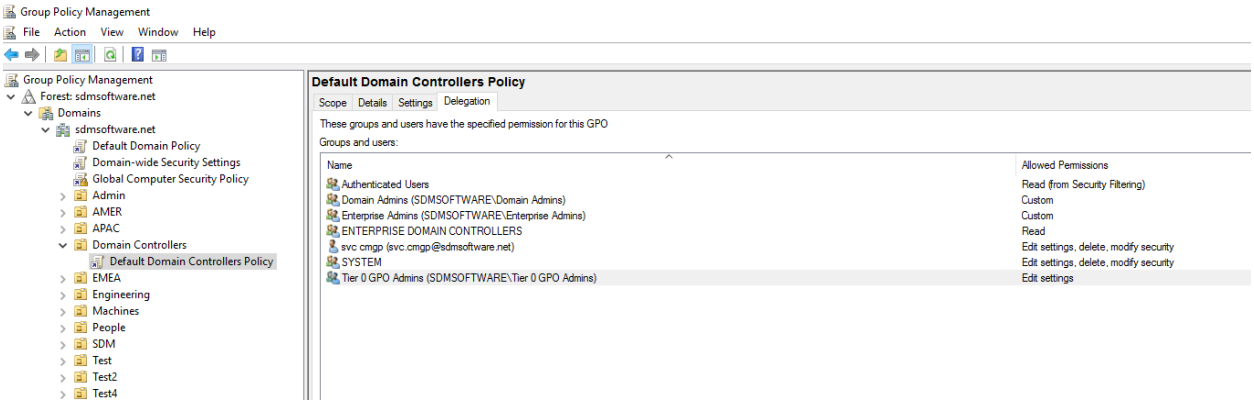

Figure 4 Delegating Tier 0 access to GPOs

Note that there are two permission sets you can grant in GPMC for editing. One is to simply allow the editing of settings within a GPO. The other, "Edit Settings, Delete, Modify Security" allows full control over the GPO, including the ability to edit settings, delete the GPO from the domain and modify the delegation on that GPO—the latter of which would be bad for your delegation model unless you implicitly trust the account doing the modification.

Once again, the process for GPO delegation by tiers is to first identify the GPOs by their tiers, then add the appropriate tiered administration group, and remove all accounts that don't respect the tiering model.

The Value of Group Policy Change Control

Everything presented so far can be accomplished with native delegation in GPMC. But the process of enforcing tiering and ensuring that, even within your tiering model, the right GPOs are being linked to the right containers, requires some additional work. In many organizations, the need for controls around something as important as configuration and hardening of your Windows systems is imperative. Change management has been a tried-and-true part of evolved IT shops. Group Policy management is no exception to this. And, with the threat of opening cyber-security related holes that attackers can take advantage of, change control is a must for many, if not all, Group Policy changes.

A Group Policy change control system should allow you to enforce the admin tiering that was described in this paper, but also allow you and your administrators to continue to be productive managing Group Policy. That is, it should not force un-helpful or difficult processes for making GPO changes, as this can lead to administrators finding ways around the solution. SDM Software developed **Change Manager for Group Policy** with these goals in mind—to allow you to secure Group Policy from attack, but also to provide quick and seamless management of Group Policy changes within your environment.

Change Manager for Group Policy allows you to delegate both GPO editing and container (site, domain, OU) linking at the object level. Meaning that you can easily create tiers of administration for Group Policy management, as shown here:

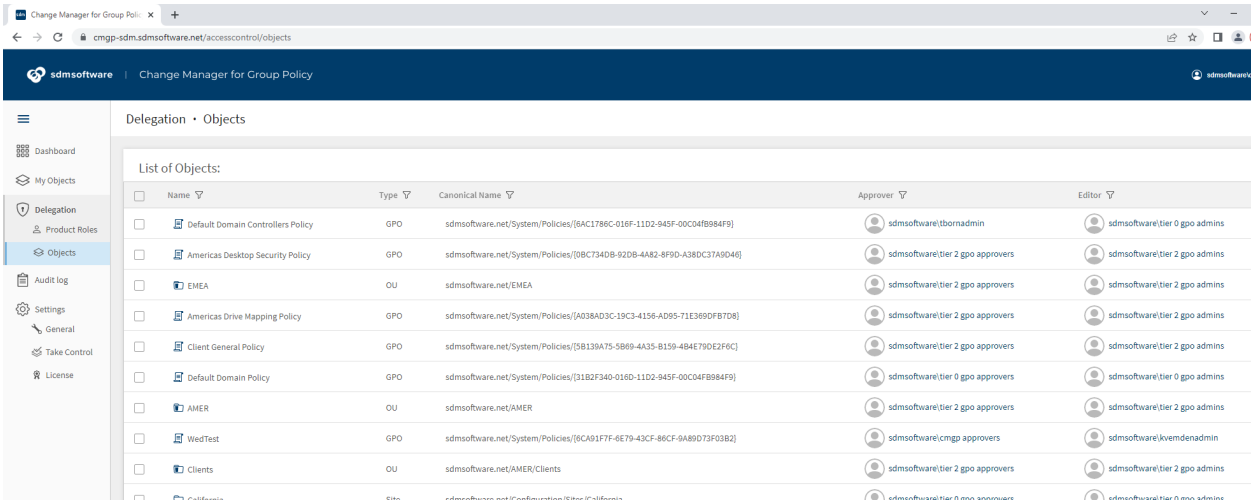

Figure 5 Delegating Tiered GPO administration in Change Manager for GP

As the figure shows, you can delegate GPO and container editing and approvals to different tiered admin groups, at the GPO or container level (or just delegate all the same if you want to simplify the model). The bottom line is that **Change Manager for Group Policy** facilitates an approval-based workflow for changes to GPOs and containers, based on the admin tiering model described in this paper, with minimal impact on your normal Group Policy management routine. So, you can protect your GPOs from attack, track changes to those GPOs and containers, and even roll back in the event of a disaster. For more information about **Change Manager for Group Policy**, you can watch these videos on our YouTube channel.