Microsoft Windows: Group Policy Controls and Their Uses

ISSC242 – Hardening Operating Systems

Corbin Osman

Dr. Byron K. Wallace

11/27/2022

**Microsoft Windows: Group Policy Controls and Their Uses**

In today’s day and age technology is used all around the world. Whether it be at home, at work or during travel, we are constantly surrounded by devices and networks that are working to keep us connected with those around us. Technology is an essential component in both individual lives and in larger scales such as businesses and organizations. Our computers, phones, and even social media accounts often contain personally identifiable information which, if viewed or accessed by the wrong person, could result in issues arising in the lives of those affected.

This idea is especially important to consider when realizing the quantity of confidential and sensitive information stored and used by many organizations and businesses. With personally identifiable information such as social security numbers and financial information such as bank account numbers, it is vital that this data is secured and protected for both clients and employees.

One method of securing systems and networks to protect this data is through the implementation of Group Policy controls. This paper will explore the definition and uses of Group Policy and the benefits of implementing policy controls within a business environment, as well as provide best practices to employ when developing group policies and procedures.

**The Role of Group Policy and Their Uses**

Group Policy, as shared by Jason Coggins in an article on the role Group Policy has in data security, is “a feature of Windows that facilitates a wide variety of advanced settings that network administrators can use to control the working environment of users and computer accounts in Active Directory” (Coggins, 2022). Understood in simple terms, Group Policy allows administrators to set policies and rules that determine how users are able to use, access, and modify system data and software. This helps network and security administrators have better control over the technological environments within their business area and ensure that data and information is secured.

Within any organization or business there are many branches or departments that interact with technology in different manners. One department may rely heavily on network and servers to perform their roles while another may not use extensive amounts of technology. No matter the level of technology used in an area it is important to have policies and procedures established that govern how devices, accounts, and networks are to be utilized.

Microsoft’s Active Directory Group Policy is a piece of software that allows Group Policy Objects (GPOs) to be set that “configure settings, behavior, and privileges for users and computers connected to the Active Directory domain” (Brown, 2022). This is performed through Microsoft Management Console (MMC) Group Policy Editor, a tool that allows for the creation, modification, and deletion of Group Policy Objects. Security administrators are then able to put these object policies in place within a network of systems to determine how systems appear and how they can be used.

Following are a few examples of Group Policy Objects that can be set. Passwords for user accounts are required to be a minimum length of eight characters and must be reset between fourteen and thirty days from their initial creation date. User accounts have access to view and modify only the files and folders they need access to in order to fulfill their work functions. Limit the number of other devices systems can see on local networks, such as printers or mobile devices.

There are many reasons why security administrators may choose to set and maintain Group Policy Objects, and it is important to understand what they enforce in the realm of security. In addition, it is critical to know what Group Policy Objects will take precedence over others, or if Group Policy Objects are the right choice for a business or enterprise environment. To better understand how Group Policy Object works within a network it is important to know how hierarchy works within Group Policy.

**Types of Group Policy and Their Hierarchy**

When a security administrator sets up Group Policy on a group of systems or a network it is important to know what policies will take precedence over another. For example, a policy on a local machine governing the allowed minimum length for passwords to be six characters would be overruled by a domain policy requiring passwords be a minimum length of eight characters. When applying Group Policy it is important to understand the order by which policies will be applied.

An article written by Josh Rickard on understanding Group Policy order helps to explain in depth the different layers of Group Policy hierarchy. This piece focuses on how Microsoft Windows looks at and applied Group Policy Objects. Two questions are presented when attempting to determine how Group Policy is being applied: Where you are and what you are.

The first question, in regard to where you are, is determined with one of the four common Group Policy layers, namely local, site, domain, and organizational unit. This is generally referred to as the L-S-D-OU rule, which is the order in which Group Policy objects are applied (Rickard, 2017). The lowest layer, Local Group Policy, is where Group Policy Objects can start, whereas the objects can be set and applied on a larger scale within an organization unit.

Within Local Group Policy, settings can be viewed and edited on an individual system or account. This can be useful if there is a specific system or account that needs special privileges or functions that would be difficult to manage with a higher layer of Group Policy. It is important to remember that while local Group Policy Objects can be created and set, they can be overwritten by policies that are set on site, domain and organizational unit Group Policies (Rickard, 2017).

In Site-based Group Policy, the structure of the network is important in knowing how Group policy objects will be applied. For example, we may have several systems residing on a domain, and in the forest or subnet there may be multiple domains that each contain a certain number of systems. Site-based Group Policy allows administrators to set Group Policy Objects for the forest or subnet in which all of the domains and systems reside, thus determining what policies are governed within the specific network of systems. This is done within an Active Directory site, which is not commonly used, thus showing how Site-based Group Policy is utilized.

Domain Group Policy is one of the most common layers used within business and enterprise environments. This is due to the ease of being able to set up the Default Domain Policy when a new domain is created (Rickard, 2017). Setting Group Policy at the domain level allows administrators to set and change policies that apply to each system within a specific domain, such as all user accounts within a certain business department. If there are specific policies or configurations that are desired to be applied to all of the systems within a domain, the best practice is to link the Group Policy Object to the root of the domain (Rickard, 2017). From there, if there are a few select systems that are not to have the same Group Policy Objects, such as administrator systems, those can be filtered to not have the Domain Group Policy apply to them.

Finally, Organizational Unit Group Policy is set up within a unit or container that can hold groups, computers and users. This unit or container is commonly found on a domain and helps to separate a group of computers and users from other groups also within the domain. An example is shared by Michael Buckbee in an article on organizational units where he states, “a domain may have 2 sub-organizations (e.g., consumer and enterprise) with 2 separate IT teams managing them. Creating 2 OUs lets each IT team administer their own policies that affect only the users, computers, etc. that fall within their unit” (Buckbee, 2015). As mentioned previously, within an organization one department may utilize technology a lot more heavily than another department, which should incentivize security administrators to ensure that all users and computer within their realm are governed by the proper Group Policy Objects to ensure integrity of data is kept.

With each of these layers better explained and understood, it is easier to determine which Group Policy layer should be following within the hierarchy. The questions “Where are you (local, site, domain, or OU)?” and “What are you (computer or user)?” will help determine what type of Group Policy should be implemented within a group or network.

**Group Policy or Individual Permissions**

When determining whether a system or user account should be governed by Group Policy Objects it is important to determine what policies need to be implemented. Within a large enterprise environment where there are multiple departments and divisions that all utilize technology it might be beneficial to implement Group Policy and divide applied objects to different domains. On the other hand, in a smaller environment where each computer or account is used for different functions it might be better to set up individual security policies on each system instead of utilizing Group Policy.

An article written by Matt Williams on Group Policy explores why it may not be the best practice to always utilize Group Policy when managing and monitoring user activity. It is a great tool and resource for IT and security managers when setting up policies for multiple systems and accounts on a network, but there are alternatives as well to Group Policy. While Group Policy Objects can be utilized for both small and large networks, organizing a large number of Group Policy Objects can be difficult and time consuming for administrators (Williams, 2012). Additionally, whether in large or small environments, it may not be easy to discern and identify what objects and policies are being applied to which device or account (Williams, 2012). For this reason, there are times when it may not be the most optimal to implement Group Policy.

This can be further understood as well when considering that there is no single Group Policy setup that will work for all Group Policy Objects that need to be implemented. As shared by Williams, what may work on one network or system may not work on another. An administrator may also face the issue of configuration error, which can result in Group Policy objects to not work as intended or to even function at all (Williams, 2012).

Williams shares a few alternatives to Group Policy, with the first being usage monitoring. There is software that allow for the monitoring of systems and activity, such as when a web browser is opened or what files and folders are accessed. Another option is to utilize software that allows for remote access to specific devices and accounts, allowing security administrators to monitor and access systems when they need to. Williams does state, however, that if the desire is to protect devices from configuration changes and downloads, policies and settings need to be put in place to manage security (Williams, 2012).

**Group Policy Best Practices**

With Group Policy better understood, and a decision made to implement Group Policy Objects, it is important to know what practices should be considered in order to create a safe and secure network. System and security administrators should have a plan when implementing Group Policy and know how they want systems, accounts and networks to be accessed by their users. Then, with that plan, they are able to choose the best Group Policy Objects and follow best practices in Group Policy implementation.

An article written by Jeff Brown explores several strong practices security administrators should consider within Group Policy. The first of these is to avoid making changes to the default policies. While it is possible to make changes to the Default Domain Policy, it is not recommended as this will affect all users and computers within the domain. Should a policy be implemented restricting access to certain functions, this could negatively affect a system that needs access to what is being blocked by the policy (Brown, 2022).

Another good practice to consider is organizing OU and domain structures. This will help to keep specific objects in the same organizational unit and avoid confusion that could be caused with an unorganized structure. One rule to follow as shared by Brown is to separate users and computers into different organizational units. This will help make the process of applying Group Policy Objects to specific computers and accounts simpler (Brown, 2022). These can also be separated into groups based upon department or branch, with each having their units for computers and users.

A similar implementation that can be applied is linking Group Policy Objects at the organizational unit level. For example, if a Group Policy Object is linked at the highest level in an organizational unit, then lower levels, or child organizational units, will be able to link the same Group Policy Objects. This is a useful tool for administrators to be able to quickly link certain policies while maintaining the current state of Group Policy Objects. If administrators decide to remove a Group Policy Object link, it is important to delete the GPO instead of solely disabling it. If done improperly, disabling the link can cause the Group Policy Object to disable across the entire domain resulting in potential issues for other users (Brown, 2022).

A few other strong practices are as follows: Consider disabling unused computers and accounts to decrease GPO processing time and reduce the chance of unused or unsecured systems or accounts from being utilized. Implement Group Policy Objects that govern the security of account credentials to ensure user accounts remain secure. Regularly backup Group Policy settings and objects to ensure that Group Policy is easily recoverable in the event of disaster. Train and inform users on practices to keep accounts and systems secure.

**Conclusion**

When considering how to best secure a network within a business or enterprise environment, there are many options administrators can choose to ensure information, systems and users remain secure. It is important to consider the positive and negative consequences that could arise with the implementation of Group Policy, and security administrators should plan as to how Group Policy would be implemented and maintained. Group Policy can be applied in both small- and large-scale organizations and can be a valuable tool to the moderation of systems and accounts within a network. At the same time, however, it can cause issues if not properly implemented and may not be easy to manage and maintain in an orderly state. Security administrators should consider both the pros and cons that are possible when implemented Group Policy Objects.

Whether deciding to implement Group Policy or not, it is important to find a way to secure information and systems on a network. In today’s world systems are constantly under the threat of attack, especially when those systems contain confidential and sensitive information. No matter if an organization chooses to implement Group Policy or some other form of management, the security of information, accounts, devices, networks, and users should always be taken seriously and considered by all security administrators.

Resources

Brown, J. (2022, April 4). 12 Group Policy Best Practices: Settings and Tips for Admins. *Varonis*. https://www.varonis.com/blog/group-policy-best-practices

Buckbee, M. (2015, June 25). Difference Between Organizational Units and Active Directory Groups. *Varonis*. https://www.varonis.com/blog/the-difference-between-organizational-units-and-active-directory-groups

Coggins, J. (2022, August 4). What is Group Policy (GPO) and What Role Does It Play in Data Security. *Lepide*. https://www.lepide.com/blog/what-is-group-policy-gpo-and-what-role-does-it-play-in-data-security/

Rickard, J. (2017, June 26). Understanding Group Policy Order. *4sysops*. https://4sysops.com/archives/understanding-group-policy-order/

Williams, M. (2012m June 5). Group Policy Not the Only Way to Manage User Activity. *Faronics*. https://www.faronics.com/news/blog/group-policy-not-the-only-way-to-manage-user-activity