# Enterprise Group Policy for Security

Sourav Mangla

MIS 517: System Security Management

April 6, 2023

Group Policy Objects are powerful tools that allow network administrators to manage the configuration of computers and users in their organization. GPOs are used to enforce policies that define security settings, control user environments, and manage software installations. These policies can be applied to specific groups of users or computers and can be customized to meet the needs of the organization. I have researched policies that can be enforced using GPOs include password complexity requirements, force logoff when logon hours expire, and force strong key protection for user keys stored on the computer. These policies play a crucial role in ensuring the security and integrity of the network.

## Password Must Meet Complexity Requirements

This group policy is a security policy that enforces the use of strong passwords for user accounts on a Windows-based network. When this policy is enabled, users will be required to create passwords that meet certain complexity requirements, such as including a combination of uppercase and lowercase letters, numbers, and special characters. When a user attempts to change or create a password that does not meet the complexity requirements, they will receive an error message and will be prompted to create a stronger password. The complexity requirements are defined in the group policy settings, which can be configured to meet the specific needs of the organization. [1]

When this policy is enabled, users will be required to create passwords that meet the defined complexity requirements. This helps to ensure that user accounts are protected with strong and secure passwords, reducing the risk of unauthorized access to the network. When this policy is disabled, users will not be required to create passwords that meet any complexity requirements. This can result in weaker passwords that are easier to guess or crack, increasing the risk of unauthorized access to the network.

This group policy includes several configurable options, such as password length, complexity, and history. These options can be customized to meet the specific needs of the organization. It is generally recommended that organizations enable this group policy with strong password complexity requirements. An organization would use these settings to improve the security of user accounts on their network. Weak passwords are a common target for attackers seeking to gain unauthorized access to sensitive data or systems. By enforcing strong password complexity requirements, organizations can significantly reduce the risk of password-related security incidents.

**System Cryptography: Force Strong Key Protection for User Keys Stored on the Computer**

This group policy setting is a security policy that can be configured using Group Policy Objects in a Windows Active Directory domain. This policy setting is designed to ensure that user keys stored on the computer are protected with strong encryption.

When enabled, this policy setting forces Windows to use strong key protection for all user keys stored on the computer.[2] This means that the keys are protected with a password or smart card, and the password or smart card must be provided to access the key. This helps to prevent unauthorized access to sensitive information, such as private keys used for encryption and digital signatures. When disabled, Windows will not enforce strong key protection for user keys stored on the computer. This means that user keys can be accessed without a password or smart card, which can pose a security risk if the computer is lost or stolen.

The recommended setting is to enable this policy setting to ensure that user keys stored on the computer are protected with strong encryption. By enforcing strong key protection, organizations can ensure the confidentiality and integrity of sensitive information and help prevent data breaches and other security incidents.

## Network Security: Force Logoff When Logon Hours Expire

This group policy setting is a security policy that can be configured using Group Policy Objects (GPOs) in a Windows Active Directory domain. This policy setting is designed to ensure that users are automatically logged off from their computers when their designated logon hours have expired.[3]

When enabled, this policy setting forces Windows to automatically log off users from their computers when their designated logon hours have expired. This helps to prevent unauthorized access to the network outside of business hours and can also help reduce the risk of data theft or loss. When disabled, Windows will not automatically log off users when their designated logon hours have expired. This means that users can continue to access the network outside of business hours, which can pose a security risk if there are no controls in place to prevent unauthorized access.

The recommended setting is to enable this policy setting to ensure that users are automatically logged off from their computers when their designated logon hours have expired. By enforcing this policy, organizations can ensure that only authorized personnel have access to the network during business hours and help prevent data breaches and other security incidents. The available options for this policy setting are "Enabled" and "Disabled." When enabled, Windows will automatically log off users from their computers when their designated logon hours have expired. When disabled, Windows will not automatically log off users when their designated logon hours have expired.

## Conclusion

In conclusion, Group Policy Objects are an essential tool for network administrators to manage the configuration of computers and users in their organization. The policies enforced

using GPOs, such as password complexity requirements, force logoff when logon hours expire, and force strong key protection for user keys stored on the computer, play a crucial role in ensuring the security and integrity of the network. By enforcing these policies, network administrators can significantly reduce the risk of unauthorized access to the network and prevent data theft or loss.

## References

[1]. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy settings/password-must-meet-complexity-requirements

[2]. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/system-cryptography-force-strong-key-protection-for-user-keys-stored-on-the-computer

[3]. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-force-logoff-when-logon-hours-expire