



Hardening- Lab 2

Group 4

Nguyen Ngo - AE8880

Dung Doan - AA7785

Syed Fawaz - AD9946

Jasper (Franciscus) van de Klundert - AG9056

Sanka De Silva - AC4892

Exercise Lab 2

Hardening

3/3/2025

Bachelor's Program of Information and Communication Technology

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 3 |
| 2 | Theory of the Lab | 3 |
| 2.1 | Microsoft Security Compliance Toolkit | 4 |
| 2.2 | Group Policy Objects (GPO) | 4 |
| 2.3 | Fine-grained password policies (FGPP) | 5 |
| 2.4 | Other terms | 5 |
| 3 | Working process..... | 6 |
| 3.1 | W11 hardening..... | 6 |
| 3.2 | Blocking Remote Access..... | 8 |
| 3.3 | Restricting Modification of Workstation Settings..... | 9 |
| 3.4 | Fine grained password policies | 16 |
| 4 | Conclusion..... | 21 |
| | References | 23 |

Figures

| | | |
|-----------|---|----|
| Figure 1 | WS01 24H2 with login jaklundert | 6 |
| Figure 2 | Update Policy(gpupdate) | 8 |
| Figure 3 | Blocking Remote Access..... | 8 |
| Figure 4 | Blocked remote access..... | 9 |
| Figure 5 | Limit_controlPanel GPO | 10 |
| Figure 6 | Restricting the Control Panel | 11 |
| Figure 7 | Allowed settings..... | 12 |
| Figure 8 | Employee Control Panel..... | 13 |
| Figure 9 | Visible pages in the Settings menu | 14 |
| Figure 10 | Settings that are visible to the worker..... | 15 |
| Figure 11 | Local Log on..... | 16 |
| Figure 12 | New security group for password policies..... | 17 |
| Figure 13 | Student_Password Properties | 18 |
| Figure 14 | Added Password Settings..... | 18 |
| Figure 15 | Adjusted Settings | 19 |
| Figure 16 | Affected Group..... | 20 |

| | |
|--------------------------------|----|
| Figure 17 Powershell test..... | 21 |
|--------------------------------|----|

1 Introduction

In this lab assignment, our goal is to harden a Windows 11 system to enhance its security. We will use a chosen hardening guide, with a focus on Microsoft's recommendations, to implement Group Policy Object (GPO) hardenings and other suggested security measures. To evaluate our progress, we will compare the system's initial and final states, potentially using the Microsoft Security Compliance Toolkit. Throughout the process, we will document our steps clearly, including relevant theories and visual evidence.

2 Theory of the Lab

Implementing hardening can be complex and time-consuming, especially in larger organizations and more complex environments. Some security features may cause additional load on the system and

affect its performance. Additionally, changes in system configurations can disrupt normal operations. When implementing hardening, it is also important to adhere to industry standards such as the Computer Information Security (CIS) Benchmarks guidelines. There is also a wide range of tools, scripts, and automations available to facilitate the implementation and analysis of the necessary changes. (Shruti456rawal. 2024).

2.1 Microsoft Security Compliance Toolkit

The Security Compliance Toolkit (SCT) is a sophisticated tool developed by Microsoft, specifically aimed at easing the management of Group Policy Objects (GPOs) and security configurations for administrators. This toolkit allows users to compare their current GPOs against Microsoft's recommended security guidelines and adjust settings to align with those recommendations. (Microsoft Security Compliance Toolkit - How to Use, 2024)

Additionally, the toolkit includes a feature called Policy Analyzer, a powerful utility within Microsoft SCT. Policy Analyzer is designed to scrutinize and contrast GPO rules, highlighting overlapping settings and identifying conflicts between different group policies. It can also compare GPO settings at the domain level to those applied locally, enabling administrators to spot any discrepancies or changes that may affect system compliance. This functionality makes it easier to detect deviations and ensures consistent security policies across different levels of the organization. (Microsoft Security Compliance Toolkit - How to Use, 2024)

2.2 Group Policy Objects (GPO)

Group Policy Objects (GPOs) are a central component of Microsoft's Active Directory infrastructure. They enable the definition of managed settings for users and computers. When designed and implemented correctly, they can significantly enhance the security of the system and improve the performance of the IT infrastructure. (Group Policy Objects, 2018)

Here are a few examples of best practices for Group Policy Objects:

1. **Division of Organizational Units (OUs)** into users and computers: Separating users and computers into distinct OUs facilitates the application of different policies. For instance, computer policies can be applied to every computer in the environment, and user policies to every user or just specific groups such as HR or SALES.
2. **Clear naming conventions for GPOs:** Use descriptive, clear names for GPOs to easily understand their purpose from the name. For example, user policies might start with "U_" and computer policies with "C_", such as "U_user_policy" and "C_computer_policy". This naming helps clarify which target each GPO affects.
3. **GPO prioritization:** GPOs are applied in the order LSDOU (Local, Site, Domain, OU). Settings at the local level have the lowest priority, while those at the OU level have the highest priority. This prioritization determines which settings ultimately take effect.

4. **Restricting access to the Control Panel:** By limiting access to the Control Panel, you can prevent regular users from making changes to system settings, a task that should be reserved for administrators. This prevents errors made by regular users and enhances security.
5. **Preventing the use of removable media:** Devices such as USB drives can pose a security risk as they may spread malware. By applying GPOs, it's possible to block their use. Considerations include how frequently removable media are used and how their restrictions might impact usability. (Group Policy Best Practices, 2024)

Additionally, it's beneficial to regularly update GPOs to align with evolving security threats and to audit them to ensure they are achieving the intended security posture without unnecessary restrictions that could hinder user productivity.

2.3 Fine-grained password policies (FGPP)

Fine-grained password policies are a feature of Active Directory (AD) that allows for the specification of different password and account lockout rules for individual users or groups within an organization. This enables more flexible and precise management of password security. (Configure fine-grained password policies for Active Directory Domain Services, 2024)

2.4 Other terms

A Windows domain covers all the devices within an environment and their centralized management. A domain allows users to log into any device within the domain, making login domain-specific, not device-specific. Domains can be managed using groups and rules that can be applied across the entire area at once, simplifying maintenance. (Hyytiäinen, 2024)

Local Admin is the administrator of a specific endpoint, who is authorized to make changes only to that device within the domain. A Domain Admin is the admin for the entire domain, capable of making changes across the entire domain. (Hyytiäinen, 2024)

Privileged Access Management (PAM) is a cybersecurity solution that protects an environment by managing users with higher access rights and auditing their activities. By controlling ordinary users' access to critical system settings, the system can be protected against potential threats such as lateral movement by hackers, or unnecessary access to firewall settings or control panel management by certain staff groups. High-level access rights on user accounts are a security risk if cyber attackers gain access to account credentials. With extensive privileges, these accounts can steal confidential information from the organization and alter critical settings on devices within the domain. Therefore, the protection of these accounts should be significantly stronger, for instance, through multi-factor authentication (MFA), compared to ordinary domain users. (Hyytiäinen, 2024)

RDP (Remote Desktop Protocol) is a protocol that enables a remote connection to another computer over a network. RDP uses the encrypted TCP (Transmission Control Protocol). (Understanding the Remote Desktop Protocol (RDP), 2023)

Gpupdate /force is a command that forces immediate updating of group policies on a computer. (gpupdate, 2023)

Gpresult /r is a command that displays the GPOs applied to a computer. (gpresult, 2023)

3 Working process

1. Downloaded the Security baseline
- We downloaded the windows security baseline

3.1 W11 hardening

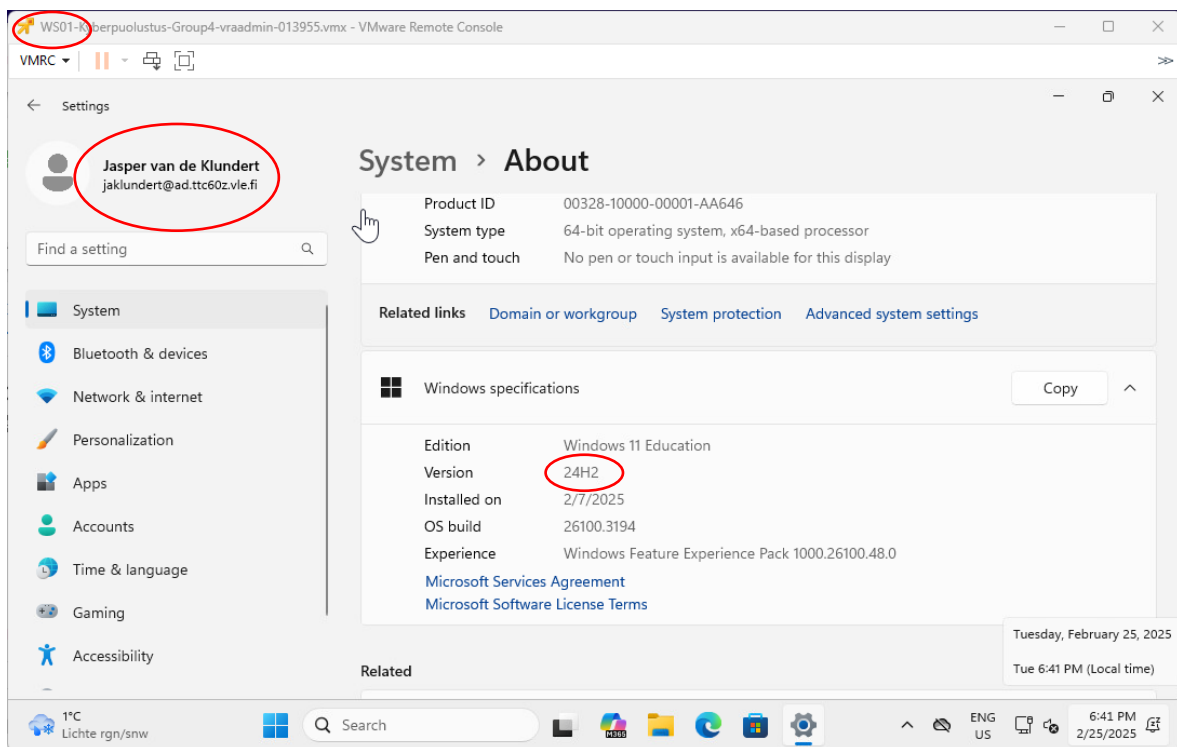
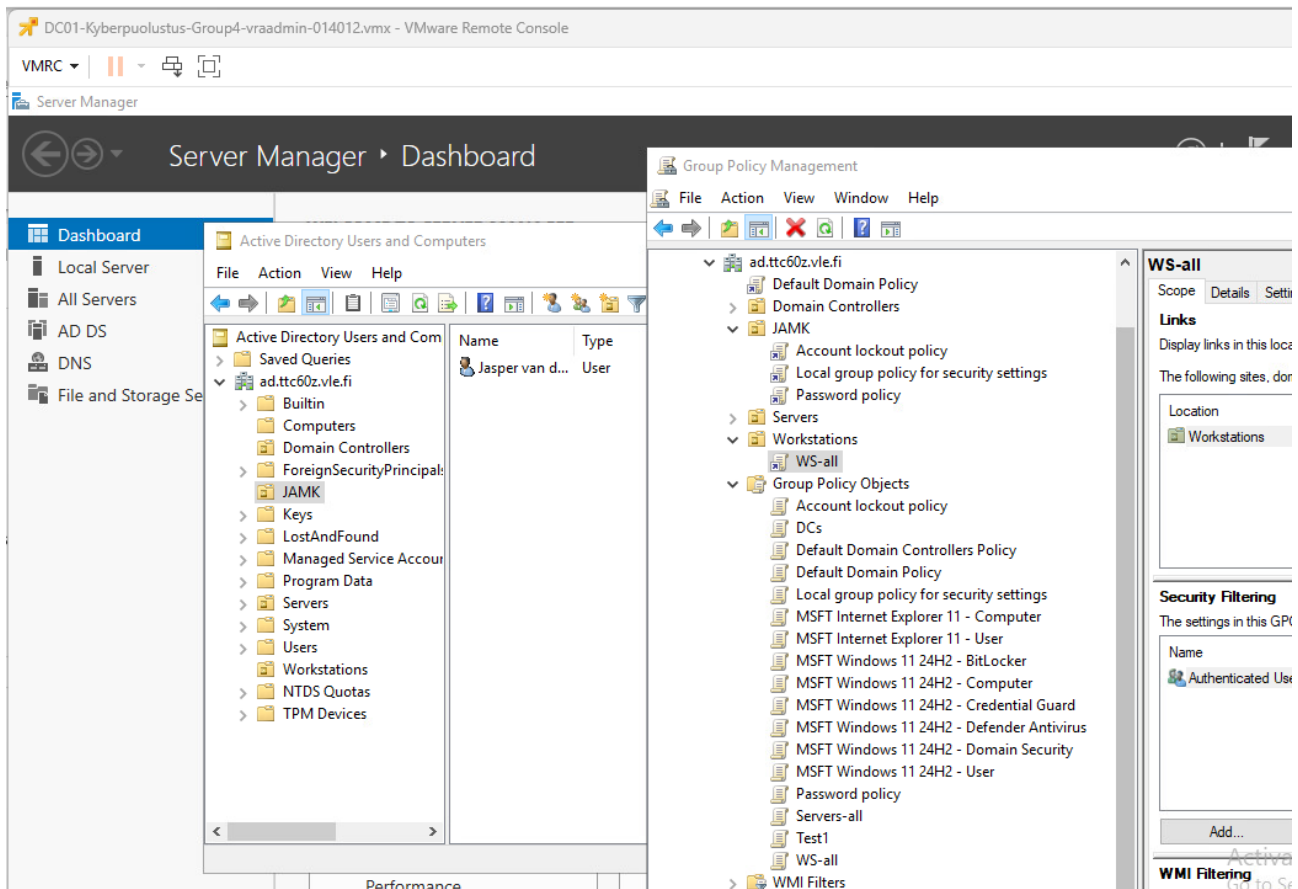
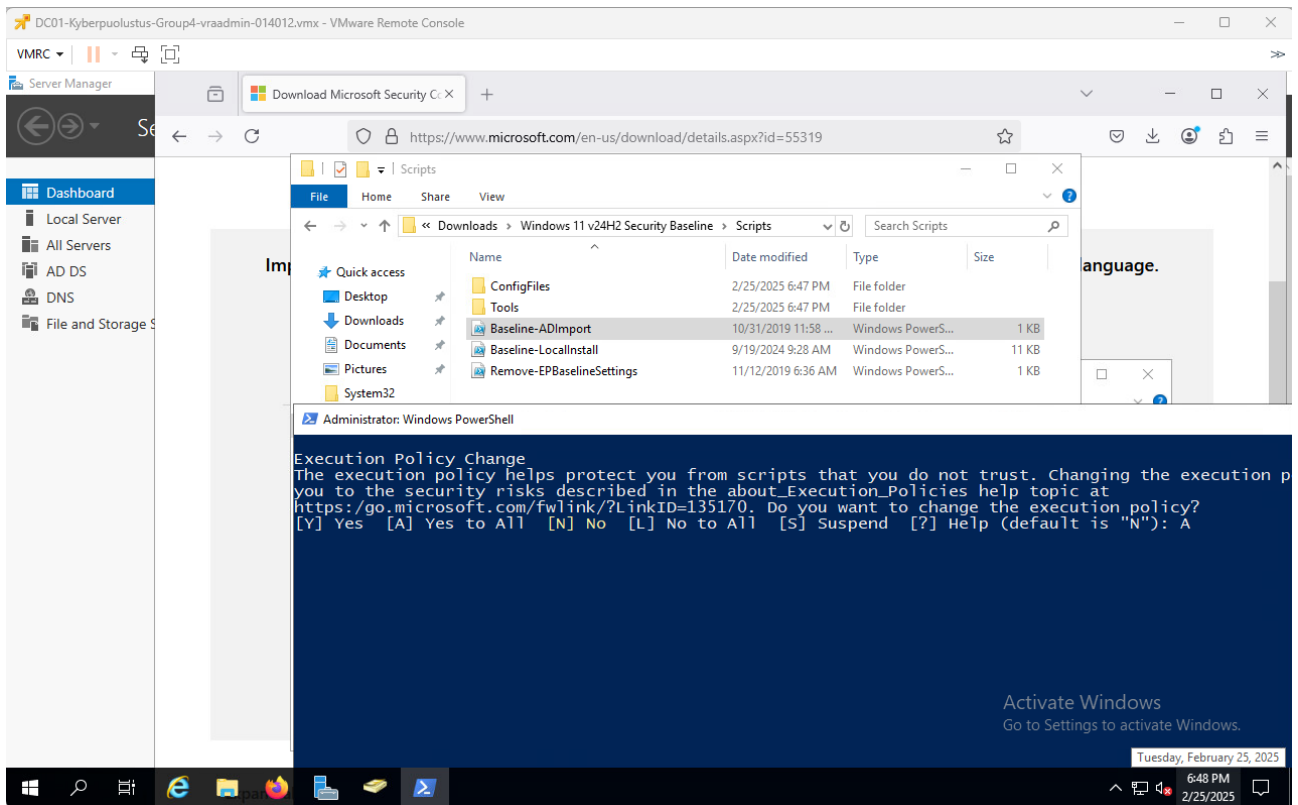


Figure 1 WS01 24H2 with login jaklundert



We ran the command `gpupdate /force` on the WS01 workstation using the command prompt to ensure that the policies were updated and applied.

```
C:\Users\Administrator>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
```

Figure 2 Update Policy(gpupdate)

3.2 Blocking Remote Access

We wanted to prevent remote access for users who do not need it, as remote access is a common security risk that attackers use to penetrate systems. Therefore, we created a new rule that restricts this access for employees. (Figure)

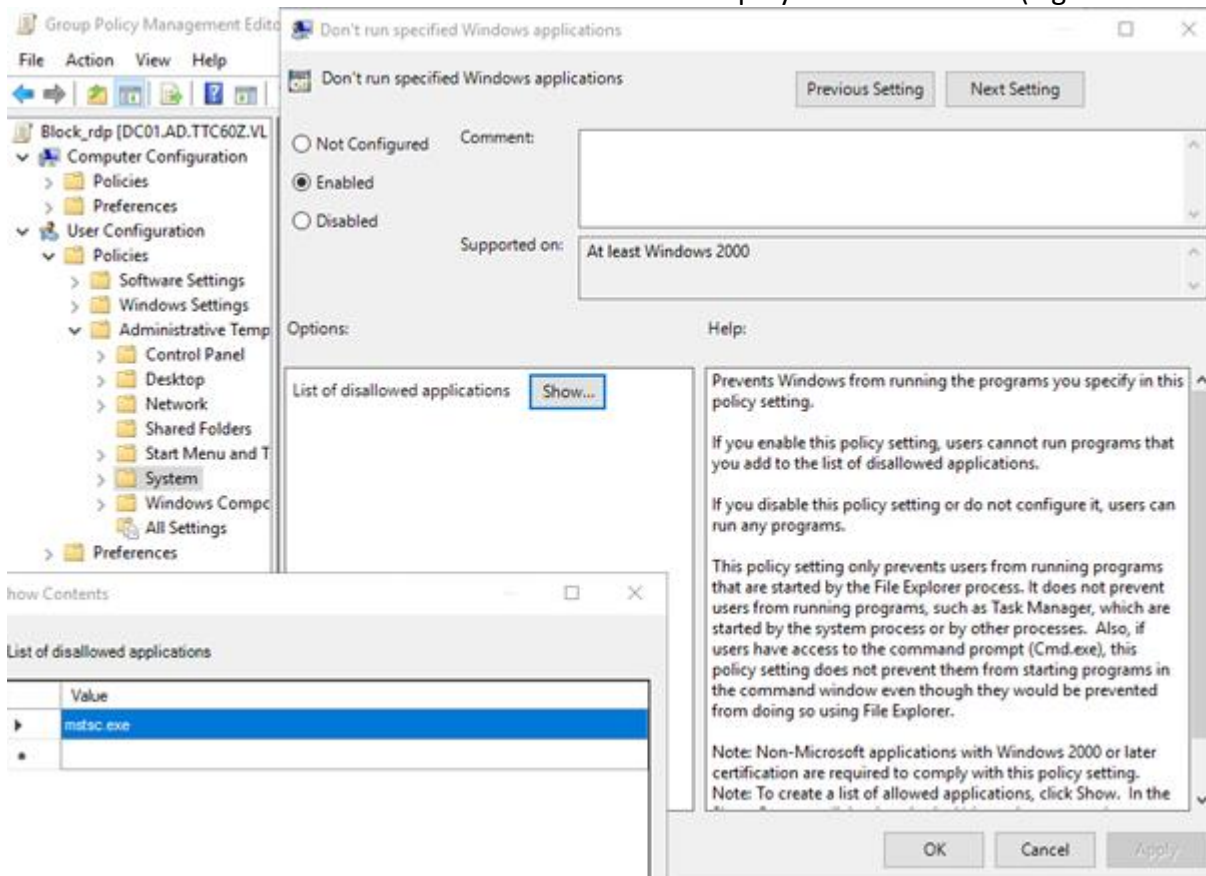


Figure 3 Blocking Remote Access

We tried to initiate remote access after logging into WS01 with an employee's credentials. This triggered an error message indicating that remote access was disabled. We also checked the policies applied to the user through the command prompt using the command `gpresult /r`, and there we found the remote access restriction policy we had created. (Figure)

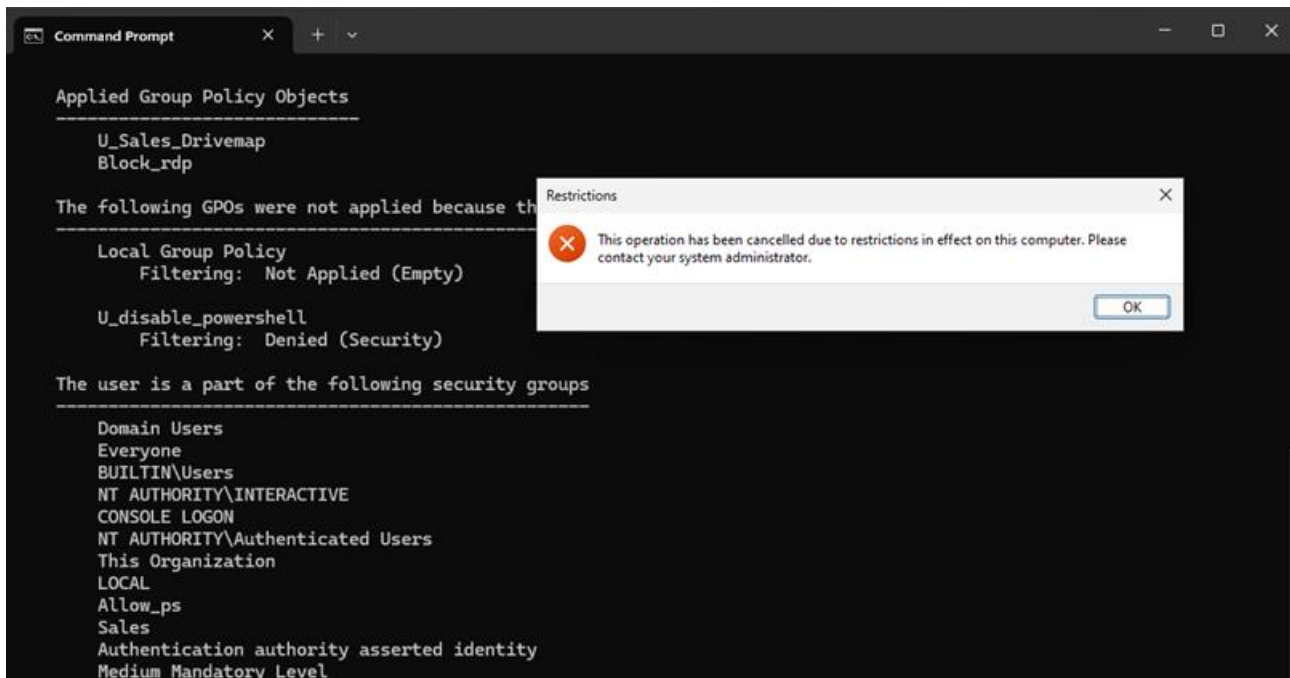


Figure 4 Blocked remote access

3.3 Restricting Modification of Workstation Settings

Not all users need access to all the settings on a workstation, so we decided to restrict the visibility of these settings. We created a new GPO called Limit_controlPanel and opened the Group Policy

Editor.

(Figure)

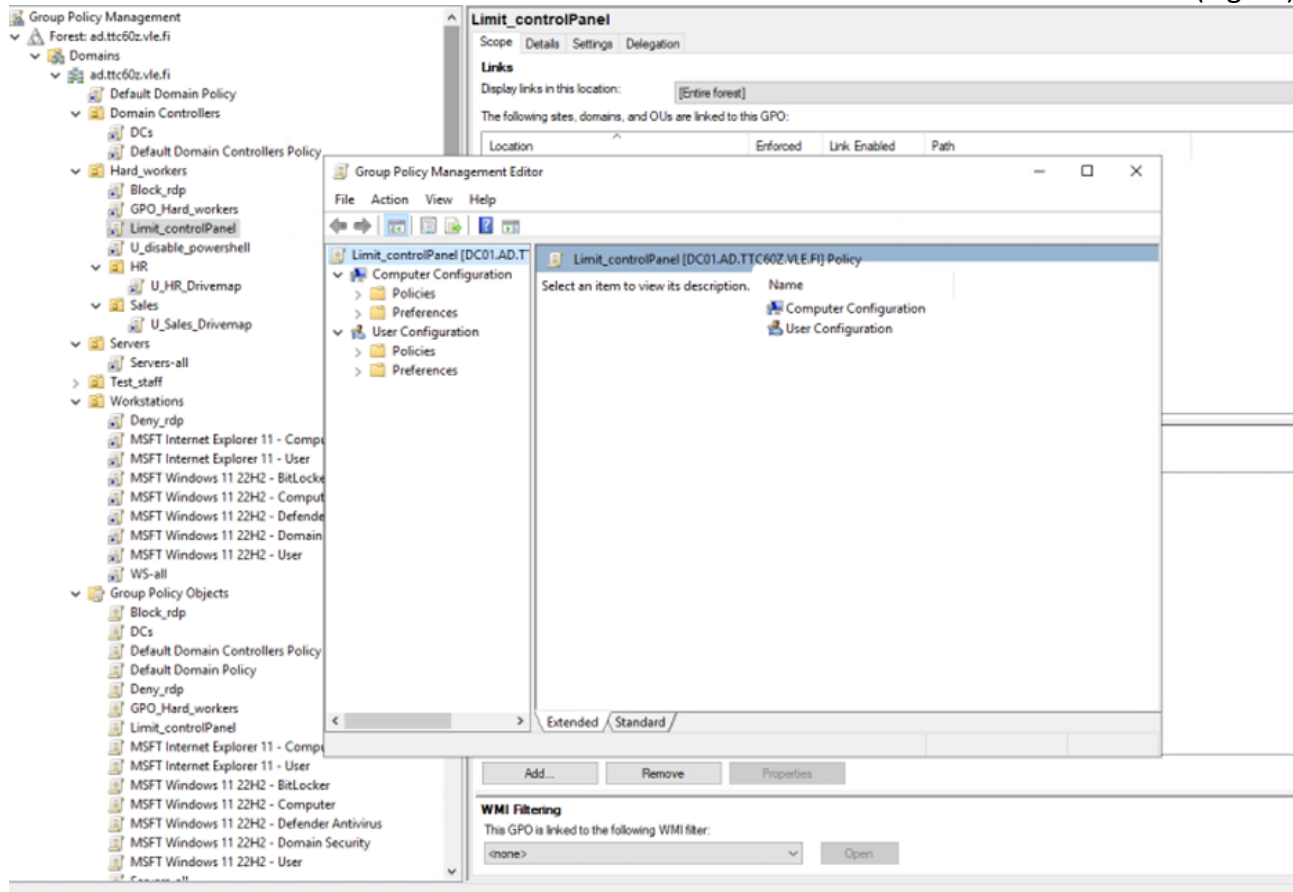


Figure 5 Limit_controlPanel GPO

We modified the setting "Show only specified Control Panel items," which allowed us to define which panel settings are visible to the user.

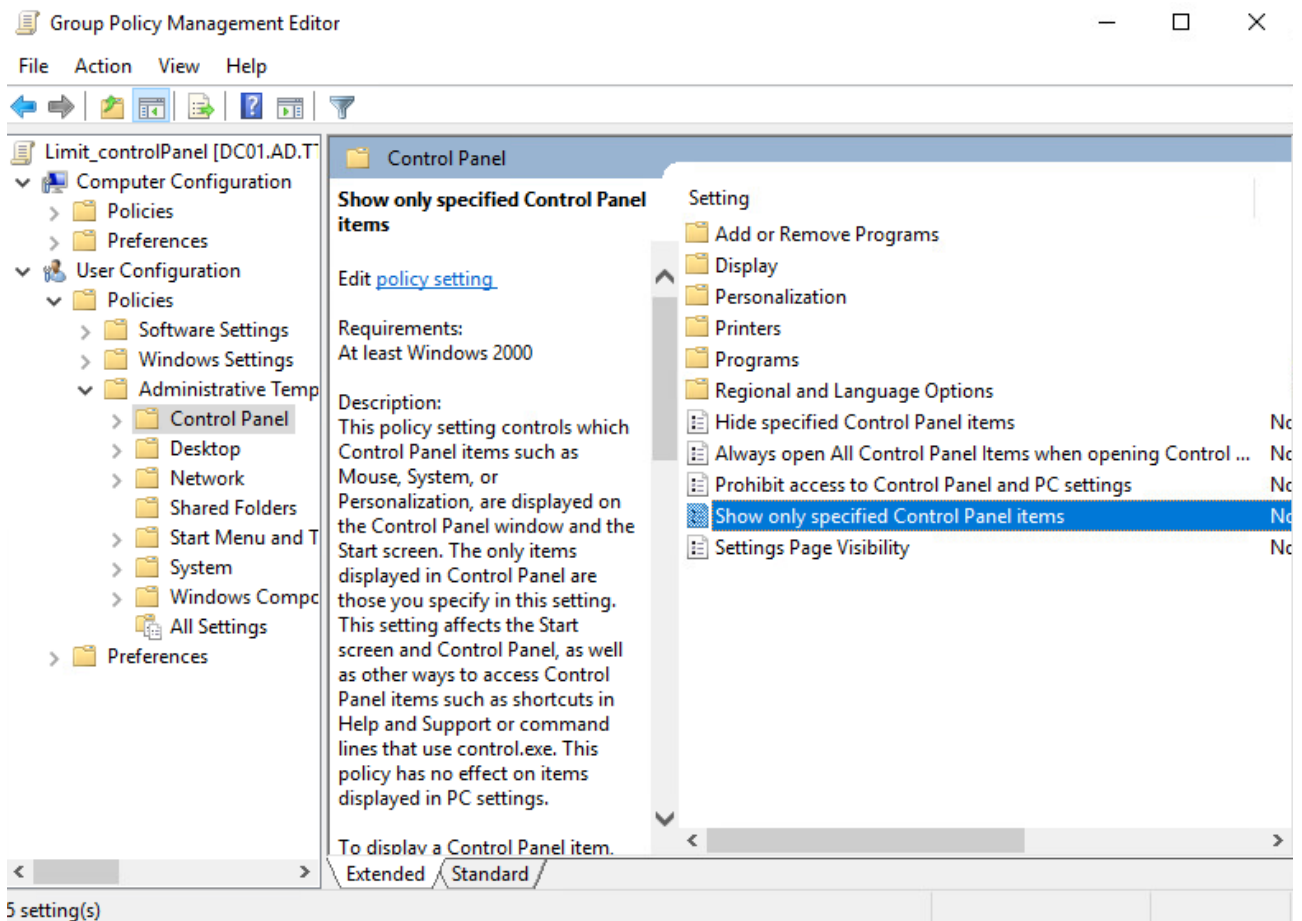


Figure 6 Restricting the Control Panel

We switched the setting to the enabled state. We added items to the control panel settings visible to users by opening the options window from the show button. We selected items as needed

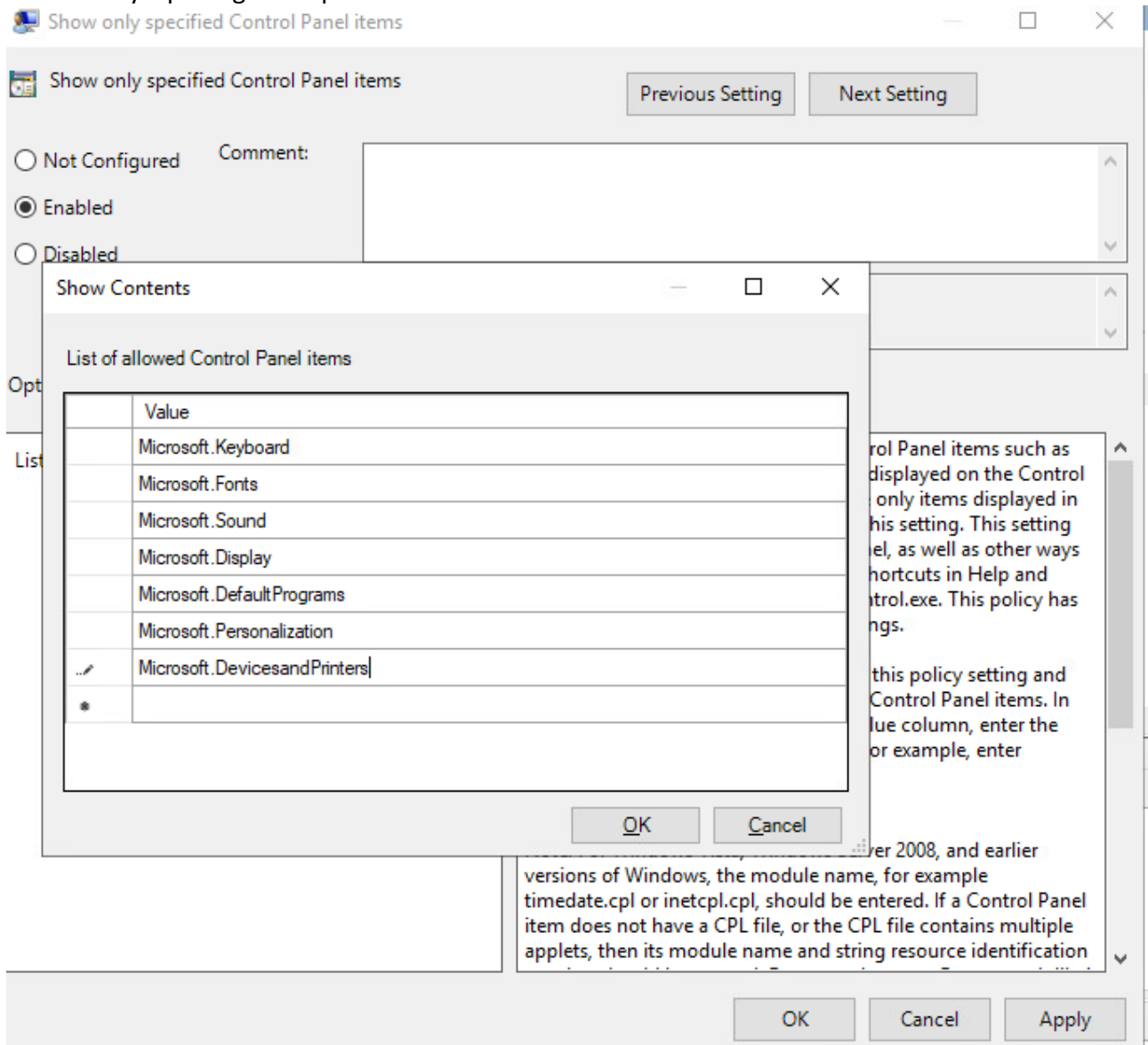


Figure 7 Allowed settings

We logged onto WS01 with an employee's credentials and the settings had taken effect. The user is now able to modify only a few settings via the control panel.

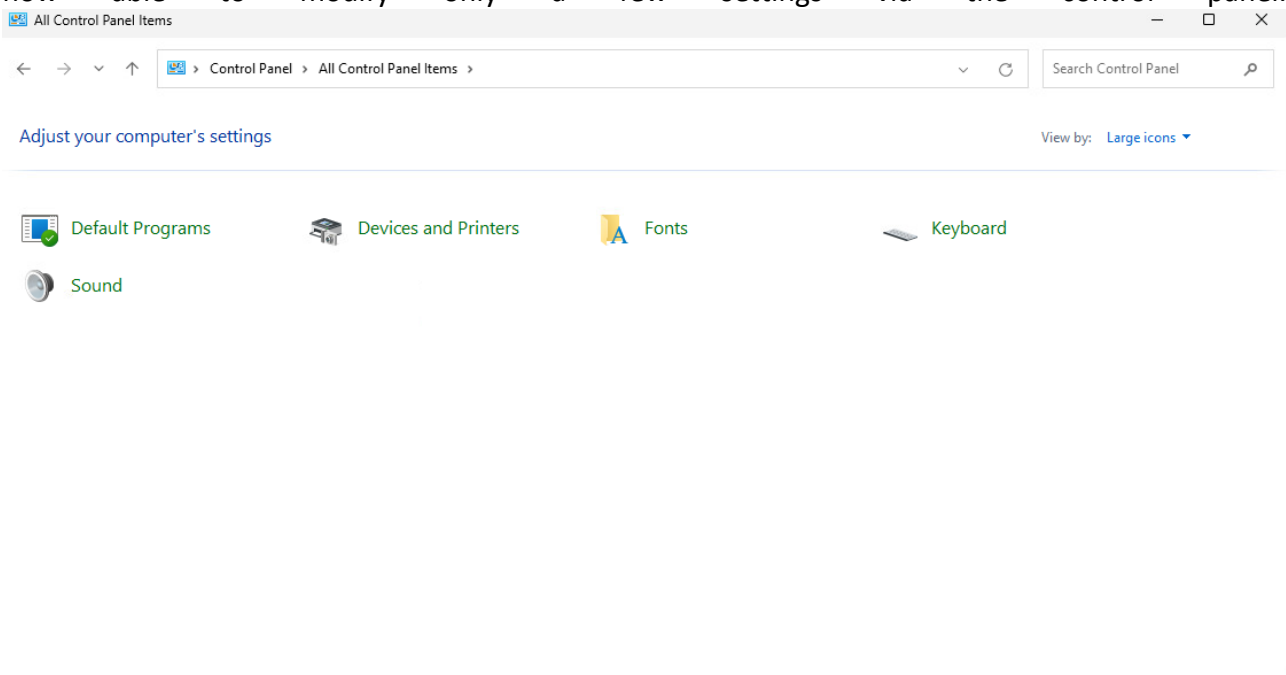


Figure 8 Employee Control Panel

We also limited the employees' ability to modify workstation settings through the Settings menu. We enabled the "Settings page visibility" option and listed the pages that we wanted to appear in

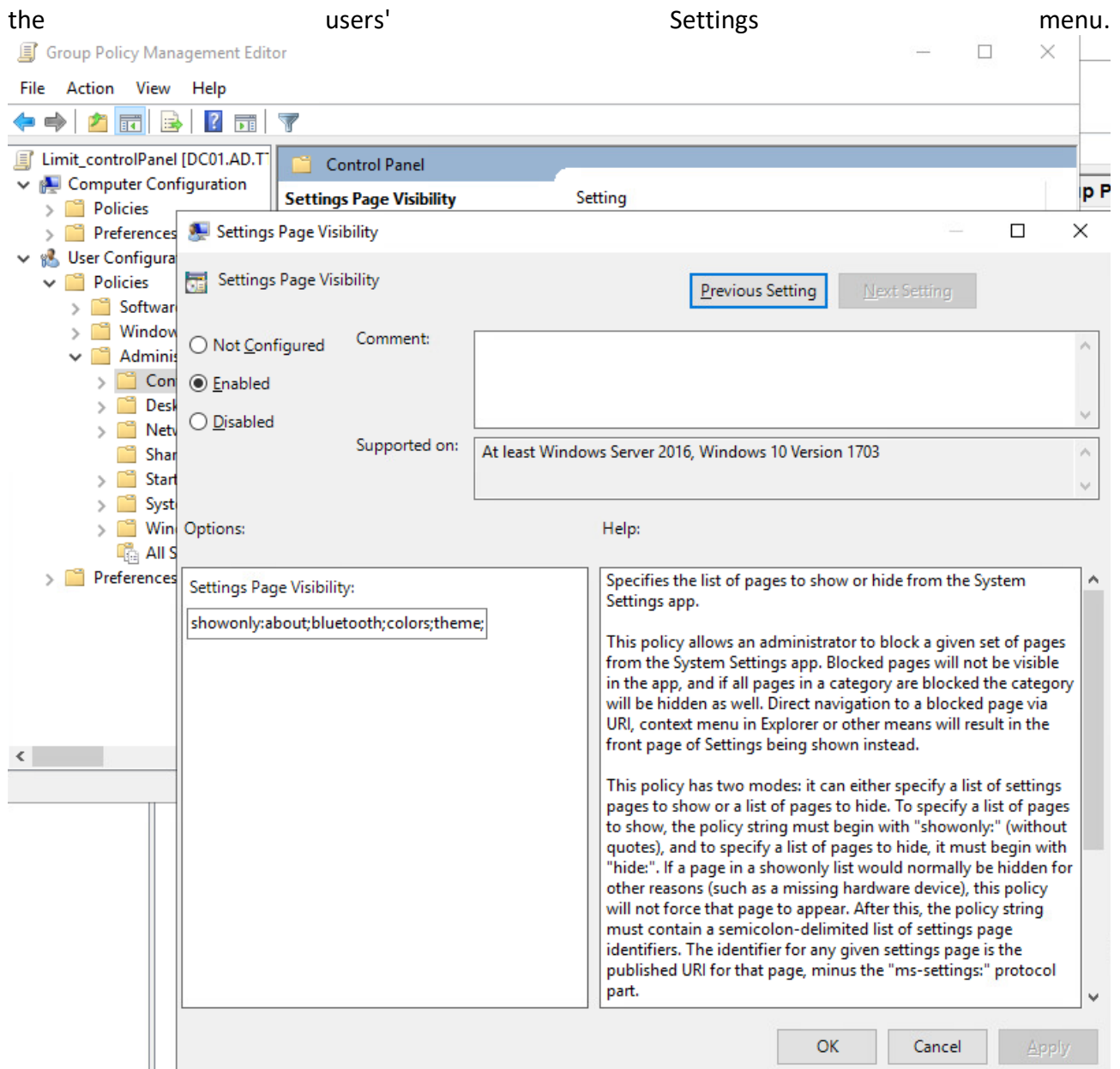


Figure 9 Visible pages in the Settings menu

After the settings took effect, the employees' Settings menu looked like the Figure

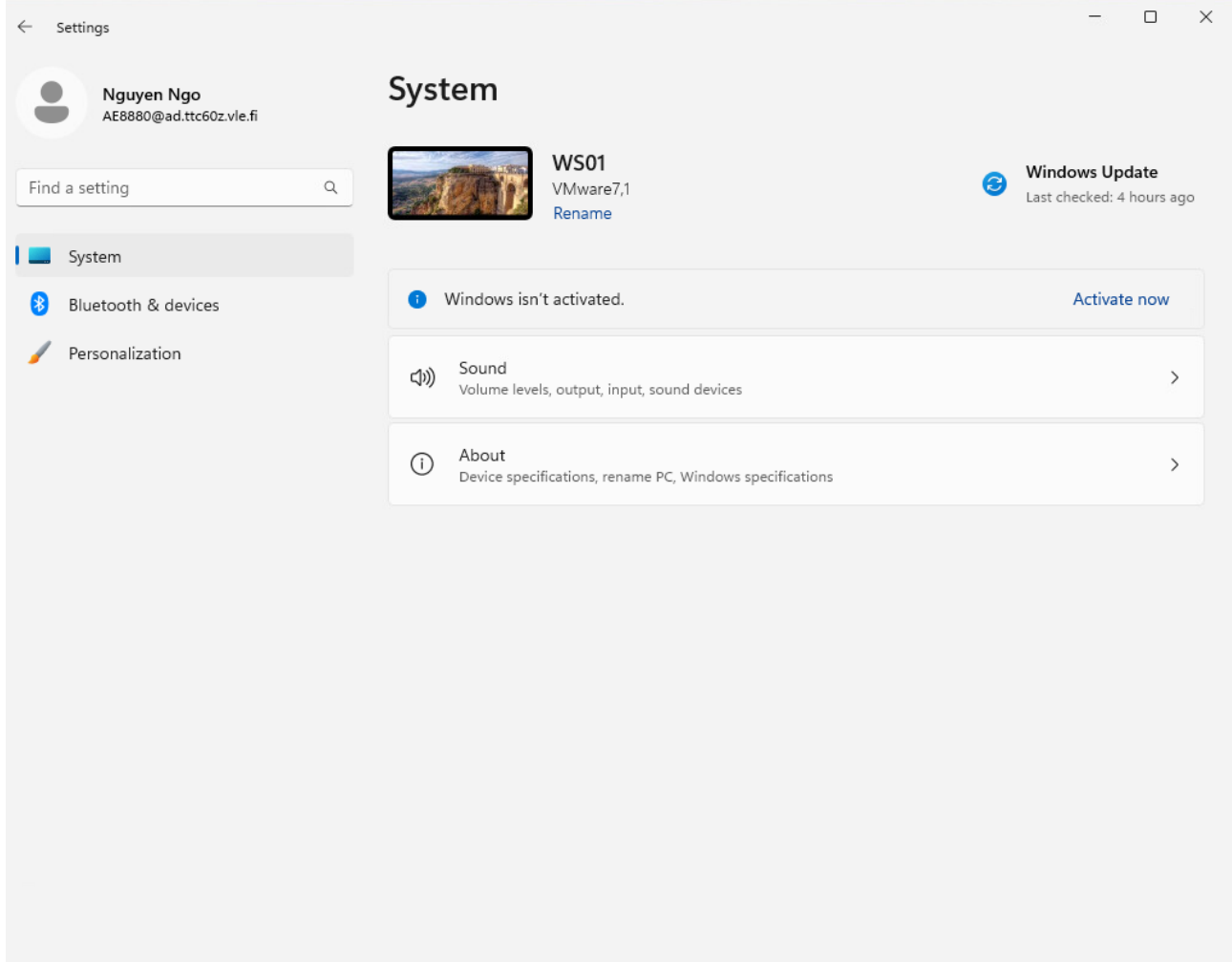


Figure 10 Settings that are visible to the worker

We noticed that the file server SRV01 could be logged in with any credentials, and we decided to for the time being, leave the login only to administrators with the Allow log on locally setting.

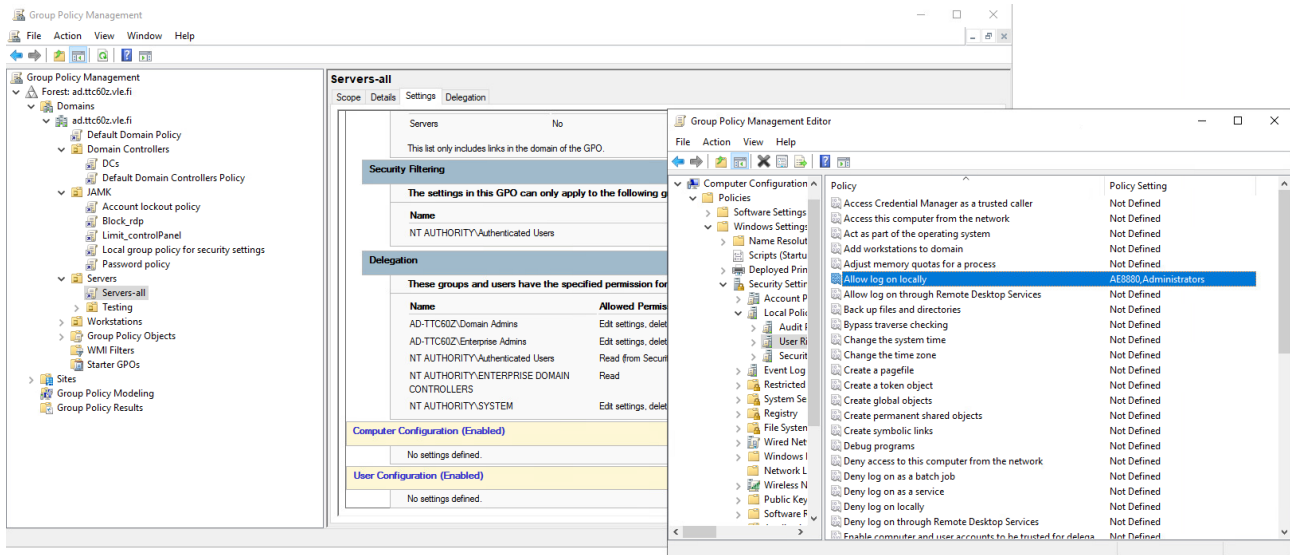
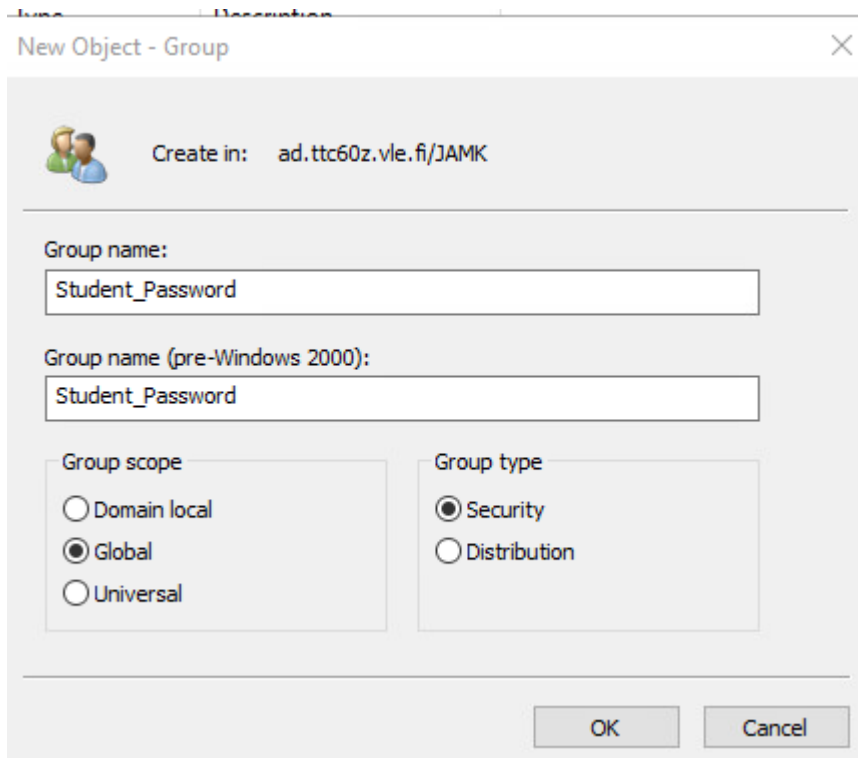


Figure 11 Local Log on

3.4 Fine grained password policies

To create password policies for a specific user group, we employed the fine-grained password policy method. We first created a security group, which we added to all students so that the password policies only apply to them. This setting would normally take effect for everyone, but we do not want to change the passwords of the administrators, as this is prohibited in the guidelines. (Figure). It would be advisable to name the security group starting with 'U_', to clarify the targeting of the policy to users.



The screenshot shows the 'New Object - Group' dialog box in Active Directory. The 'Create in' field is set to 'ad.ttc60z.vle.fi/JAMK'. The 'Group name' and 'Group name (pre-Windows 2000)' fields both contain 'Student_Password'. Under 'Group scope', the 'Global' radio button is selected. Under 'Group type', the 'Security' radio button is selected. The 'OK' and 'Cancel' buttons are at the bottom right.

Create in: ad.ttc60z.vle.fi/JAMK

Group name:
Student_Password

Group name (pre-Windows 2000):
Student_Password

Group scope

- ☐ Domain local
- ☒ Global
- ☐ Universal

Group type

- ☒ Security
- ☐ Distribution

OK Cancel

Figure 12 New security group for password policies

We added the created group to our student' users. We also moved the previously created AD group under the JAMK OU.

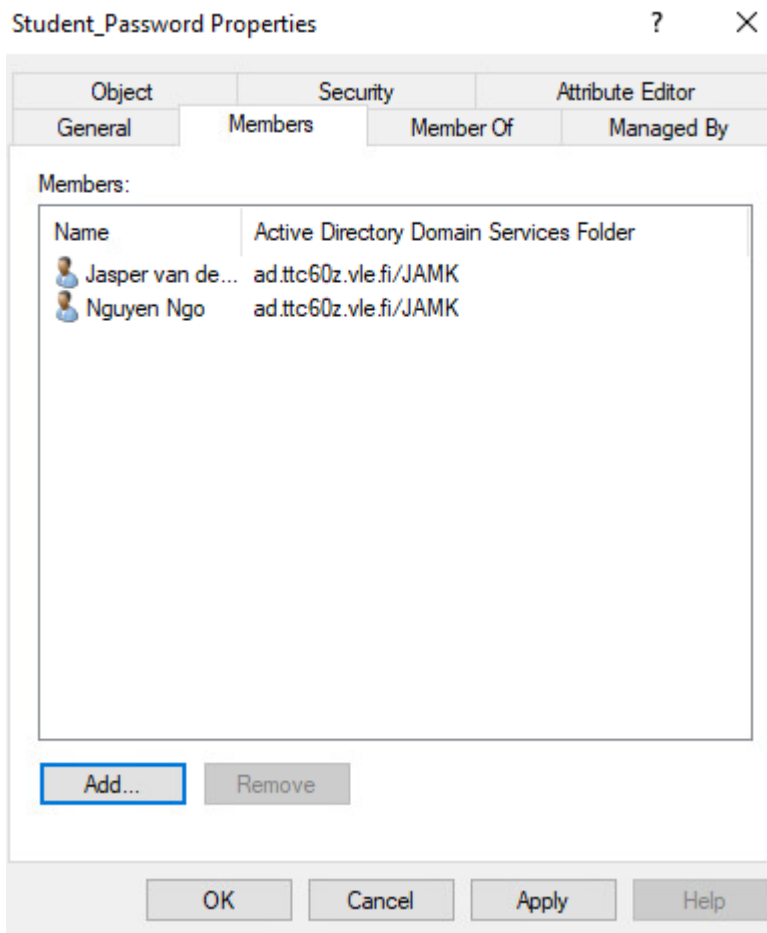


Figure 13 Student_Password Properties

We opened the Admin Directory Administrative Center on DC01 and navigated to the System\Password Settings Container where we created a new password policy.

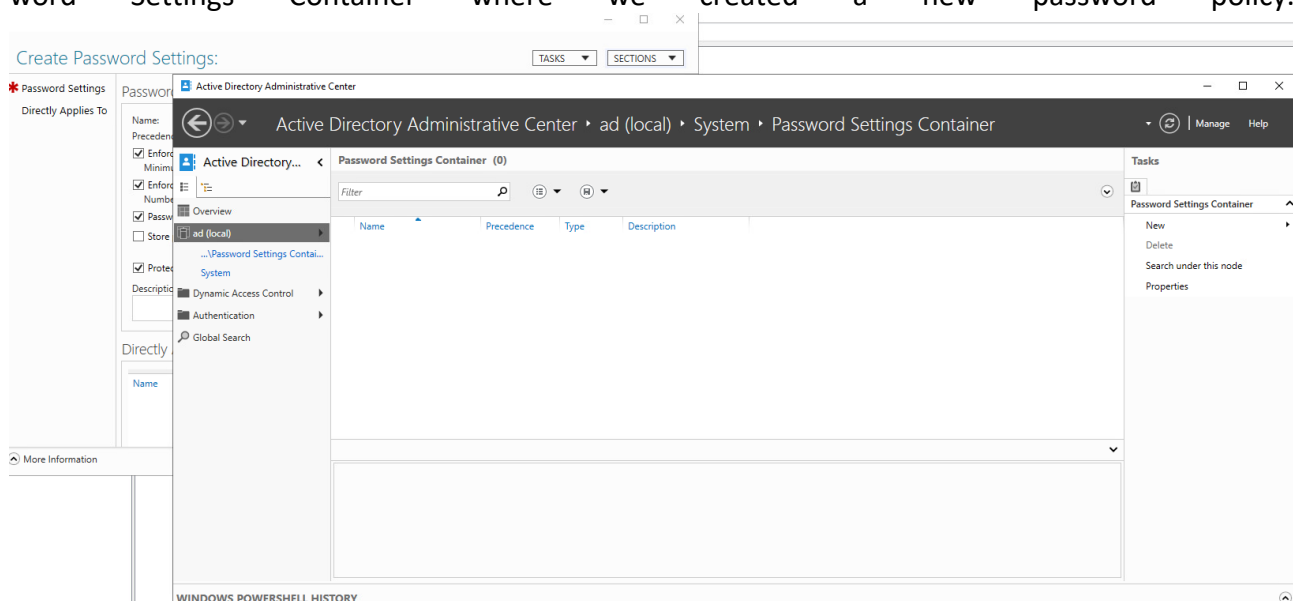


Figure 14 Added Password Settings

We entered the restrictions for the password policy along with the group it applies to. We wanted the students' passwords to be at least 10 characters long, to be changed every 42 days, and that old passwords could not be reused.

Create Password Settings: Student_passwd_policy

Password Settings

Directly Applies To

Name: * Student_passwd_policy
Precedence: * 10

☒ Enforce minimum password length
Minimum password length (characters): * 10

☒ Enforce password history
Number of passwords remembered: * 24

☒ Password must meet complexity requirements

☐ Store password using reversible encryption

☒ Protect from accidental deletion

Description:

Password age options:

☒ Enforce minimum password age
User cannot change the password withi... * 1

☒ Enforce maximum password age
User must change the password after (... * 42

☒ Enforce account lockout policy:
Number of failed logon attempts allowed: * 4
Reset failed logon attempts count after (m... * 30
Account will be locked out
☐ For a duration of (mins): * 30
☒ Until an administrator manually unlocks the account

Directly Applies To

| Name | Mail |
|------------------|------|
| Student_Password | |

Add...
Remove

More Information

OK Cancel

Figure 15 Adjusted Settings

When we went to view the password settings affecting the Student_Password group in the password settings section, we saw the password policy we had implemented there.

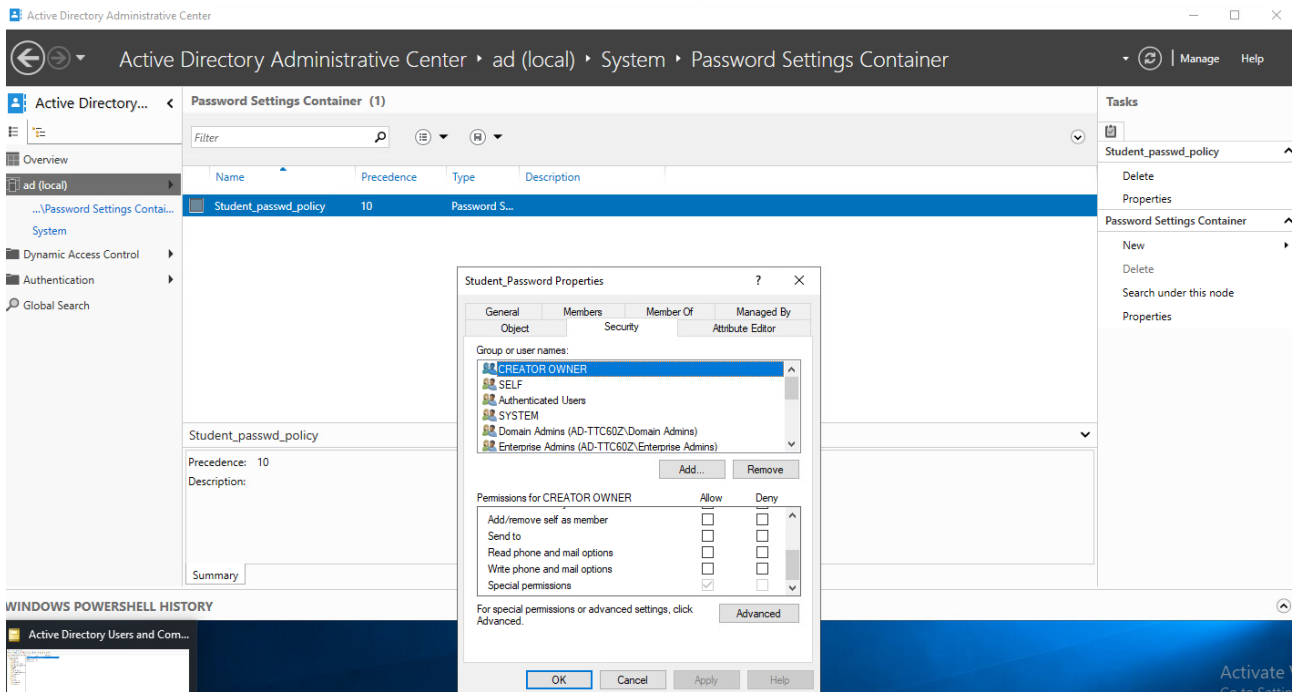
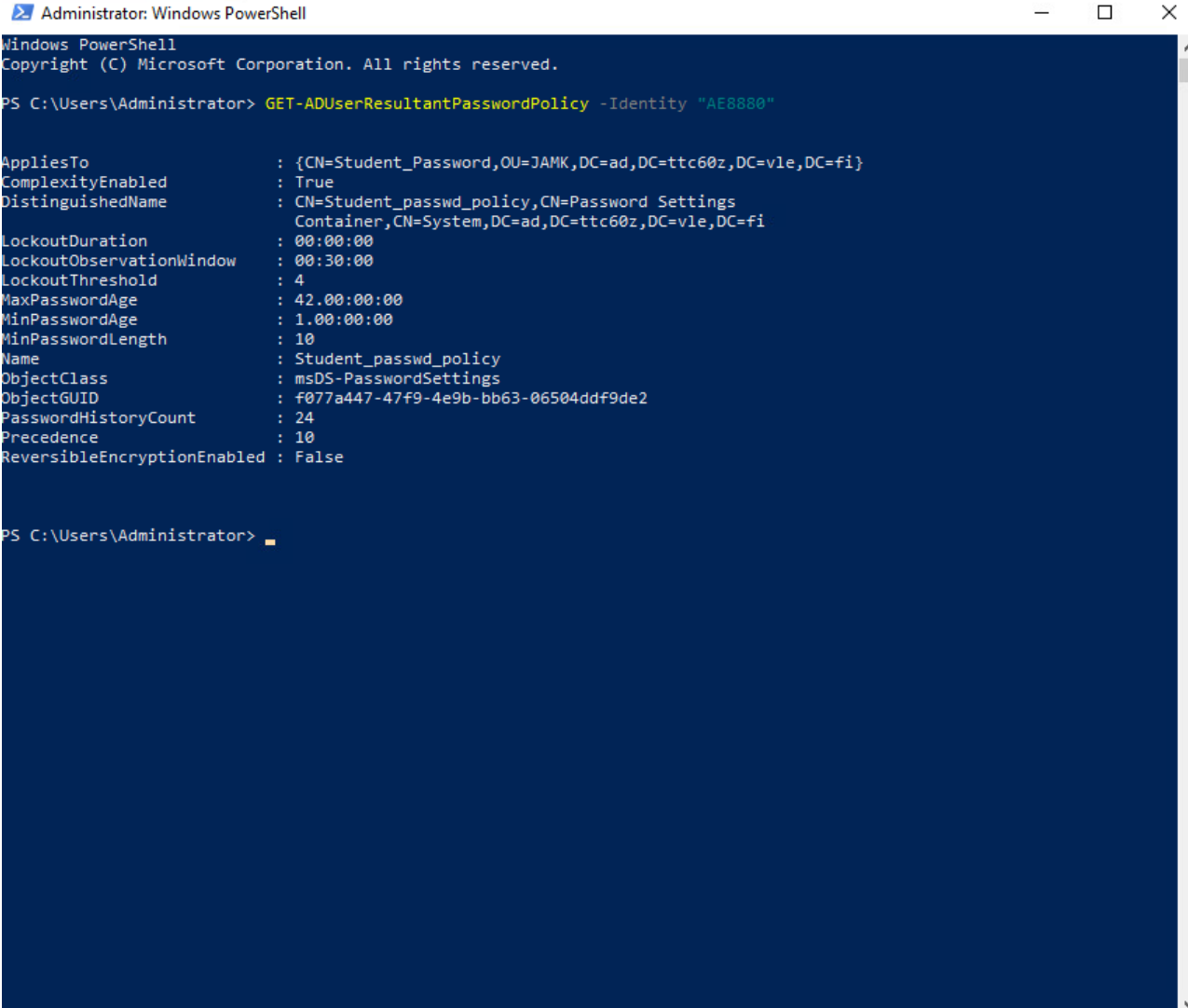


Figure 16 Affected Group

We ran a PowerShell command and confirmed that the password policy had been implemented for the students.



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> GET-ADUserResultantPasswordPolicy -Identity "AE8880"

AppliesTo           : {CN=Student_Password,OU=JAMK,DC=ad,DC=ttc60z,DC=vle,DC=fi}
ComplexityEnabled    : True
DistinguishedName    : CN=Student_passwd_policy,CN=Password Settings
                    : Container,CN=System,DC=ad,DC=ttc60z,DC=vle,DC=fi
LockoutDuration      : 00:00:00
LockoutObservationWindow : 00:30:00
LockoutThreshold      : 4
MaxPasswordAge       : 42.00:00:00
MinPasswordAge       : 1.00:00:00
MinPasswordLength    : 10
Name                 : Student_passwd_policy
ObjectClass           : msDS-PasswordSettings
ObjectGUID           : f077a447-47f9-4e9b-bb63-06504ddf9de2
PasswordHistoryCount  : 24
Precedence            : 10
ReversibleEncryptionEnabled : False

PS C:\Users\Administrator>

```

Figure 17 Powershell test

4 Conclusion

In our second hardening lab, we explored hardening techniques and utilized Microsoft's Security Compliance Toolkit to implement GPO hardenings. This experience enhanced our understanding of how GPOs behave and how their settings can be modified.

A key insight from this lab was the versatility and efficacy of Group Policy Objects (GPOs) in managing organizational security. GPOs enable centralized management and specification of security settings across numerous workstations and user groups, which diminishes the chance of human errors and boosts overall security management. This was particularly evident when we managed to block RDP access for certain user groups and limited access to Control Panel and settings menus, which minimizes misuse risks and streamlines the user experience.

Moreover, learning about password policies (Fine-Grained Password Policies) was a novel aspect for us. These policies allowed us to customize password requirements suitable for different user groups, adding flexibility to our security practices. This approach ensures that groups with higher security

risks, such as administrators, are subject to stricter password requirements compared to regular users.

The lab work proceeded smoothly for the most part, and any issues encountered were collectively resolved, providing valuable learning opportunities. For example, the introduction to using the SCT and FGPP was particularly enlightening. We also explored the management of group policies at the OU level more deeply.

References

- Shruti456rawal. What is System Hardening? Article on the Geeksforgeeks website. March 1, 2024. https://www.geeksforgeeks.org/what-is-system-hardening/?ref=header_outind
- Microsoft Security Compliance Toolkit - How to use. Microsoft Learn article. 2024. <https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/security-compliance-toolkit-10>
- Group Policy Best Practices. Netwrix guide. 2024. https://www.netwrix.com/group_policy_best_practices.html
- Configure fine grained password policies for Active Directory Domain Services. Microsoft Learn article. 2024. <https://learn.microsoft.com/en-us/windows-server/identity/adds/get-started/adac/fine-grained-password-policies?tabs=adac>
- gpresult. Microsoft Learn article. 2023. <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/gpresult>
- gpupdate. Microsoft Learn article. 2023. <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate>
- Pasi Hyytiäinen. TTC6050-Hardening AD, PIM & PAM, JIT & JEA. JAMK teaching PDF. 2024. [Hardening: AD & JIT](#)
- Understanding the Remote Desktop Protocol (RDP). Microsoft Learn article. 2023. <https://learn.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol>
- Group Policy Objects. Microsoft Learn article. 2018. <https://learn.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-objects>

