Network Security Policy Design and Implementation

Module 04

Lab 1

Implementing Policies using the Group Policy Management Console (GPMC)

The Group Policy Management Console (GPMC) is a scriptable Microsoft Management Console (MMC) snap-in, providing a single administrative tool for managing Group Policy across the enterprise. GPMC is the standard tool for managing Group Policy.

ICON KEY

- Valuable Information
- Test Your Knowledge
- Web Exercise
- Workbook Review

Lab Scenario

Administrators use GPMC to perform all Group Policy management tasks with the exception of configuring individual policy settings in Group Policy Objects themselves. This is done with Group Policy Object Editor. The scenarios below describe how an administrator uses GPMC to manage Group Policy.

Lab Objectives

This lab demonstrates how to use Group Policy Management.

Lab Environment

To carry out this lab, you need:

- A virtual machine running Windows Server 2008
- A virtual machine running Windows 10

Lab Duration

Time: 20 Minutes

Overview of the Lab

Group Policy Preferences, introduced in Windows Server 2008, provide more than twenty Group Policy extensions that expand the range of configurable preference settings in a Group Policy object (GPO). Group Policy lets you manage drive

mappings, registry settings, local users and groups, services, files, and folders without the need to learn a scripting language.

Lab Tasks

TASK 1

Launch Group Policy Management

Before starting this lab make sure that the Windows 10 machine is turned on.

1. Launch the Windows Server 2008 machine and log in as a domain administrator
2. Once you have logged in, close the Server Manager window, if it appears.
3. To launch Group Policy Management, navigate to **Start** → **Administrative Tools** and click **Group Policy Management** as shown in the screenshot
4. Alternatively you can also launch by typing **gpmc.msc** in the Start Search field and press Enter to launch.

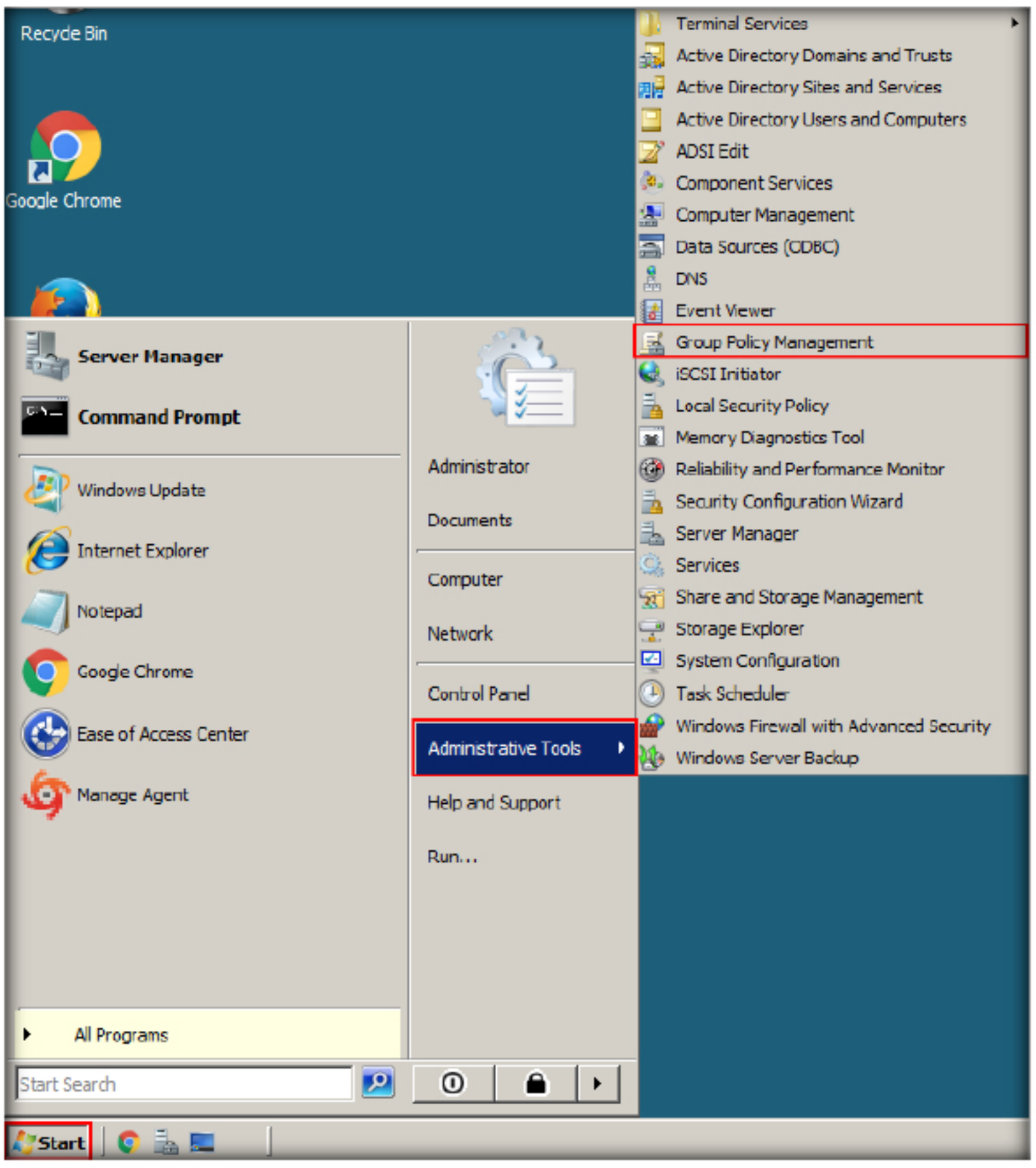

FIGURE 1.1: Launch Group Policy Management

The GPMC uses files that have .adm, .admx, and .adml extensions to display the friendly names of policy settings when generating HTML reports for GPOs, Group Policy Modeling, and Group Policy Results. These options let you control the location from which the GPMC reads only .adm files.

5. The Group Policy Management main window appears as shown in the screenshot. Expand the Forest: CND.com domain tree

If you add or change an .adm or ADMX file in an existing location, you must restart GPMC for the GPMC to display the change in the .adm or .admx file when displaying HTML reports.

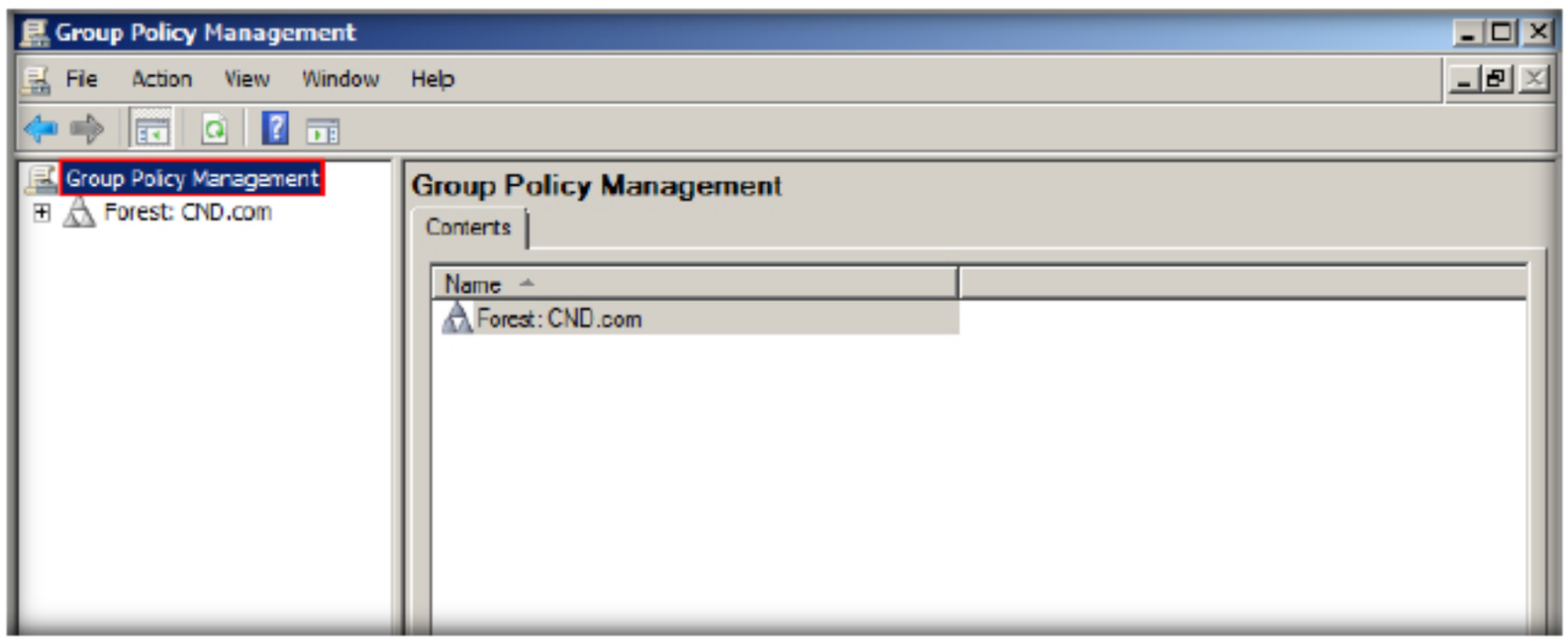

FIGURE 1.2: Group Policy Management Main Window

TASK 2

Configure Group Policy Management

6. Expand the **Domains** tree, **CND.com** tree and select the **Default Domain Policy** profile from the left pane and click **Settings** under the Default Domain Policy in the right pane as shown in the screenshot.

The GPMC lets you configure preferences when you edit any domain-based GPO. The Preferences node appears under Computer Configuration and User Configuration.

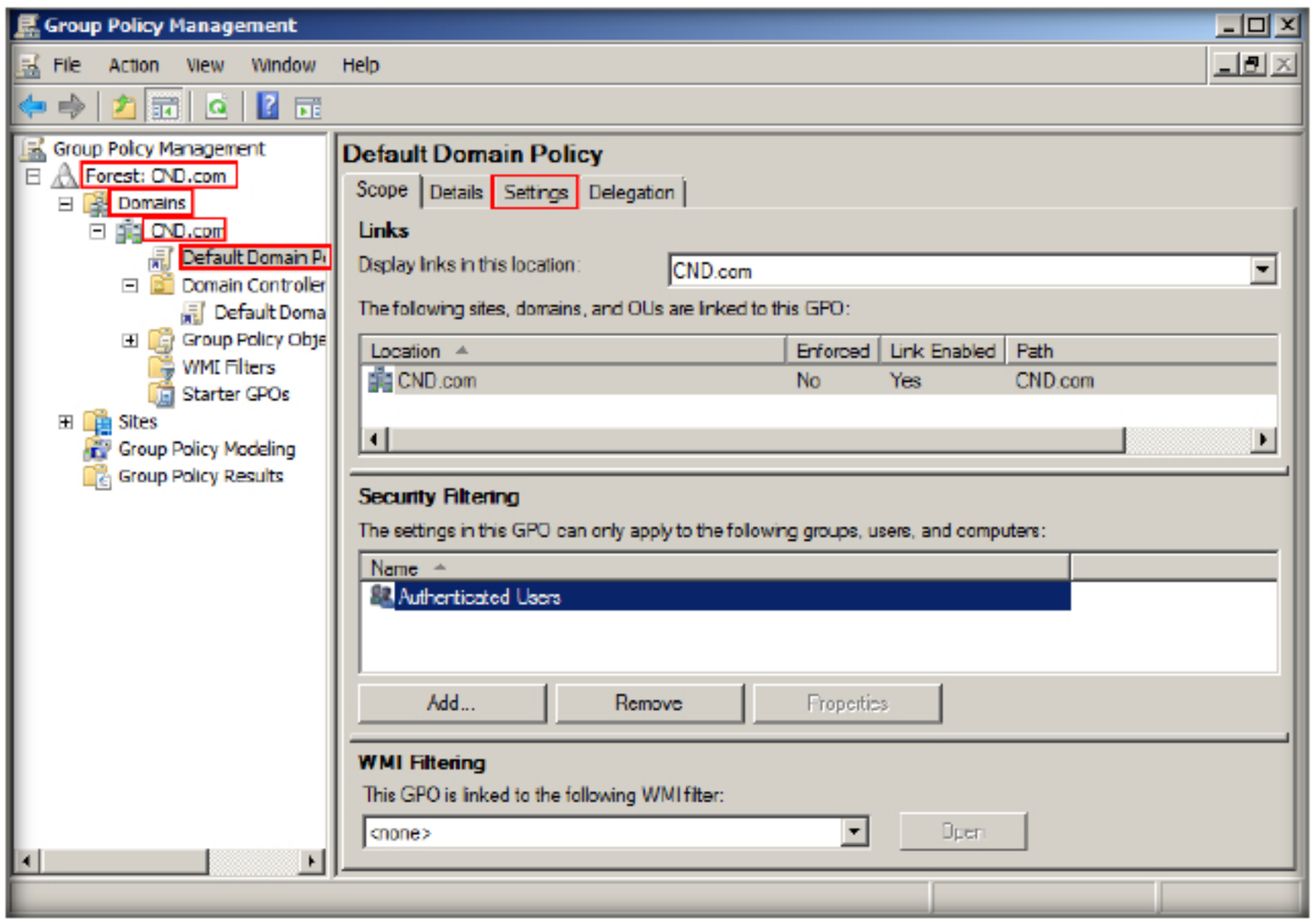

FIGURE 1.3: Default Domain Policy

7. Click to expand the **Policies**, **Windows Settings** and **Security Settings**, right-click on **Account Policies/Password Policy** and click **Edit** from the context menu as shown in the screenshot.

8. With this you can configure the password policies for domain users.

The policy settings under Account Policies are implemented at the domain level. A Windows Server 2003 domain must have a single password policy, account lockout policy, and Kerberos version 5 authentication protocol policy for the domain.

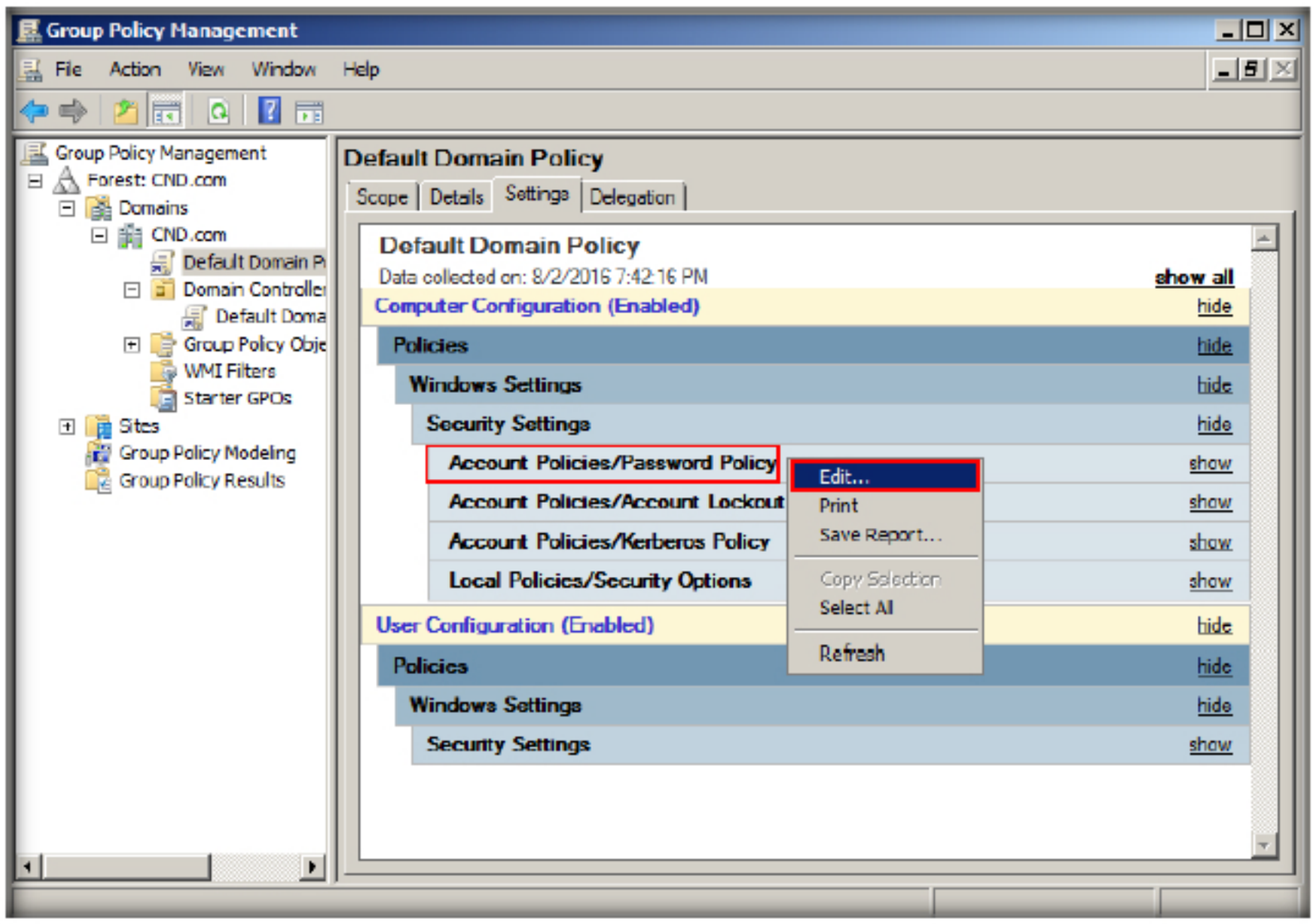

FIGURE 1.4: Editing Account Policies/Password Policy

9. In this lab we are going to set the password policies for the domain users. The Group Policy Management Editor Window appears; expand Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies and click Password Policy in the left pane.

10. As soon as you click on Password Policy in the left pane you will see the Policy and its Policy Settings in the right pane as shown in the screenshot

Configuring these policy settings at any other level in Active Directory will only affect local accounts on member servers. If there are groups that require separate password policies, they should be segmented into another domain or forest, based on any additional requirements.

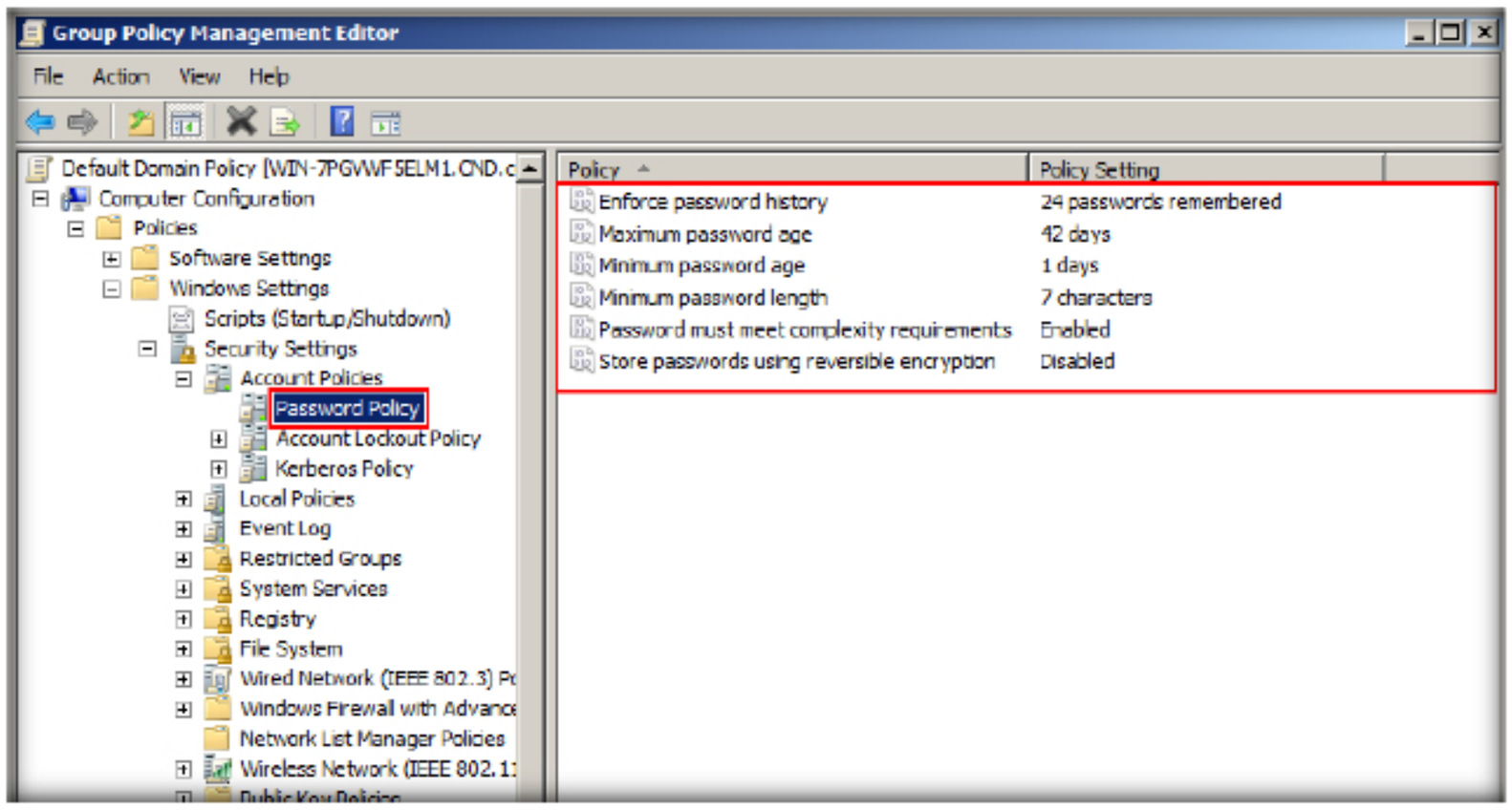

FIGURE 1.5: Group Policy Management Editor

11. Set the Password Policies according to your organization's policy. To edit the policy settings right-click on the policy and click Properties from the context menu.

Password Policy: These policy settings are used for domain or local user accounts. They determine settings for passwords, such as enforcement and lifetimes.

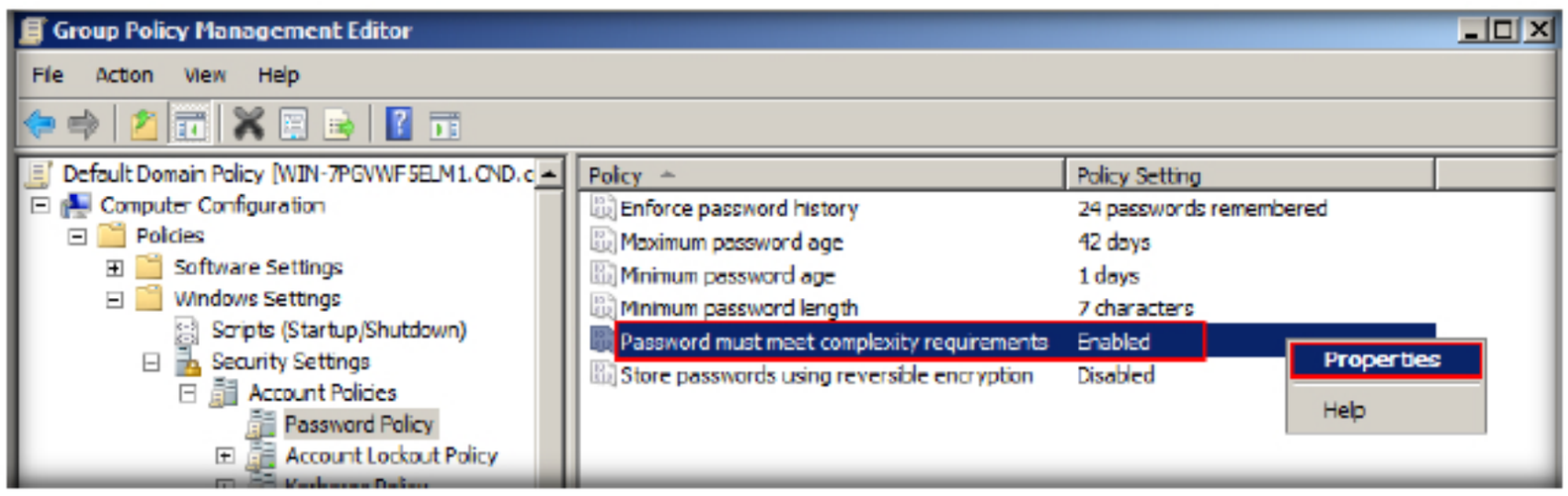

FIGURE 1.6: Password Policies

12. The selected policy properties window appears; you can define the policy settings under the Security Policy Setting tab

Account Lockout Policy: These policy settings are used for domain or local user accounts. They determine the circumstances and length of time that an account will be locked out of the system.

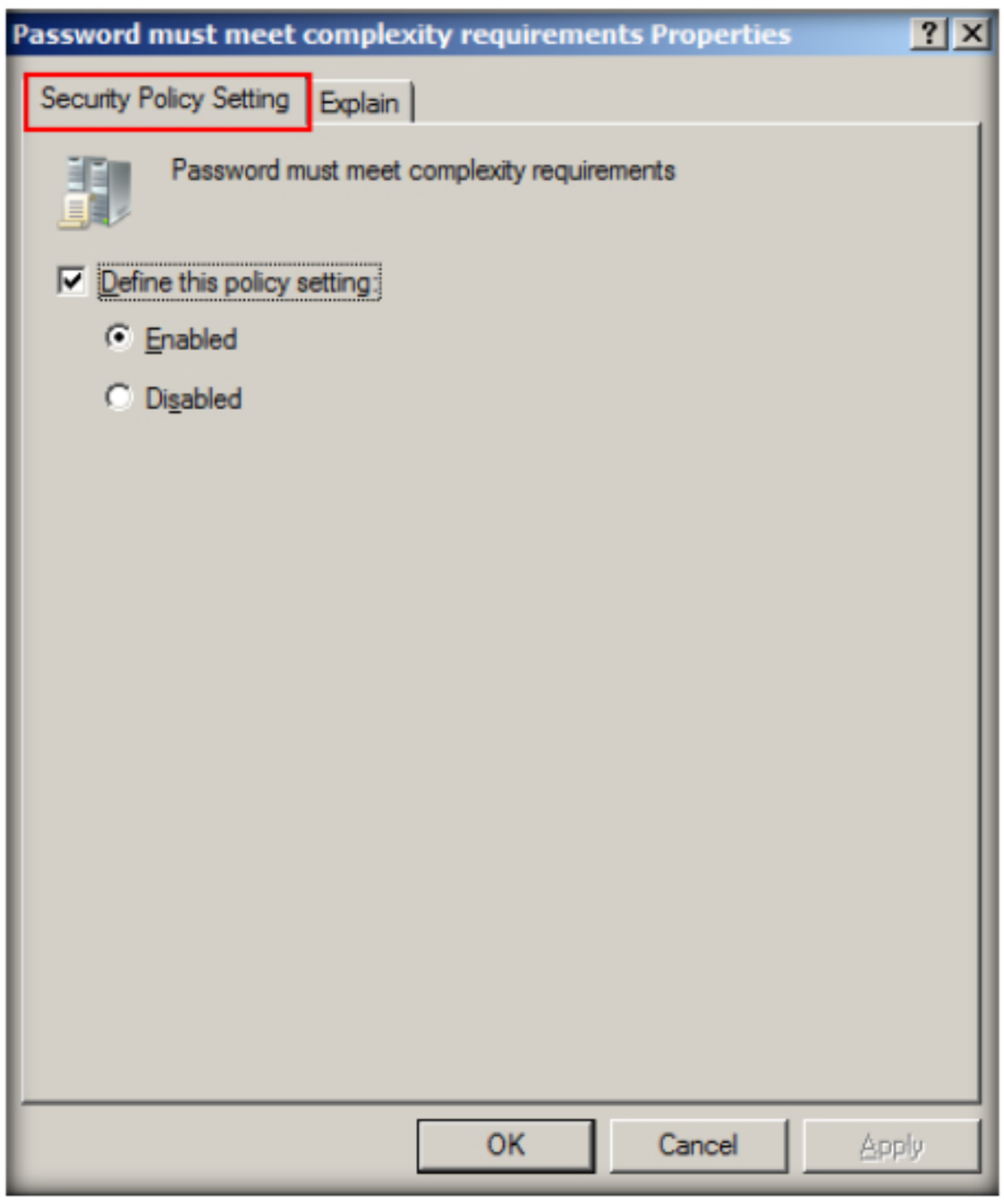

FIGURE 1.7: Properties of Policy

13. In the Explain tab you will have a brief description of the selected policy, read the explanation and edit the policy following your organization's policy.

14. Click the **OK** button to close the policy properties window.

Kerberos Policy: These policy settings are used for domain user accounts. They determine Kerberos-related settings, such as ticket lifetimes and enforcement. Kerberos policy settings do not exist in local computer policy.

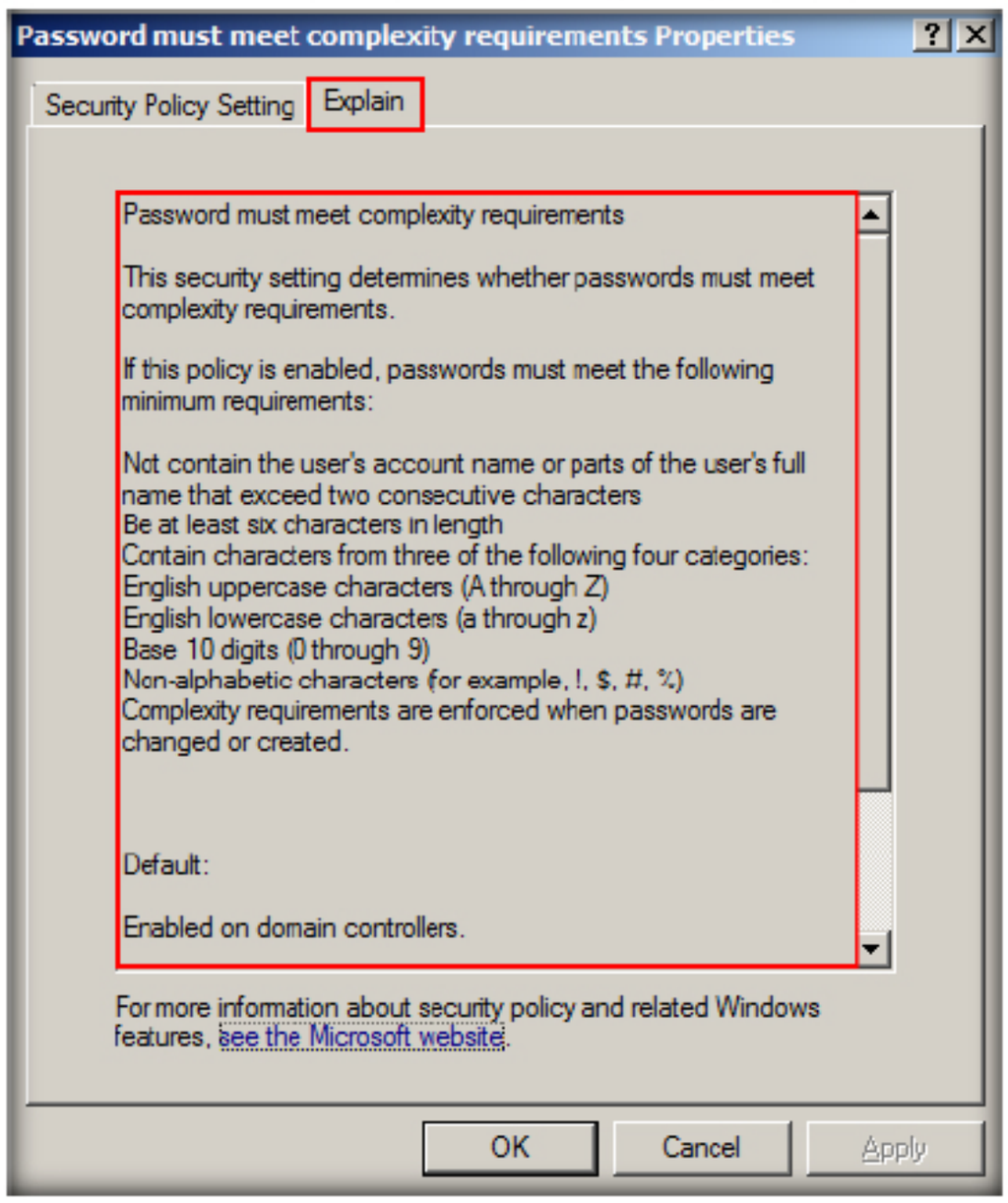

FIGURE 1.8: Policy Explanation

15. Similarly, you can configure the Password Policies according to your organization's policies.

Lab Analysis

Analyze and document the results of the lab exercise. Give your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs