Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024

Lab 4.5.9 Enforcing User Account Control (UAC) on an Active Directory Domain

In this lab, I will be ensuring and enforcing that User Account Control (UAC, a Windows Security Tool) is active and properly set on an Active Directory Domain.

“The scenario for this lab is as follows:

1. **You are the IT administrator for a small corporate network. The company has a single Active Directory domain named CorpNet.local. You need to increase the domain's authentication security. You need to make sure that User Account Control (UAC) settings are consistent throughout the domain and in accordance with industry recommendations.**
2. **In this lab, your task is to configure the following UAC settings in the Default Domain Policy on CorpDC as follows:**

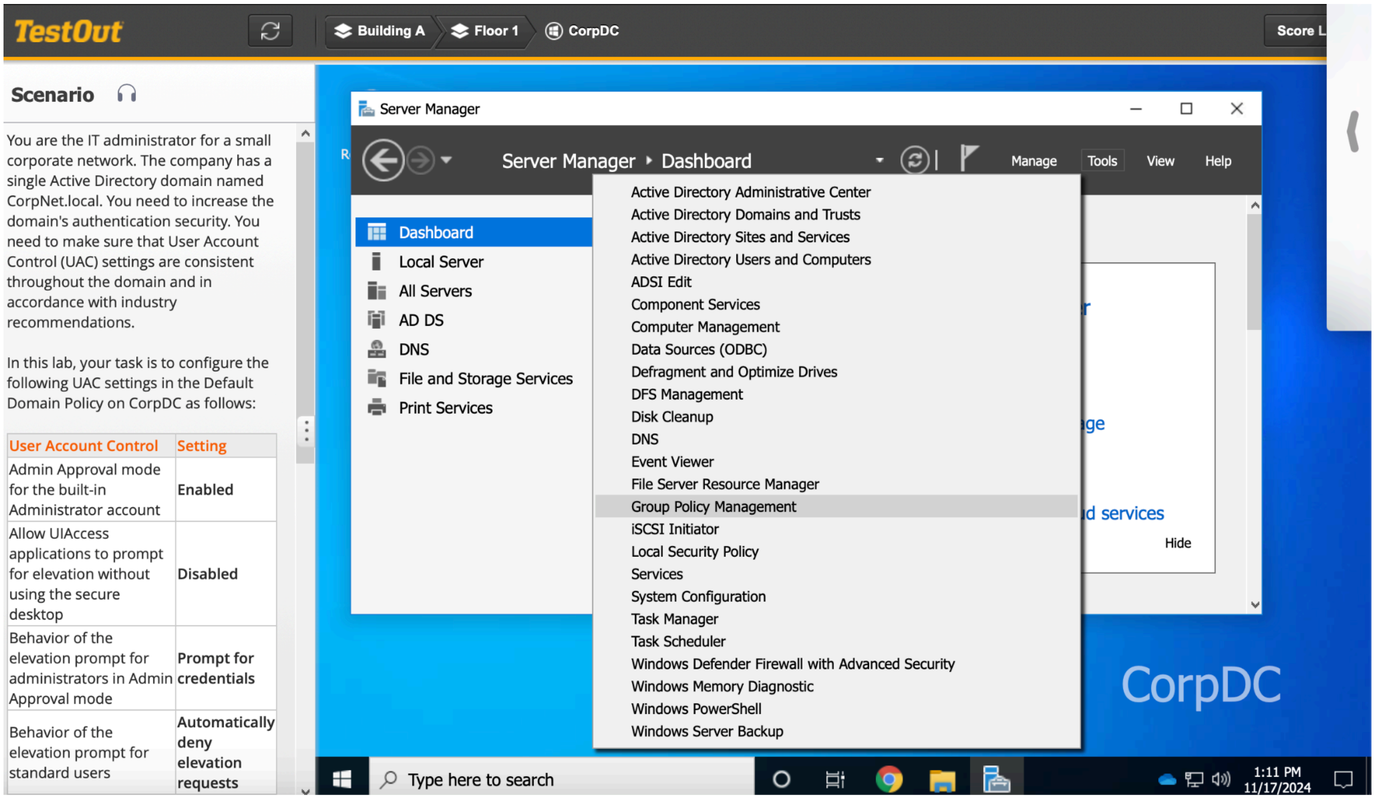
User Account Control	**Setting**
Admin Approval mode for the built-in Administrator account	**Enabled**
Allow UIAccess applications to prompt for elevation without using the secure desktop	**Disabled**
Behavior of the elevation prompt for administrators in Admin Approval mode	**Prompt for credentials**
Behavior of the elevation prompt for standard users	**Automatically deny elevation requests**

Detect application installations and prompt for elevation	**Enabled**
Only elevate UIAccess applications that are installed in secure locations	**Enabled**
Only elevate executables that are signed and validated	**Disabled**
Run all administrators in Admin Approval mode	**Enabled**
Switch to the secure desktop when prompting for elevation	**Enabled**
Virtualize file and registry write failures to per-user locations	**Enabled**

To change UAC settings we would need to configure it on every Computer in the domain manually. This would be a pain, but thanks to Microsoft Active Directory, we can make this change once on our Domain Controller and have it apply to all computers in the domain. Our domain in this lab happens to be CorpNet.local with our Domain Controller named “CorpDC.”

The tool we will use on the Server Manager app on our Domain Controller will be “Group Policy Management.”

Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024



Scenario

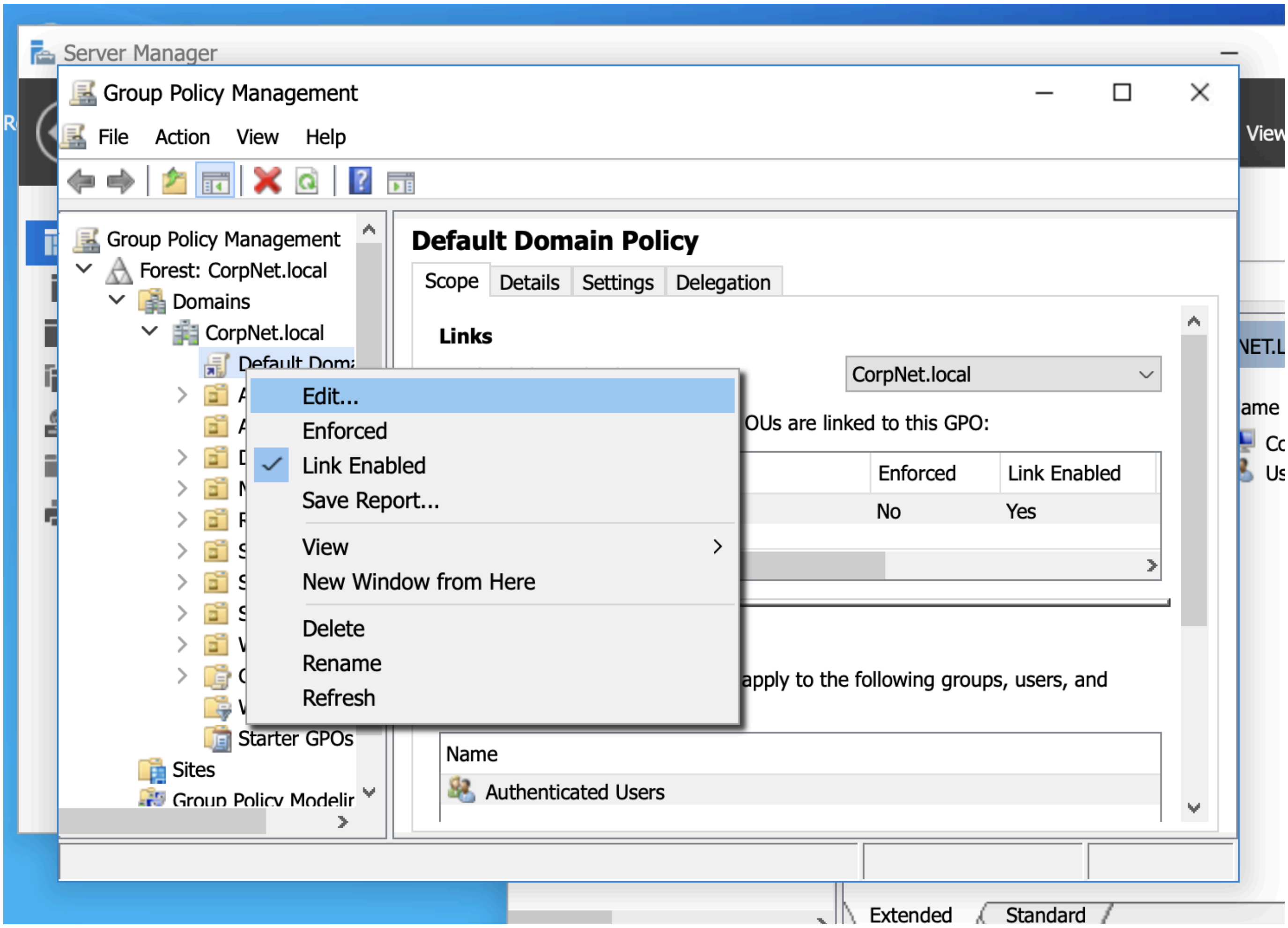
You are the IT administrator for a small corporate network. The company has a single Active Directory domain named CorpNet.local. You need to increase the domain's authentication security. You need to make sure that User Account Control (UAC) settings are consistent throughout the domain and in accordance with industry recommendations.

In this lab, your task is to configure the following UAC settings in the Default Domain Policy on CorpDC as follows:

User Account Control	Setting
Admin Approval mode for the built-in Administrator account	**Enabled**
Allow UIAccess applications to prompt for elevation without using the secure desktop	**Disabled**
Behavior of the elevation prompt for administrators in Admin Approval mode	**Prompt for credentials**
Behavior of the elevation prompt for standard users	**Automatically deny elevation requests**

Once you click it an window will pop up. Expand the tree view on the left to navigate to Forest: CorpNet.local > Domains > CorpNet.local > Default Domain Policy.

Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024



Default Domain Policy

Links

OUs are linked to this GPO:

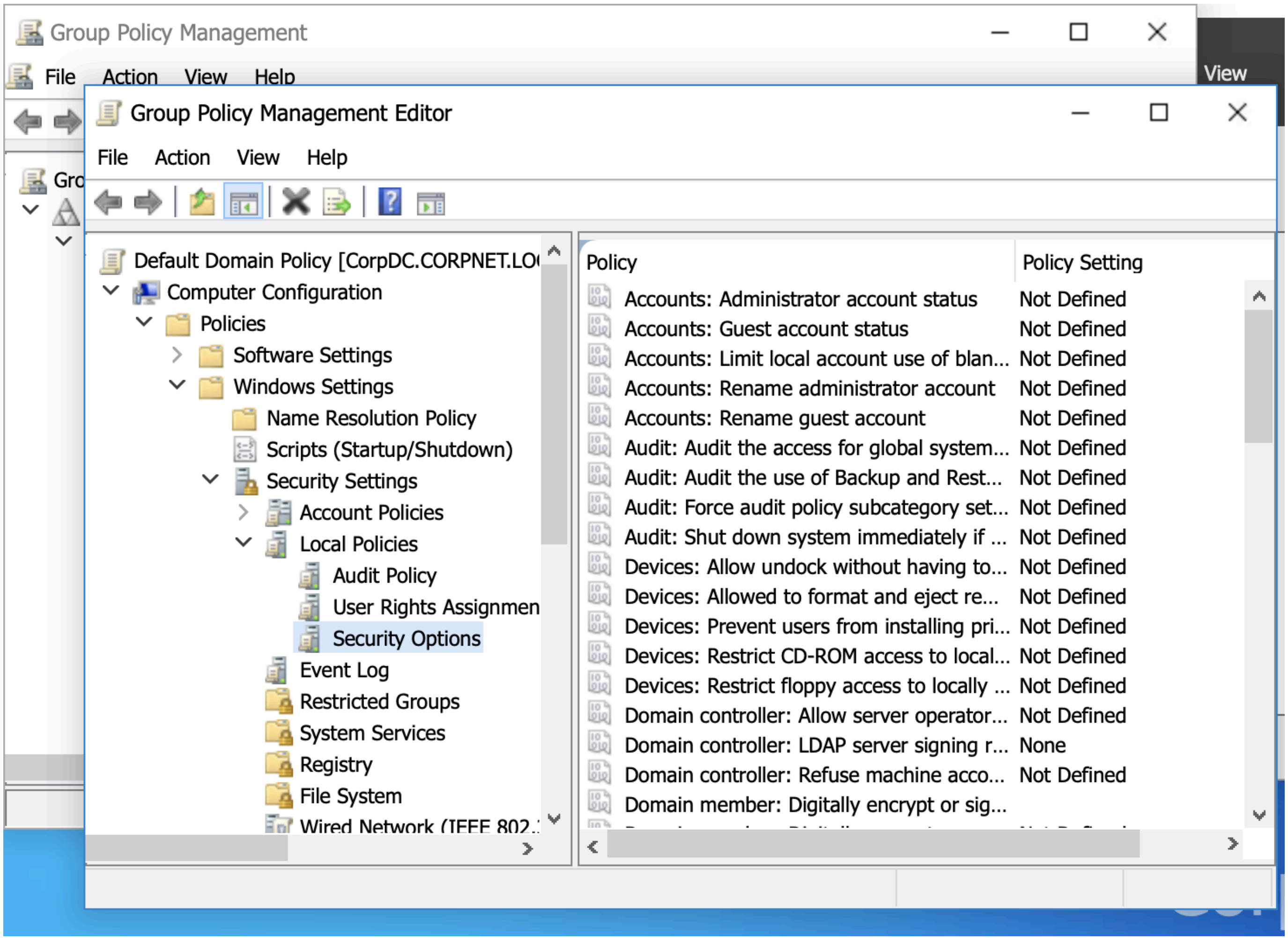
	Enforced	Link Enabled
	No	Yes

apply to the following groups, users, and

Name
Authenticated Users

Clicking “Edit” bring up the Group Policy Management Editor. From here , we will navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options.

Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024



- Default Domain Policy [CorpDC.CORPNET.LO
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
          - Account Policies
          - Local Policies
            - Audit Policy
            - User Rights Assignmen
            - Security Options
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.

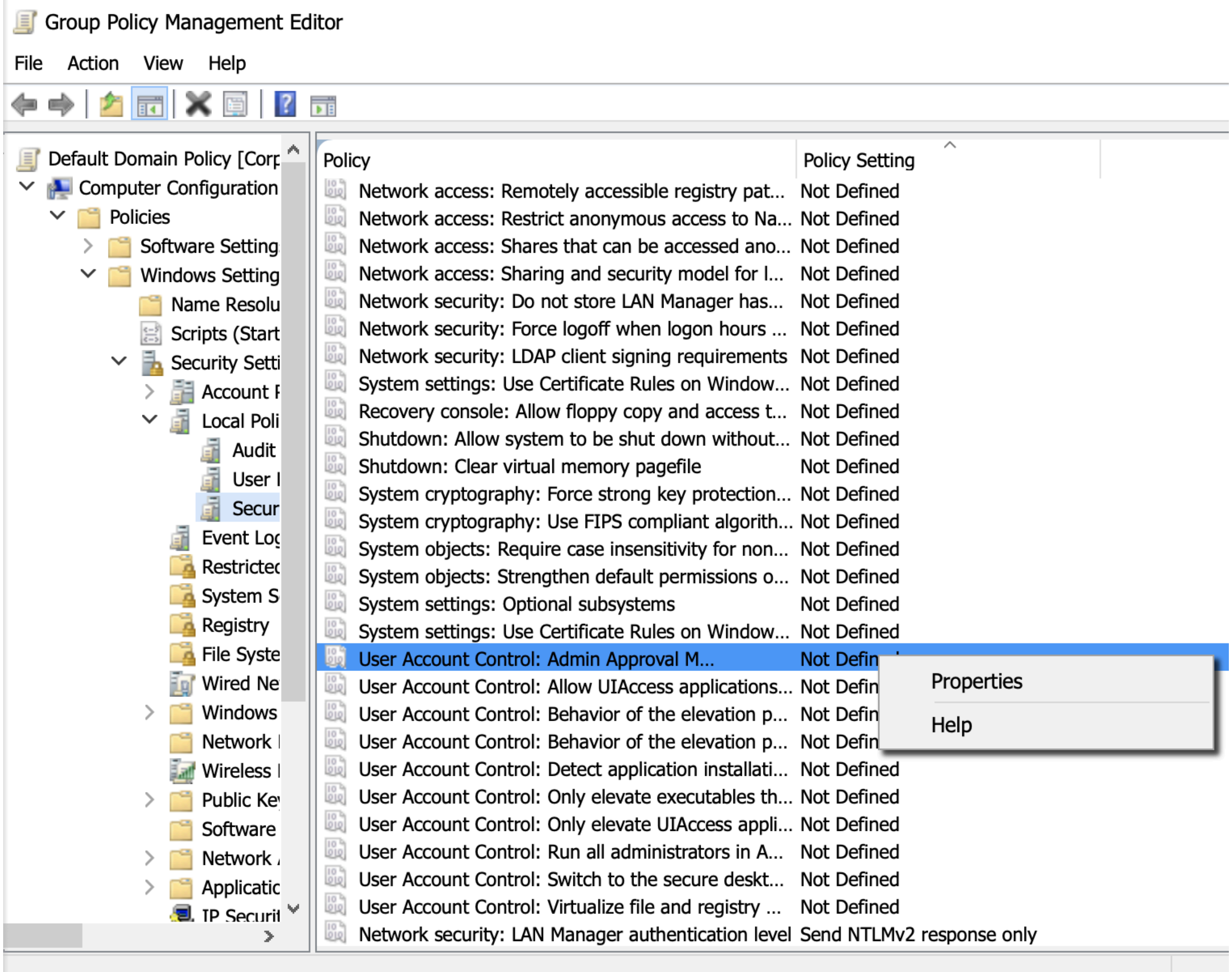
Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blan...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access for global system...	Not Defined
Audit: Audit the use of Backup and Rest...	Not Defined
Audit: Force audit policy subcategory set...	Not Defined
Audit: Shut down system immediately if ...	Not Defined
Devices: Allow undock without having to...	Not Defined
Devices: Allowed to format and eject re...	Not Defined
Devices: Prevent users from installing pri...	Not Defined
Devices: Restrict CD-ROM access to local...	Not Defined
Devices: Restrict floppy access to locally ...	Not Defined
Domain controller: Allow server operator...	Not Defined
Domain controller: LDAP server signing r...	None
Domain controller: Refuse machine acco...	Not Defined
Domain member: Digitally encrypt or sig...	

Here, we can access the configuration for UAC. Now that we have it pulled up we can begin to configure everything asked from us in the table above (scenario). I'll repaste it again below here for review

User Account Control	**Setting**
Admin Approval mode for the built-in Administrator account	**Enabled**
Allow UIAccess applications to prompt for elevation without using the secure desktop	**Disabled**

Behavior of the elevation prompt for administrators in Admin Approval mode	**Prompt for credentials**
Behavior of the elevation prompt for standard users	**Automatically deny elevation requests**
Detect application installations and prompt for elevation	**Enabled**
Only elevate UIAccess applications that are installed in secure locations	**Enabled**
Only elevate executables that are signed and validated	**Disabled**
Run all administrators in Admin Approval mode	**Enabled**
Switch to the secure desktop when prompting for elevation	**Enabled**
Virtualize file and registry write failures to per-user locations	**Enabled**

Scroll down the table above and apply the corresponding settings in the Group Policy Management Editor we have pulled up in the screenshot above.

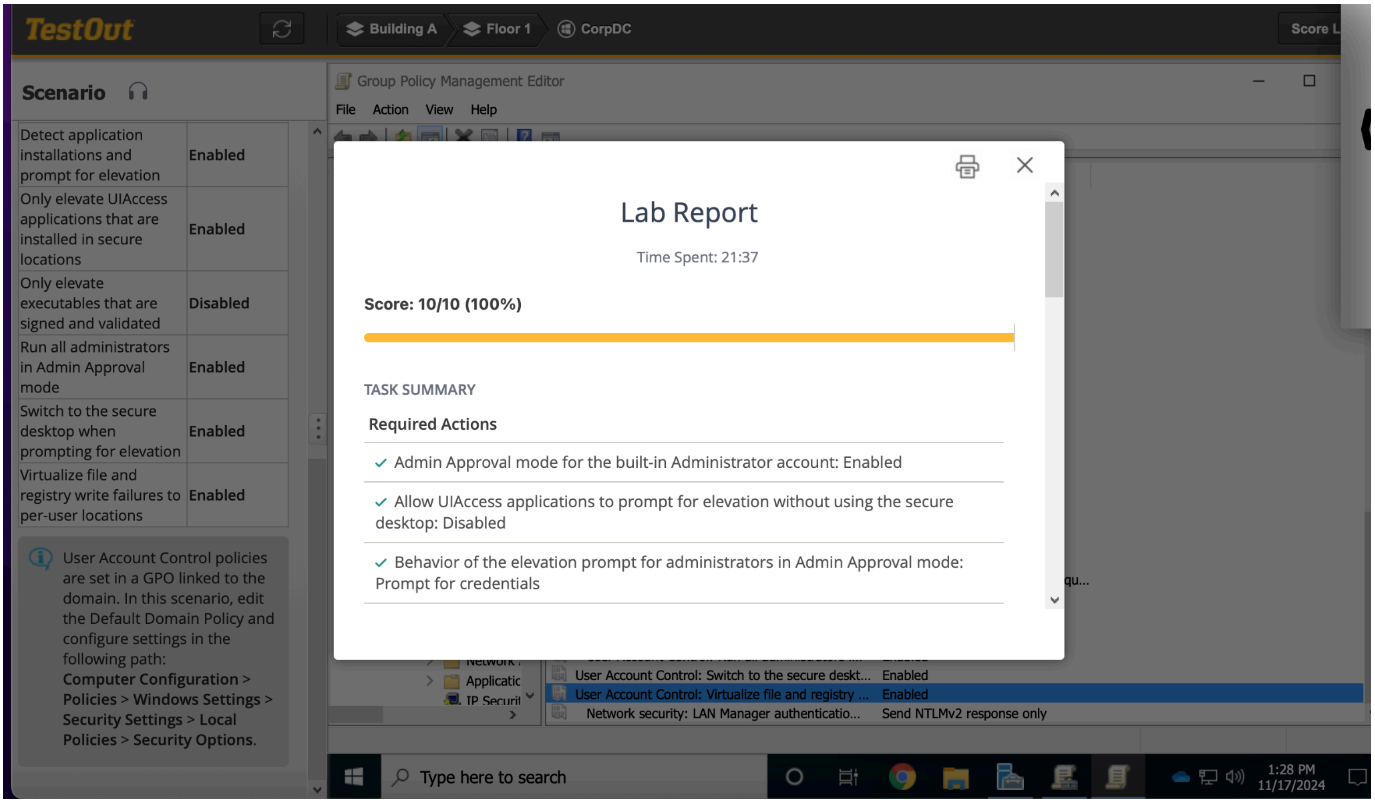


Policy	Policy Setting
Network access: Remotely accessible registry pat...	Not Defined
Network access: Restrict anonymous access to Na...	Not Defined
Network access: Shares that can be accessed ano...	Not Defined
Network access: Sharing and security model for l...	Not Defined
Network security: Do not store LAN Manager has...	Not Defined
Network security: Force logoff when logon hours ...	Not Defined
Network security: LDAP client signing requirements	Not Defined
System settings: Use Certificate Rules on Window...	Not Defined
Recovery console: Allow floppy copy and access t...	Not Defined
Shutdown: Allow system to be shut down without...	Not Defined
Shutdown: Clear virtual memory pagefile	Not Defined
System cryptography: Force strong key protection...	Not Defined
System cryptography: Use FIPS compliant algorith...	Not Defined
System objects: Require case insensitivity for non...	Not Defined
System objects: Strengthen default permissions o...	Not Defined
System settings: Optional subsystems	Not Defined
System settings: Use Certificate Rules on Window...	Not Defined
User Account Control: Admin Approval M...	Not Defin
User Account Control: Allow UIAccess applications...	Not Defin
User Account Control: Behavior of the elevation p...	Not Defin
User Account Control: Behavior of the elevation p...	Not Defin
User Account Control: Detect application installati...	Not Defined
User Account Control: Only elevate executables th...	Not Defined
User Account Control: Only elevate UIAccess appli...	Not Defined
User Account Control: Run all administrators in A...	Not Defined
User Account Control: Switch to the secure deskt...	Not Defined
User Account Control: Virtualize file and registry ...	Not Defined
Network security: LAN Manager authentication level	Send NTLMv2 response only

Notice after you are done applying everything that there are no final Apply or OK buttons anywhere. The polices get pushed down individually as soon as you click the Apply button in the window where you are configuring the policy. Now that we have applied all our desired settings, these changes will be pushed to out Domain Controller and then to all computers connected to the domain.

This concludes this lab.

Robert Carpenter
github.com/robertmcarpenter
Sun November 17th 2024



Scenario

Detect application installations and prompt for elevation	Enabled
Only elevate UIAccess applications that are installed in secure locations	Enabled
Only elevate executables that are signed and validated	Disabled
Run all administrators in Admin Approval mode	Enabled
Switch to the secure desktop when prompting for elevation	Enabled
Virtualize file and registry write failures to per-user locations	Enabled

User Account Control policies are set in a GPO linked to the domain. In this scenario, edit the Default Domain Policy and configure settings in the following path: **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.

Lab Report

Time Spent: 21:37

Score: 10/10 (100%)

TASK SUMMARY

Required Actions

- ✓ Admin Approval mode for the built-in Administrator account: Enabled
- ✓ Allow UIAccess applications to prompt for elevation without using the secure desktop: Disabled
- ✓ Behavior of the elevation prompt for administrators in Admin Approval mode: Prompt for credentials

User Account Control: Switch to the secure deskt...	Enabled
User Account Control: Virtualize file and registry ...	Enabled
Network security: LAN Manager authenticatio...	Send NTLMv2 response only