Lab Number: 6 Group Policy

Student name: Raine

Section Summary

Section 6: Group policy and security

Goals

- Configure and test Group Policy objects (GPOs) for Software settings, Windows settings and Administrative templates
- Link GPOs to AD objects
- Enforce GPO inheritance
- Configure Windows server update services (WSUS) on WS1
- Configure and test Windows defender firewall rules

Implementation steps

1. Where do you find and edit GPOs? What are the default GPOs present before any custom configurations?

2. Enforce the Default Domain policy inheritance. What does this do?

3. Configure Group Policy objects and link to the appropriate AD objects (OU/group) on WS2:
    - Note you may need to delete the Filescreens created in a previous section to be able to do the following. The VM will also require a restart.

    - Administrative templates
        - Create a shared folder called wallpaper and save two .jpg files. All groups read access
        - Create **group-specific** desktop wallpaper for each group
        - Disable access to the Control panel and command prompt for Accounts users only
    - Windows settings
        - Set maximum password age and length for all users
        - Set account lockout threshold and reset lock counter values
    - Software settings :
        - User configurations: set one application to be assigned for the developers group only
            - Create a shared folder and assign all groups to have read access to it
            - Save and application .exe in the shared folder called ‘applications’ in section 4

- Convert .exe to .msi using a free third-party tool and save it to the applications folder
- What is the difference between assigned and published applications?

4. Apply GPOs using the Command prompt

5. Login as different users to test the GPOs above

6. Configure Windows server update services (WSUS) on WS1
   - Add WSUS role to WS1
   - Ensure WS1 has a second virtual network adapter that is bridged to a physical adapter connected to the internet e.g. your wireless adapter on your laptop
   - Configure such that updates are
     - Save to E: drive (second virtual hard-drive you created in project 4)
     - Synchronised with Microsoft
     - no proxy

7. Create a new Windows Defender Firewall inbound rules to only allow traffic required by the previous sections of this project and block any other traffic

   - What ports did you allow and why?

8. Test that expected traffic is allowed into the server and unwanted traffic is blocked

1

Group Policy Objects (GPOs) can be found and edited using several tools in Windows Server. The most common tools are the **Group Policy Management Console (GPMC)** and the **Local Group Policy Editor**.

Using Group Policy Management Console (GPMC)

1. **Open Group Policy Management Console**:
   - Click on the **Start** menu.
   - Type gpmc.msc and press Enter.
   - Alternatively, you can open **Server Manager**, click on **Tools**, and then select **Group Policy Management**.
2. **Navigating GPOs in GPMC**:
   - In the **Group Policy Management** console, you will see a tree structure on the left pane.
   - Expand **Forest: <Your Forest Name>** > **Domains** > **<Your Domain Name>**.

   - Under your domain, you will see **Group Policy Objects**, which lists all the GPOs.
3. **Editing a GPO**:
   - To edit an existing GPO, right-click on the GPO you want to edit and select **Edit**.
   - This will open the **Group Policy Management Editor**, where you can make changes to the policy settings.

Using Local Group Policy Editor

1. **Open Local Group Policy Editor**:
   - Click on the **Start** menu.
   - Type gpedit.msc and press Enter.
2. **Navigating Local Policies**:
   - In the **Local Group Policy Editor**, you will see two main categories: **Computer Configuration** and **User Configuration**.
   - Under each category, you will find several subcategories where you can edit policy settings.

Default GPOs Present Before Any Custom Configurations

When you first set up a Windows Server environment, there are two default GPOs that are created automatically:

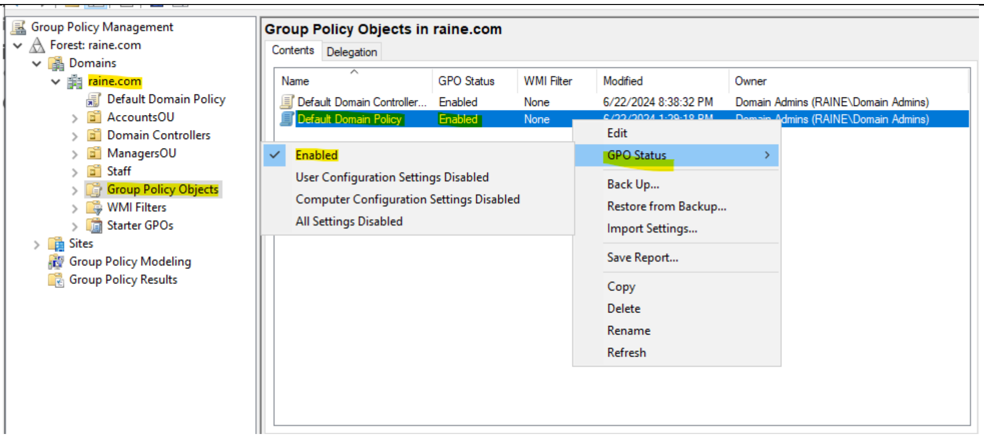
1. **Default Domain Policy**:
   - This GPO is linked to the domain and contains default settings for the entire domain.
   - It is applied to all users and computers within the domain.
   - Common settings include password policies, account lockout policies, and Kerberos policies.
   - **Location in GPMC**: Group Policy Management > Forest: <Your Forest Name> > Domains > <Your Domain Name> > Group Policy Objects > Default Domain Policy.
2. **Default Domain Controllers Policy**:
   - This GPO is linked to the Domain Controllers OU and contains default settings for all domain controllers.
   - It is applied to all domain controllers in the domain.
   - Common settings include user rights assignments and security options specific to domain controllers.
   - **Location in GPMC**: Group Policy Management > Forest: <Your Forest Name> > Domains > <Your Domain Name> > Domain Controllers > Group Policy Objects > Default Domain Controllers Policy.

Example Steps to Edit a GPO

1. **Edit the Default Domain Policy**:
   - Open **GPMC**.
   - Navigate to Forest: <Your Forest Name> > Domains > <Your Domain Name> > Group Policy Objects.
   - Right-click on **Default Domain Policy** and select **Edit**.
   - In the **Group Policy Management Editor**, navigate to the settings you want to configure (e.g., Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy).
   - Make the necessary changes and close the editor.

2. **Edit the Default Domain Controllers Policy**:
    - Open **GPMC**.
    - Navigate to Forest: <Your Forest Name> > Domains > <Your Domain Name> > Domain Controllers.
    - Right-click on **Default Domain Controllers Policy** and select **Edit**.
    - In the **Group Policy Management Editor**, navigate to the settings you want to configure (e.g., Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment).
    - Make the necessary changes and close the editor.

2



Group Policy Management
Forest: raine.com
Domains
raine.com
Default Domain Policy
AccountsOU
Domain Controllers
ManagersOU
Staff
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results

Group Policy Objects in raine.com

Contents | Delegation

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controller...	Enabled	None	6/22/2024 8:38:32 PM	Domain Admins (RAINE\Domain Admins)
Default Domain Policy	Enabled	None	6/22/2024 1:29:18 PM	Domain Admins (RAINE\Domain Admins)

Default Domain Policy enabled, which means it is now being enforced.

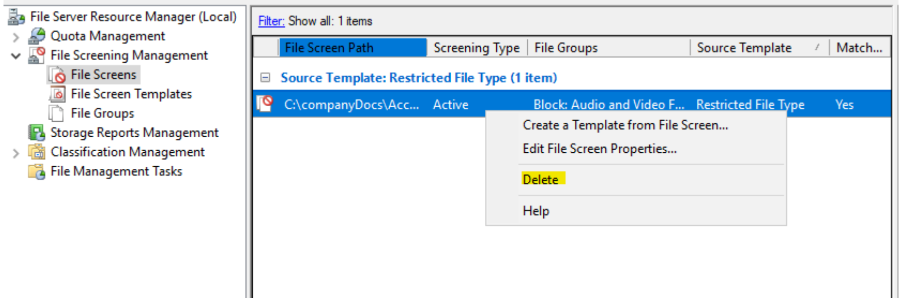
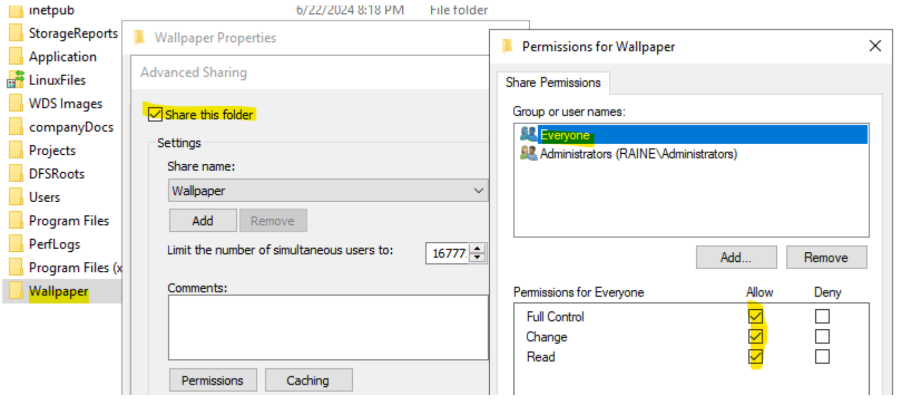
What Enforcing a GPO Does

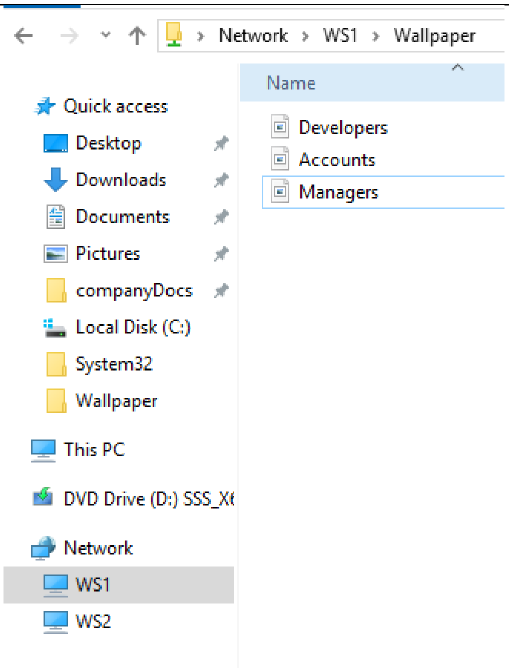
When you enforce a GPO, it means that:

1. **Precedence**:
    - The enforced GPO takes precedence over other GPOs. Even if other GPOs with conflicting settings are linked to OUs or objects lower in the Active Directory hierarchy, the settings in the enforced GPO will override those conflicts.
2. **Inheritance**:
    - The enforced GPO's settings are inherited by all child OUs and objects within the domain. This inheritance cannot be blocked by lower-level OUs or objects, ensuring consistent application of the policy across the entire domain.
3. **Policy Conflicts**:
    - If there are conflicting settings between the enforced GPO and other GPOs, the settings in the enforced GPO will be applied. This ensures that critical settings defined in the enforced GPO are always applied, regardless of other policies.

Example Scenario

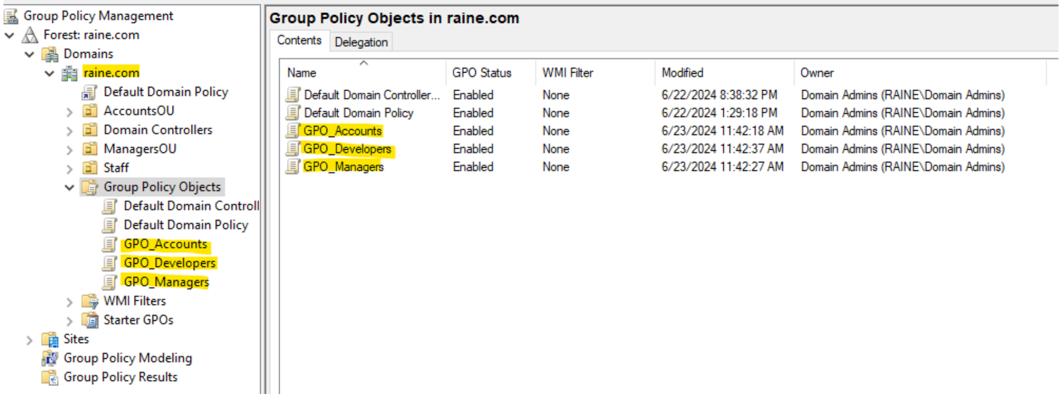
- **Without Enforcement**:
    - The Default Domain Policy is applied at the domain level, and it includes settings such as password policies and account lockout policies.
    - An OU named **Sales** has a separate GPO linked to it with different password policies.

	○ If the Sales GPO is higher in the link order, its settings may override those in the Default Domain Policy. • **With Enforcement**: ○ Enforcing the Default Domain Policy ensures that the password policies and account lockout policies defined in it are applied to the **Sales** OU, even if the Sales GPO has different settings. ○ This means that the critical security settings defined in the Default Domain Policy are consistently applied across all users and computers in the domain, regardless of other GPOs.
3	 File Server Resource Manager (Local) Quota Management File Screening Management File Screens File Screen Templates File Groups Storage Reports Management Classification Management File Management Tasks Filter: Show all: 1 items File Screen Path | Screening Type | File Groups | Source Template | Match... Source Template: Restricted File Type (1 item) C:\companyDocs\Acc... | Active | Block: Audio and Video F... | Restricted File Type | Yes Create a Template from File Screen... Edit File Screen Properties... Delete Help File Screen configured in LAB 4 deleted.  inetpub 6/22/2024 8:18 PM File folder StorageReports Application LinuxFiles WDS Images companyDocs Projects DFSRoots Users Program Files PerfLogs Program Files (x Wallpaper Wallpaper Properties Advanced Sharing ☑ Share this folder Settings Share name: Wallpaper Add Remove Limit the number of simultaneous users to: 16777 Comments: Permissions Caching Permissions for Wallpaper Share Permissions Group or user names: Everyone Administrators (RAINE\Administrators) Add... Remove Permissions for Everyone | Allow | Deny Full Control ☑ □ Change ☑ □ Read ☑ □ Create shared folder called wallpaper, three jpgs saved to folder.



Developers
Accounts
Managers

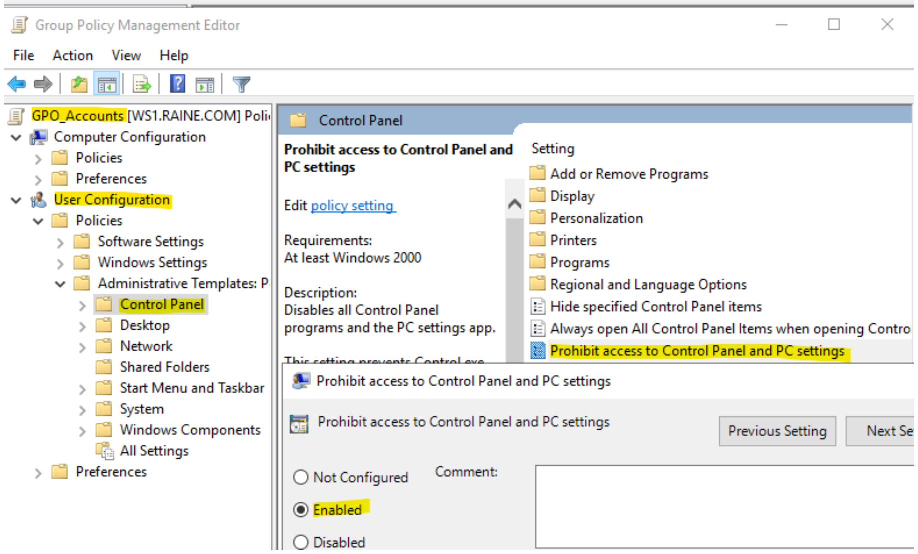
Three wallpapers saved to the shared folder labeled for each group to be assigned in GPO



Group Policy Objects in raine.com

Name	GPO Status	WMI Filter	Modified	Owner
Default Domain Controller...	Enabled	None	6/22/2024 8:38:32 PM	Domain Admins (RAINE\Domain Admins)
Default Domain Policy	Enabled	None	6/22/2024 1:29:18 PM	Domain Admins (RAINE\Domain Admins)
GPO_Accounts	Enabled	None	6/23/2024 11:42:18 AM	Domain Admins (RAINE\Domain Admins)
GPO_Developers	Enabled	None	6/23/2024 11:42:37 AM	Domain Admins (RAINE\Domain Admins)
GPO_Managers	Enabled	None	6/23/2024 11:42:27 AM	Domain Admins (RAINE\Domain Admins)

Configure account specific GPO’s with each GPO assigned a separate wallpaper from the Wallpapers shared folder.



Prohibit access to Control Panel and PC settings

Edit policy setting

Requirements:
At least Windows 2000

Description:
Disables all Control Panel programs and the PC settings app.

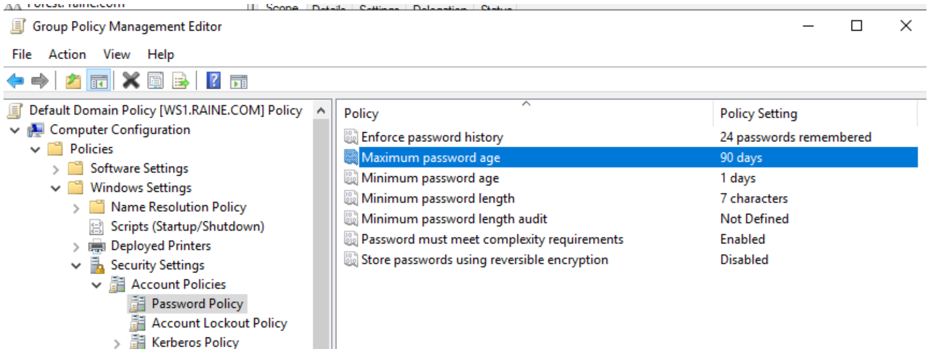
Setting
Add or Remove Programs
Display
Personalization
Printers
Programs
Regional and Language Options
Hide specified Control Panel items
Always open All Control Panel Items when opening Contro
Prohibit access to Control Panel and PC settings

Prohibit access to Control Panel and PC settings

Prohibit access to Control Panel and PC settings

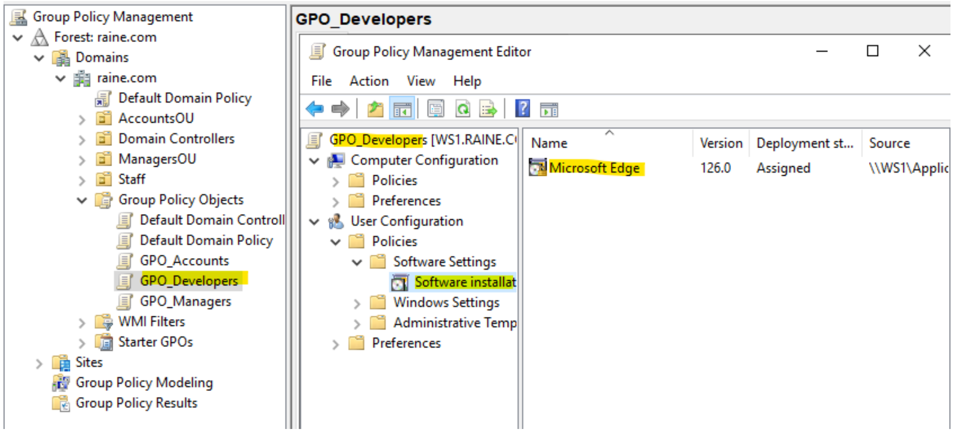
○ Not Configured   Comment:
● Enabled
○ Disabled

Configure the GPO_Accounts policy to prohibit access to Control Panel



Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	7 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

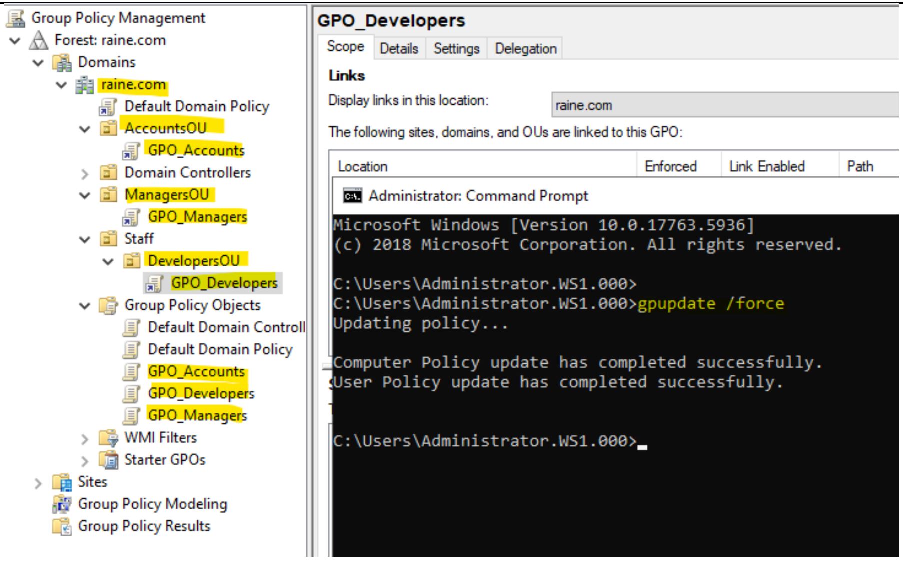
Configure the maximum password age, length and account lockout threshold and reset lock counter values for all users using default domain policy.



Name	Version	Deployment st...	Source
Microsoft Edge	126.0	Assigned	\\WS1\Applic

Configure GPO_Developers to automatically install Microsoft Edge MSi located in the Applications shared folder created in LAB 4

4



GPO_Developers

Links

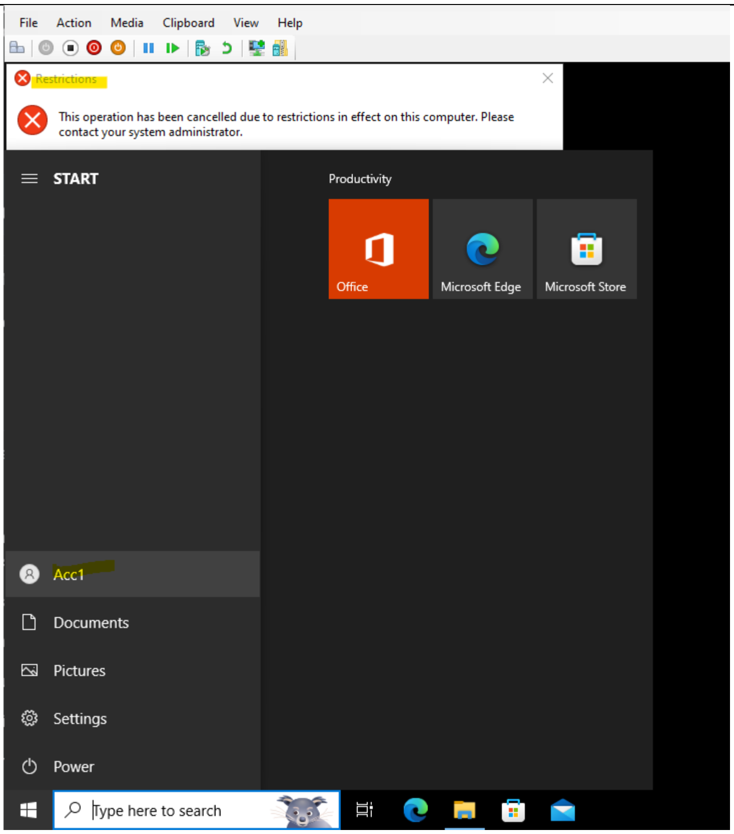
Display links in this location: raine.com

The following sites, domains, and OUs are linked to this GPO:

```
Microsoft Windows [Version 10.0.17763.5936]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.WS1.000>
C:\Users\Administrator.WS1.000>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Users\Administrator.WS1.000>_
```

Apply GPO's to the OU and apply them with a cmd using gpupdate /force /force updates both user policy and computer policy

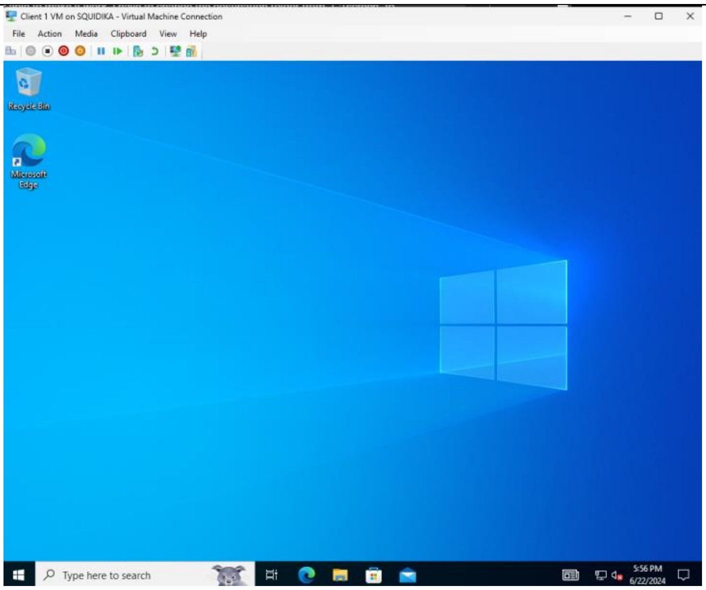
5

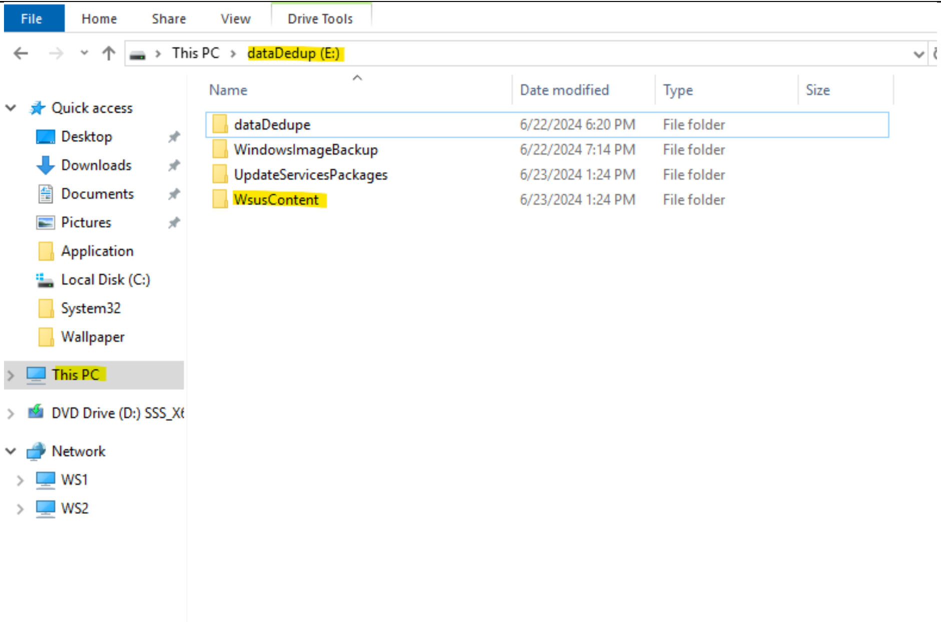


Restrictions

This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

Acc1 being denied access to the Control Panel and Computer settings, you can see the background is not configured because the Client VM is unlicensed.

<table>
<tr><td></td><td>


This is what the Admin account looks like, who ahs not been automatically configured with a wallpaper through GPO. The GPO's set for Accounts, Dev and Man attempt to get the backgrounds but are blocked by the license.
</td></tr>
<tr><td>6</td><td>


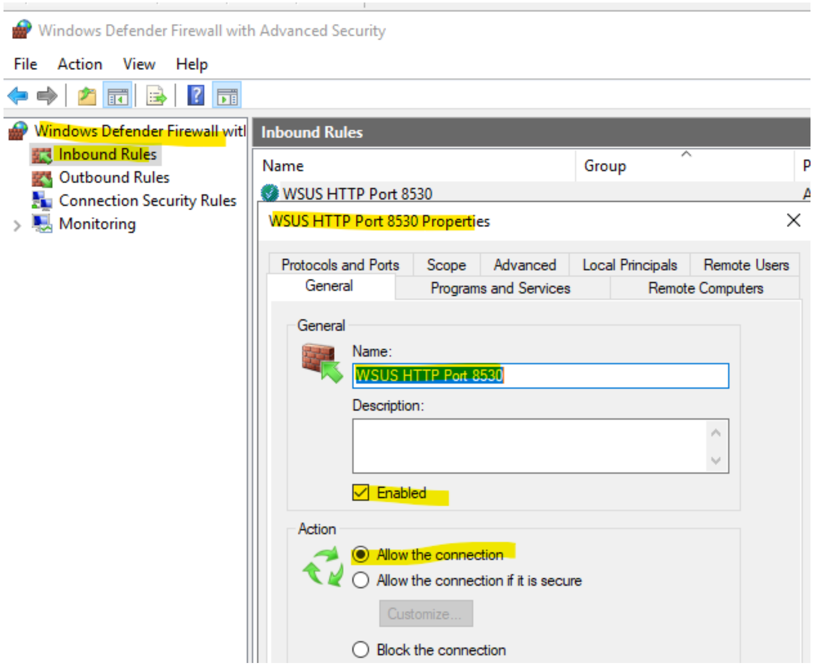
Name	Date modified	Type	Size
dataDedupe	6/22/2024 6:20 PM	File folder	
WindowsImageBackup	6/22/2024 7:14 PM	File folder	
UpdateServicesPackages	6/23/2024 1:24 PM	File folder	
WsusContent	6/23/2024 1:24 PM	File folder	

WSUS configured and saving updated to the E:/ drive we configured in LAB 4
</td></tr>
<tr><td>7</td><td>

Required Ports and Their Purposes

1. **WSUS (Windows Server Update Services)**:
   - **Port 8530**: Used for HTTP traffic between WSUS server and clients.
   - **Port 8531**: Used for HTTPS traffic between WSUS server and clients (if configured to use SSL).
2. **Remote Desktop Services**:
   - **Port 3389**: Used for Remote Desktop Protocol (RDP) to allow remote management and access to the server.
</td></tr>
</table>

3. **File Sharing (SMB)**:
    - **Port 445**: Used for SMB over TCP/IP, essential for shared folders like wallpaper, applications, and shareFoldersWindowsBackup.
4. **HTTP/HTTPS for Web Access**:
    - **Port 80**: Used for HTTP traffic.
    - **Port 443**: Used for HTTPS traffic.
5. **Active Directory and Group Policy**:
    - **Port 389**: Used for LDAP.
    - **Port 636**: Used for LDAP over SSL.
    - **Port 88**: Used for Kerberos authentication.
    - **Port 3268**: Used for Global Catalog.



WSUS HTTP Port 8530 Properties

General

Name: WSUS HTTP Port 8530

Description:

☑ Enabled

Action

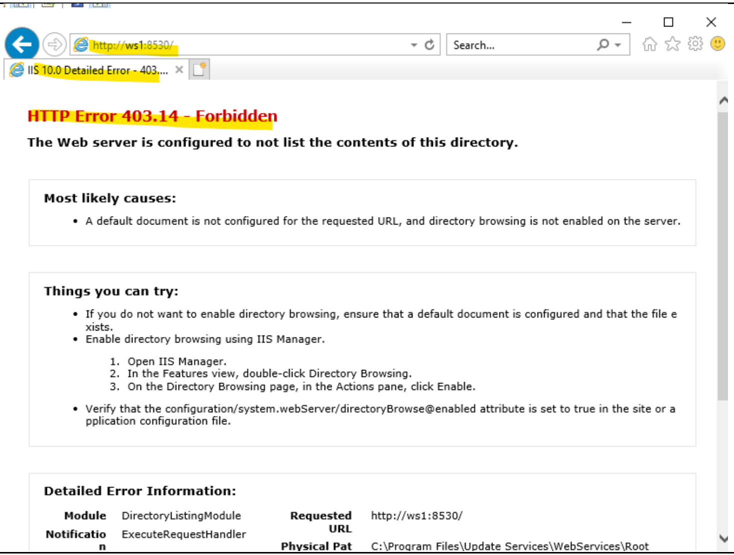
● Allow the connection

○ Allow the connection if it is secure

○ Block the connection

Example of configured inbound rule on HTTP port in Windows Defender Firewall with Advanced Security

8



HTTP Error 403.14 - Forbidden

The Web server is configured to not list the contents of this directory.

Most likely causes:

- A default document is not configured for the requested URL, and directory browsing is not enabled on the server.

Things you can try:

- If you do not want to enable directory browsing, ensure that a default document is configured and that the file exists.
- Enable directory browsing using IIS Manager.
    1. Open IIS Manager.
    2. In the Features view, double-click Directory Browsing.
    3. On the Directory Browsing page, in the Actions pane, click Enable.
- Verify that the configuration/system.webServer/directoryBrowse@enabled attribute is set to true in the site or application configuration file.

Detailed Error Information:

Module	DirectoryListingModule	**Requested URL**	http://ws1:8530/
Notification	ExecuteRequestHandler	**Physical Pat**	C:\Program Files\Update Services\WebServices\Root

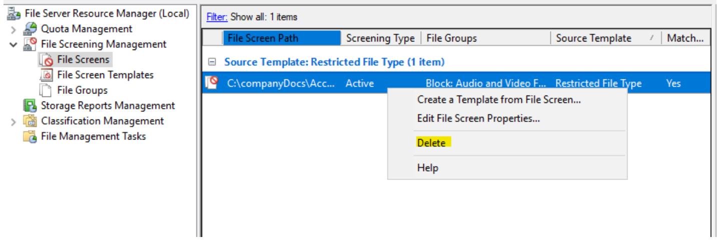
	Testing the connection to the HTTP port, page loads but the specific console is forbidden access as it has not been configured in IIS.

List At the three most useful Internet resources that you used (provided by the tutor)

• Create and Link GPOs • https://www.pcwdld.com/group-policy-management
• GPO Administrative templates • https://www.youtube.com/watch?v=Afzd9AgU57U • GPO Desktop wallpaper • Deploy Desktop Background Wallpaper using Group Policy
• GPO Windows settings • http://woshub.com/password-policy-active-directory/

List all (at least three) Internet resources that you found and used that were not provided by the tutor)

https://www.youtube.com/watch?v=2olvZOgn0LQ
https://www.youtube.com/watch?v=Yv0qjxdX5yw&t=441s
https://www.youtube.com/watch?v=o4KXp9Wefbw

Problem	Solution
Pictures not accessible by the accounts group	 File Server Resource Manager (Local) Quota Management File Screening Management File Screens File Screen Templates File Groups Storage Reports Management Classification Management File Management Tasks Create a Template from File Screen... Edit File Screen Properties... Delete Help Filter: Show all: 1 items File Screen Path | Screening Type | File Groups | Source Template | Match... Source Template: Restricted File Type (1 item) C:\companyDocs\Acc... | Active | Block: Audio and Video F... | Restricted File Type | Yes The file screen must be deleted that was set up in LAB4
No backgrounds set due to unlicensed Client VM	The GPO to configure backgrounds could not assign backgrounds via the shared wallpaper folder as the client VM did not have a valid copy of windows installed.