

Lab ADDS / Group Policy

Objectives:

- Create an organizational unit (OU) in our domain.
- Create a group policy that enforces various options.
- Apply settings to the groups and computers in the newly created OU.

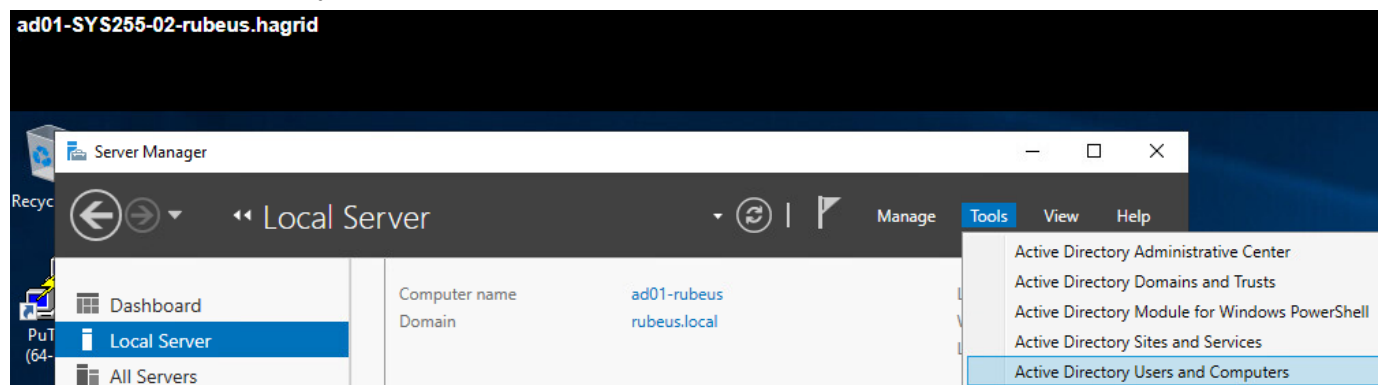
Prerequisites:

Lab 4 is complete and is in a happy place.

💣 **Achtung:** Watch this lab's firm Due Date. As mentioned in class, the current VM infrastructure will be deleted, and be replaced with newer VMs just prior to the next class for the Assessment. Additionally, since this is a lighter lab, there are no extensions.

OU Structure Creation

Open up Active Directory Users and Computers

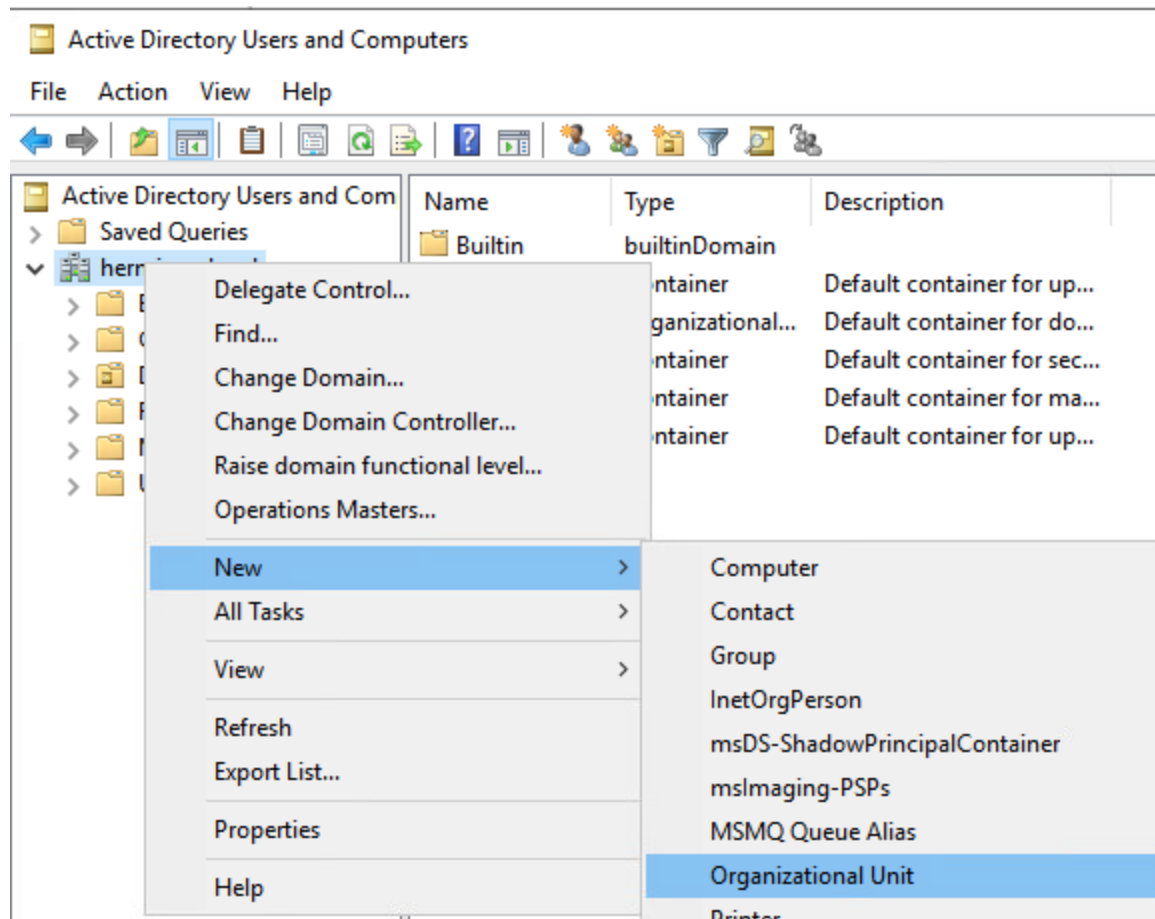


The first thing we want to do is create an organizational unit called "SYS255", & within this OU we will add child OU's for Accounts, Computers, and Groups.

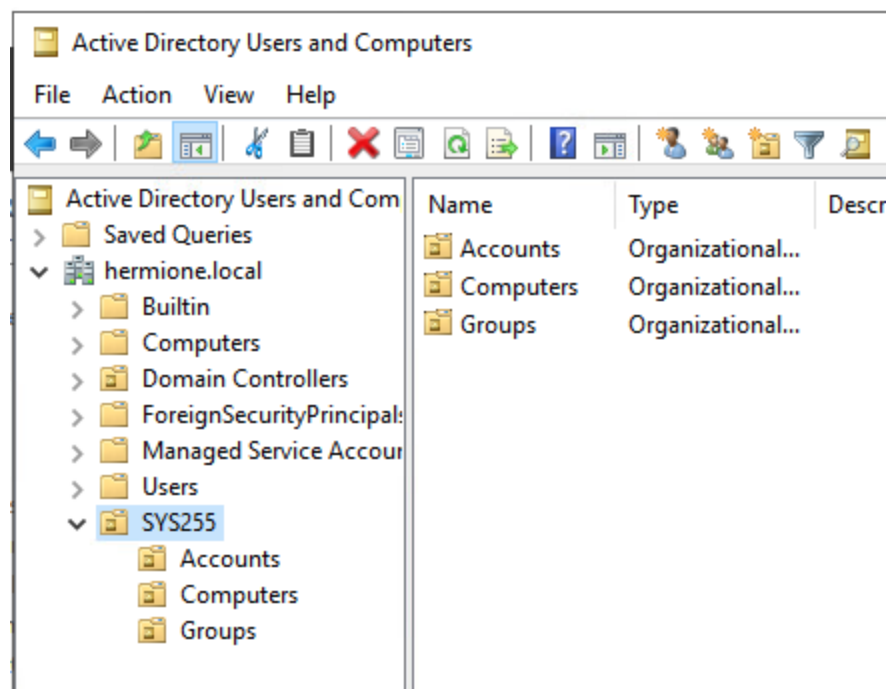
💡 Although the default installation of ADDS provides a structure for Users and Computers, we are adding our own to distinguish the objects we add from those that are included by default.



LET US DARE

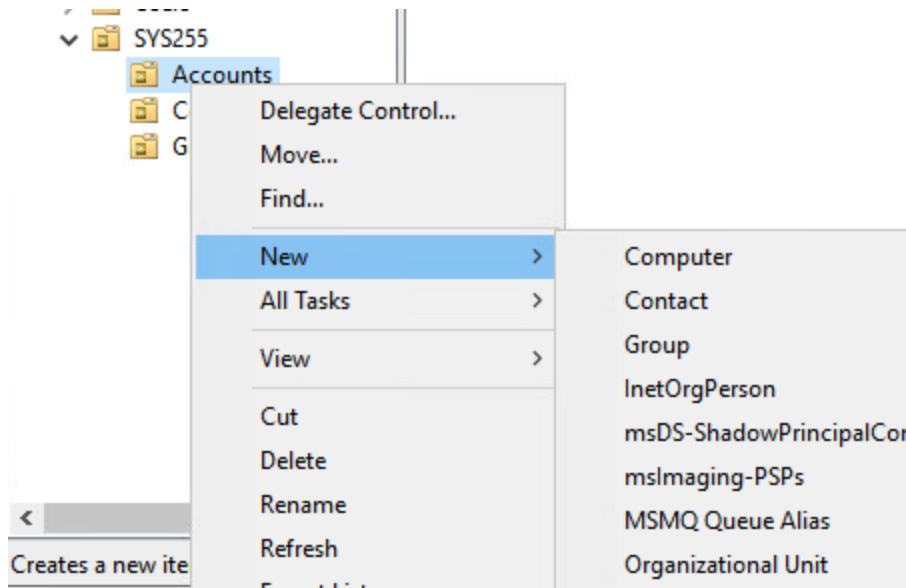


Here's the completed structure shown below:



LET US DARE

💡 Notice that now this is created, we can right-click and create users, groups, and other domain objects in Active Directory. All of these objects are defined by what's known as the Schema, which can be thought of as an instruction sheet listing all the available pieces in AD. In this case, the schema objects make up a database, which is what ADDS essentially is.



Create Users and Groups

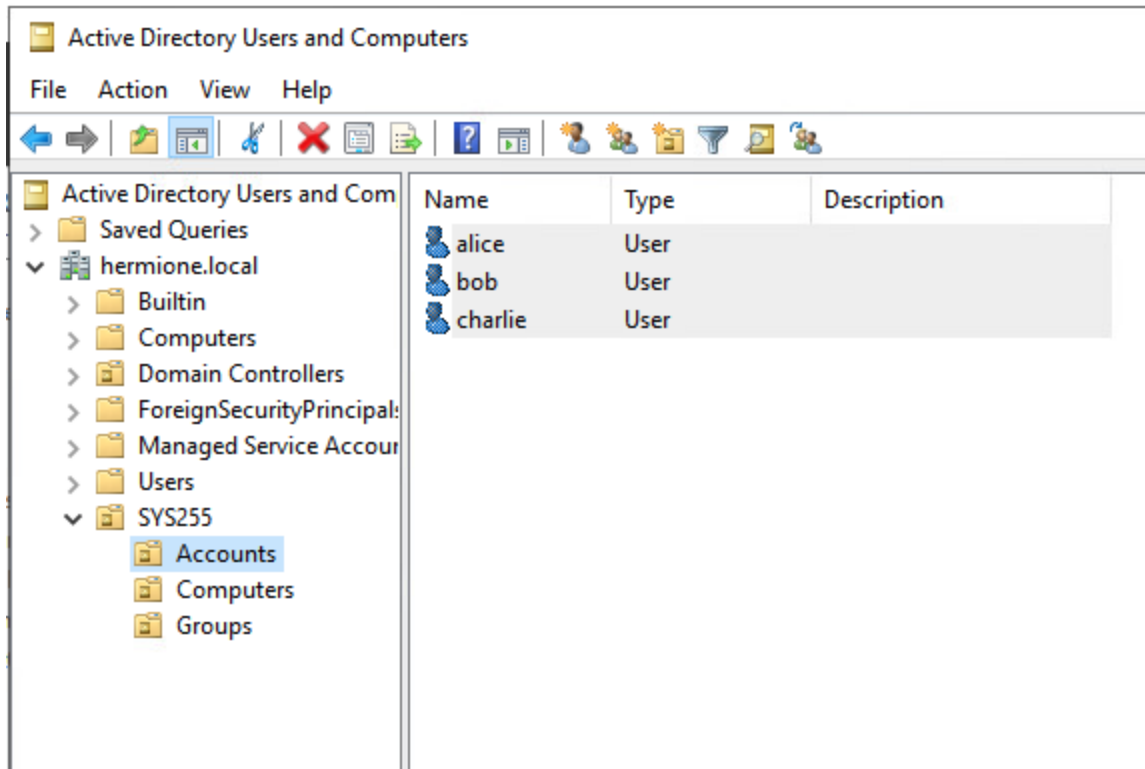
Within the SYS255\Accounts OU, create users Alice, Bob and Charlie

💡 When creating accounts for other users, it is wise to allow them to create a new password at first login. For purposes of the lab, you can clear this check mark.

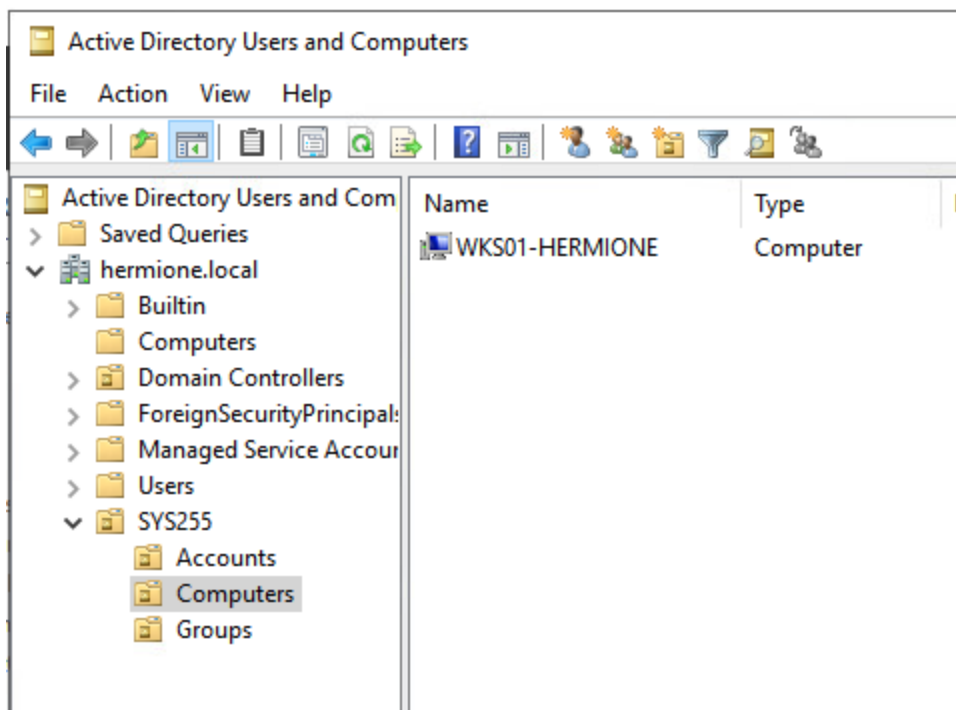
☒ User must change password at next logon



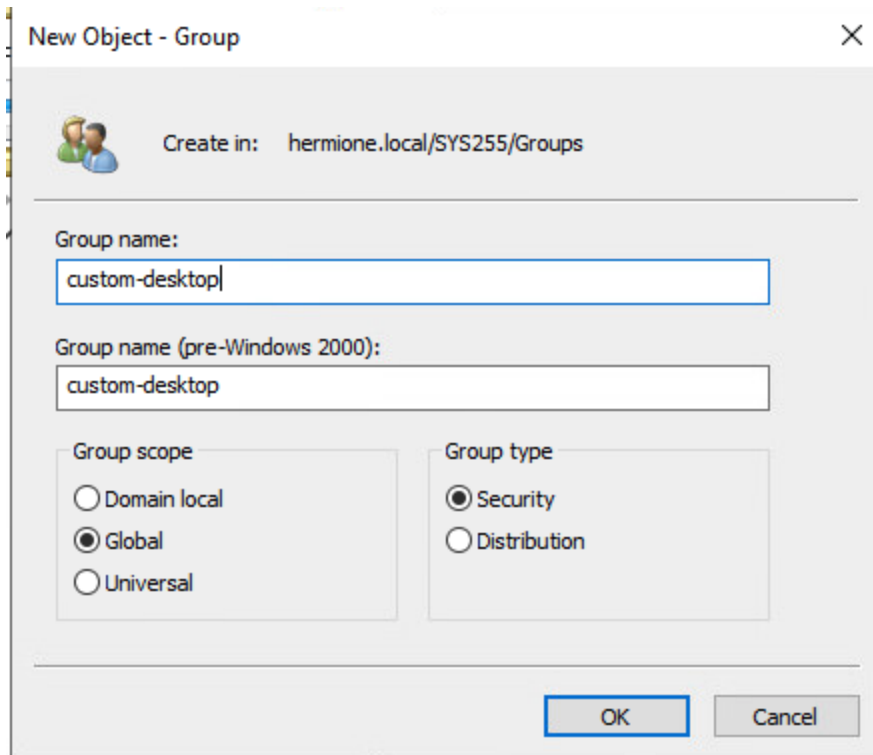
LET US DARE



Drag WKS01 from the yourname.local\Computers Folder to the SYS255\Computers OU. This will allow us to treat SYS255 OU Computers differently than others.



Within the SYS255\Groups OU, add a global security group called *custom-desktop* with users Alice and Bob (not Charlie) as members.



The screenshot shows the 'New Object - Group' dialog box in Active Directory. The 'Create in' field is set to 'hermione.local/SYS255/Groups'. The 'Group name' field contains 'custom-desktop'. The 'Group name (pre-Windows 2000)' field also contains 'custom-desktop'. Under 'Group scope', the 'Global' radio button is selected. Under 'Group type', the 'Security' radio button is selected. The 'OK' button is highlighted with a blue border.

New Object - Group

Create in: hermione.local/SYS255/Groups

Group name:
custom-desktop

Group name (pre-Windows 2000):
custom-desktop

Group scope

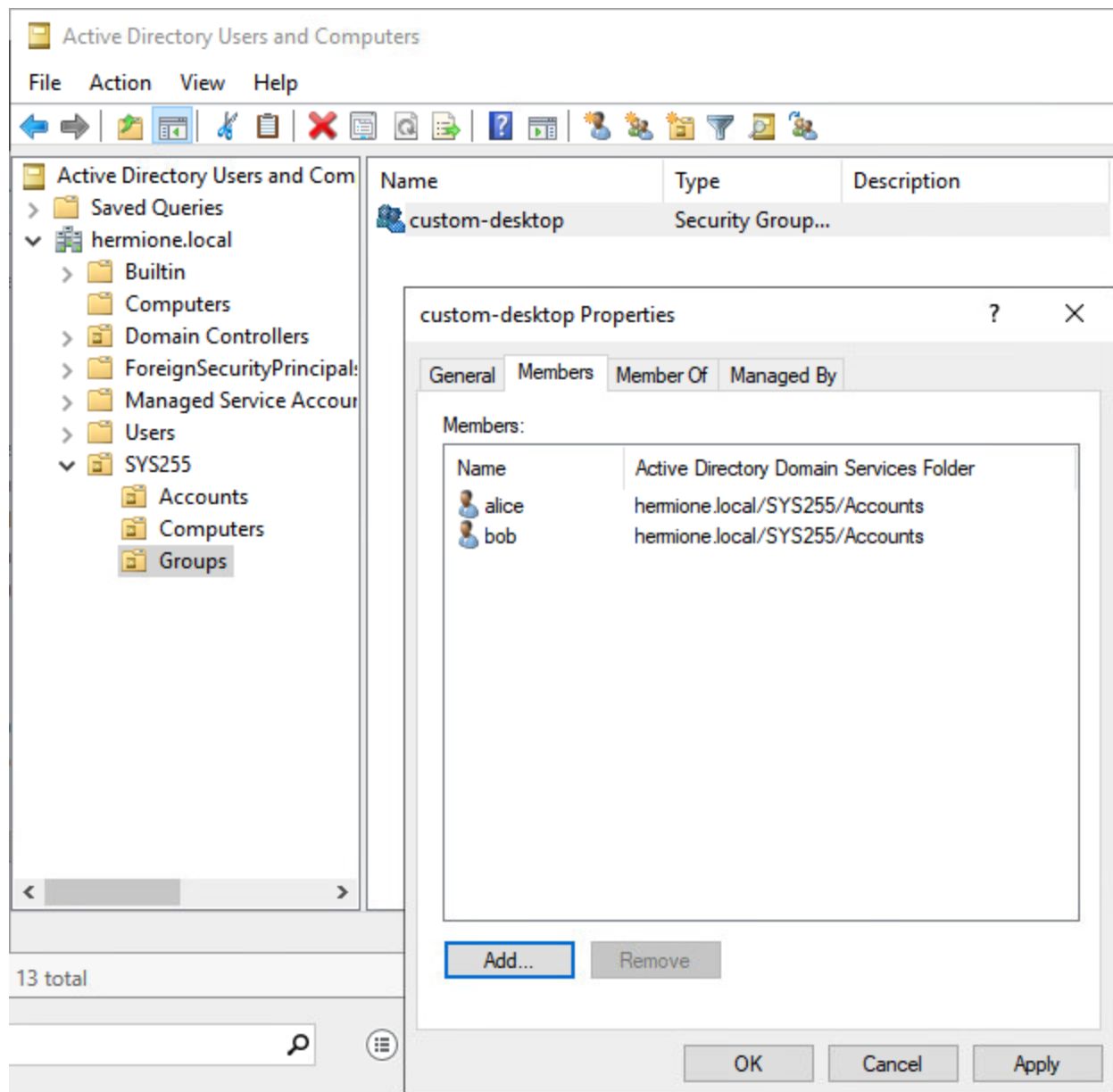
- ☐ Domain local
- ☒ Global
- ☐ Universal

Group type

- ☒ Security
- ☐ Distribution

OK Cancel





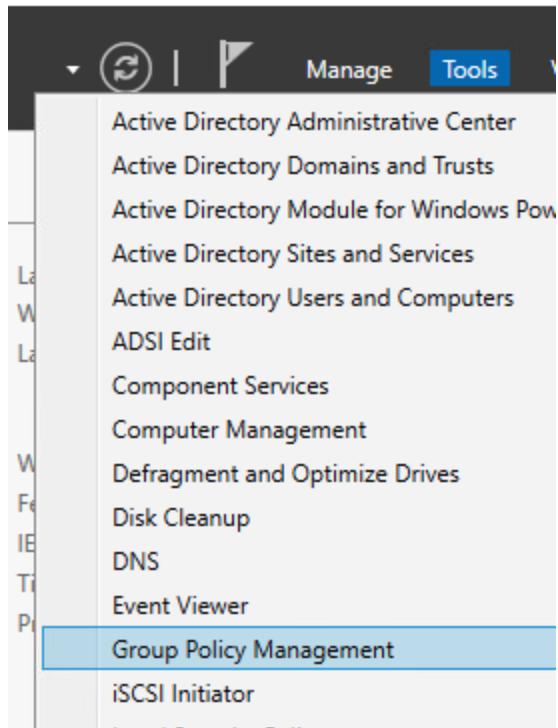
💡 **BEST PRACTICE FOR GROUPS:** Many times, organizations will have a number of groups defined in their AD domain. For this reason, it is a best practice to have a naming convention that purposefully describes what the groups do. A lot of times, groups allow or disallow users permission to folders and resources on the network. For this reason, a commonly found group membership is in the form of something like this: DepartmentName_RW_ACL or GP_WindowsIESettings_ACL. This gives administrators an idea of what the group is for, and who may need to be a member.



LET US DARE

Group Policy - User

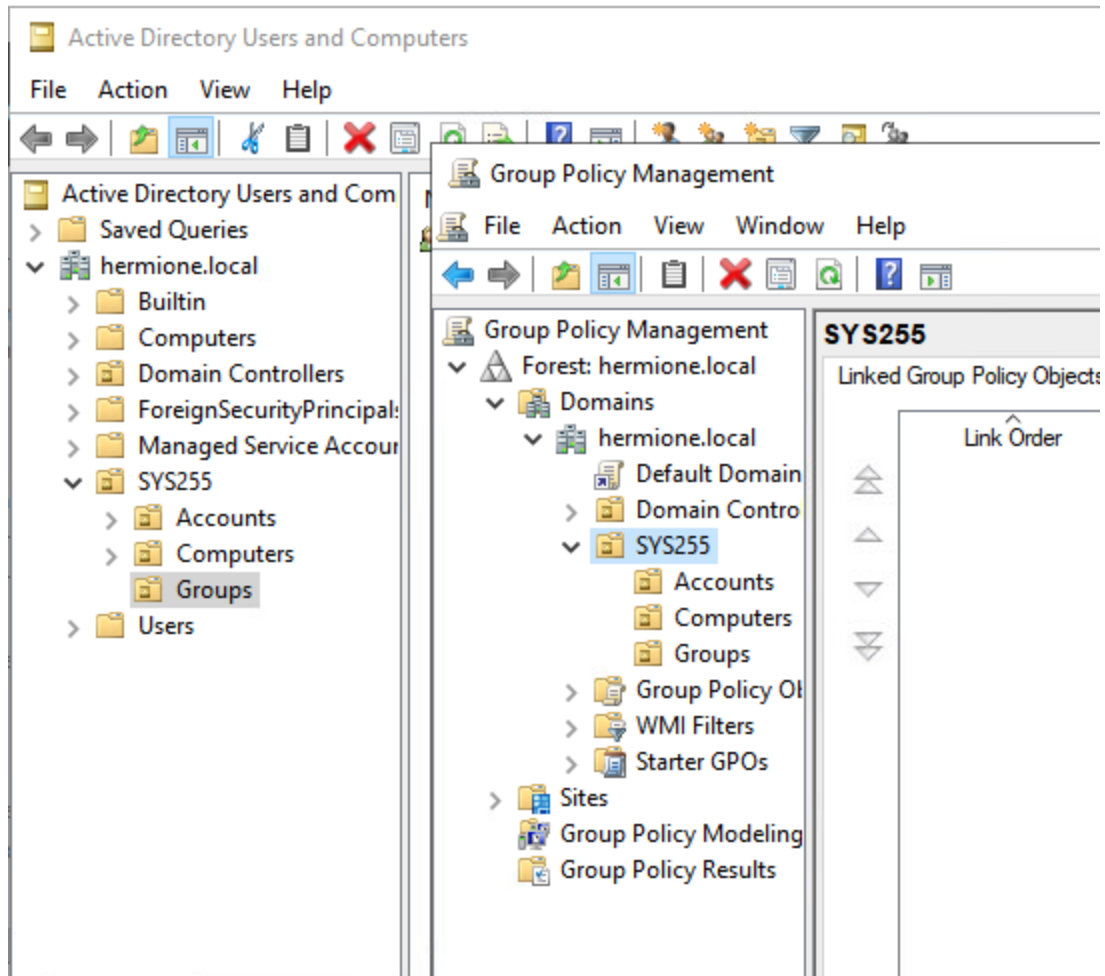
Now, let's create a group policy that defines some User level settings:



The following screenshot illustrates the relationship between the OU's created in Active Directory and the Policy hierarchy shown in the Group Policy Management window. The big takeaway is that the group policy window does not show the contents of an OU like accounts and computers, but allows you to apply policy to them.



LET US DARE



Notice how there is already a Default Domain Policy. This is what controls that pesky default password expiration and complexity requirements.

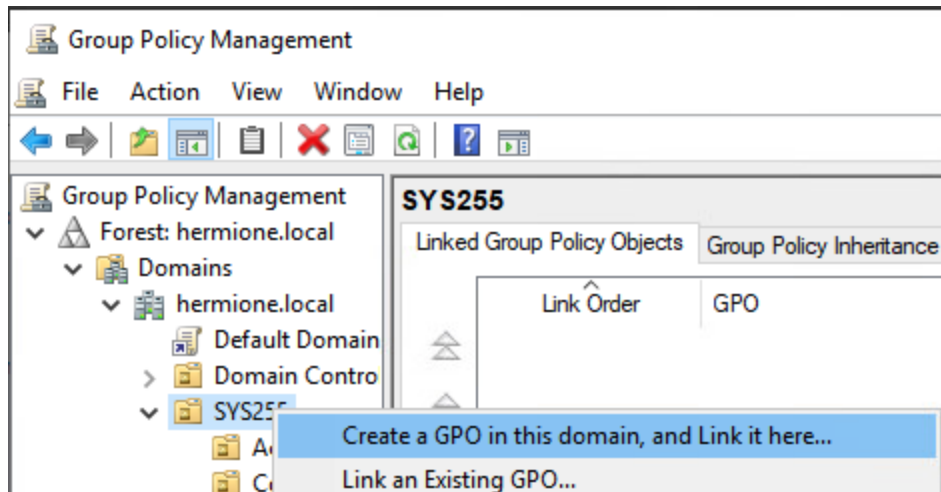
💣 Weak Administrator credentials are the root cause for many security breaches! While the default password complexity rules are good, one should only increase security of credentials.

Creating a User Policy

Select the SYS255 OU and create a new group policy object (GPO) called sys255-desktop. Once created, right click on the object and select Edit.



LET US DARE

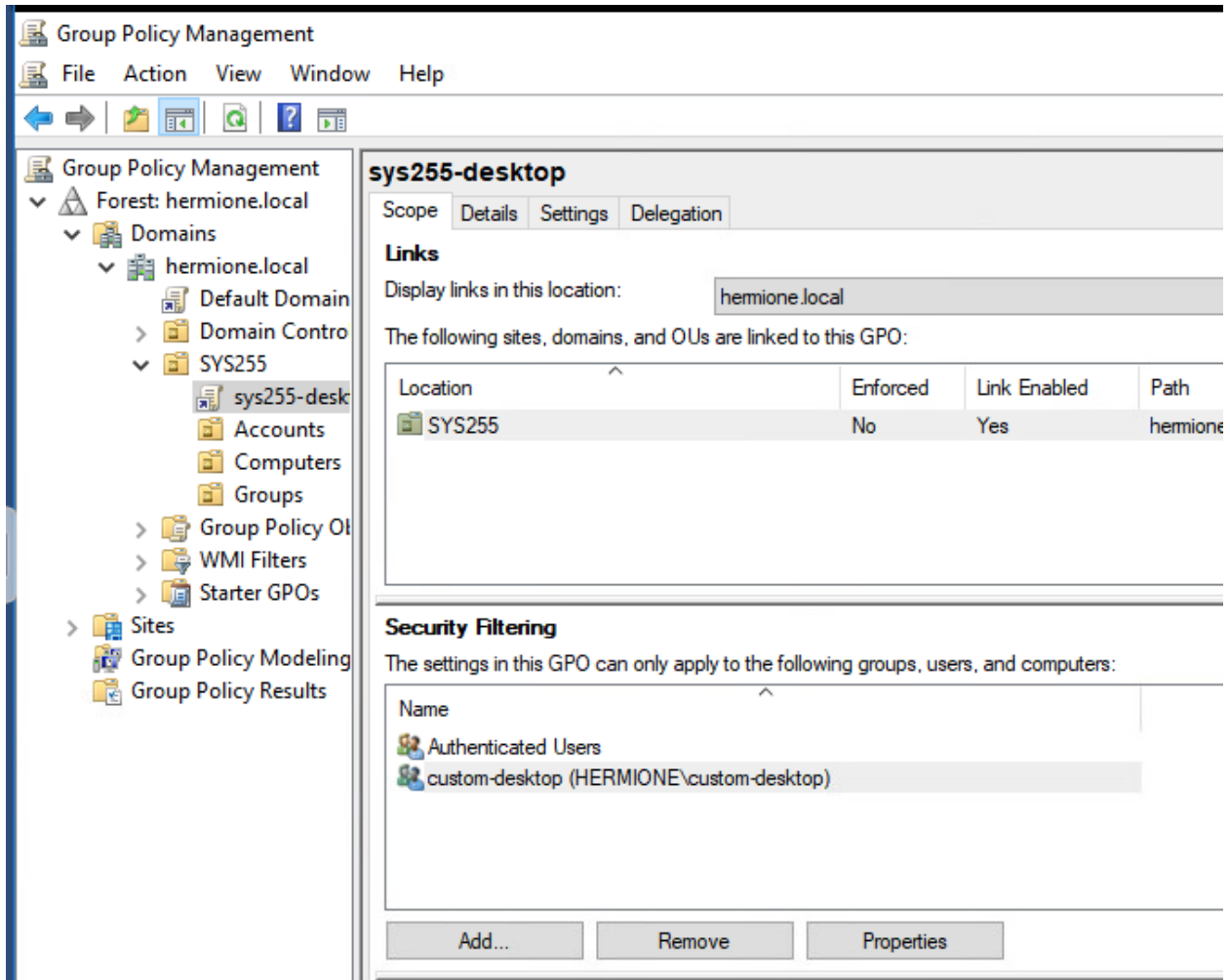


Now, this SYS255-desktop Group Policy should only apply to those users in this OU who are members of the custom-desktop security group. You set this using the security filters section of the group policy. By default, All Authenticated Users have access to apply and read group policy, we will restrict this through the following steps.

Step 1. Add the custom-desktop group created earlier to the Security Filter



LET US DARE

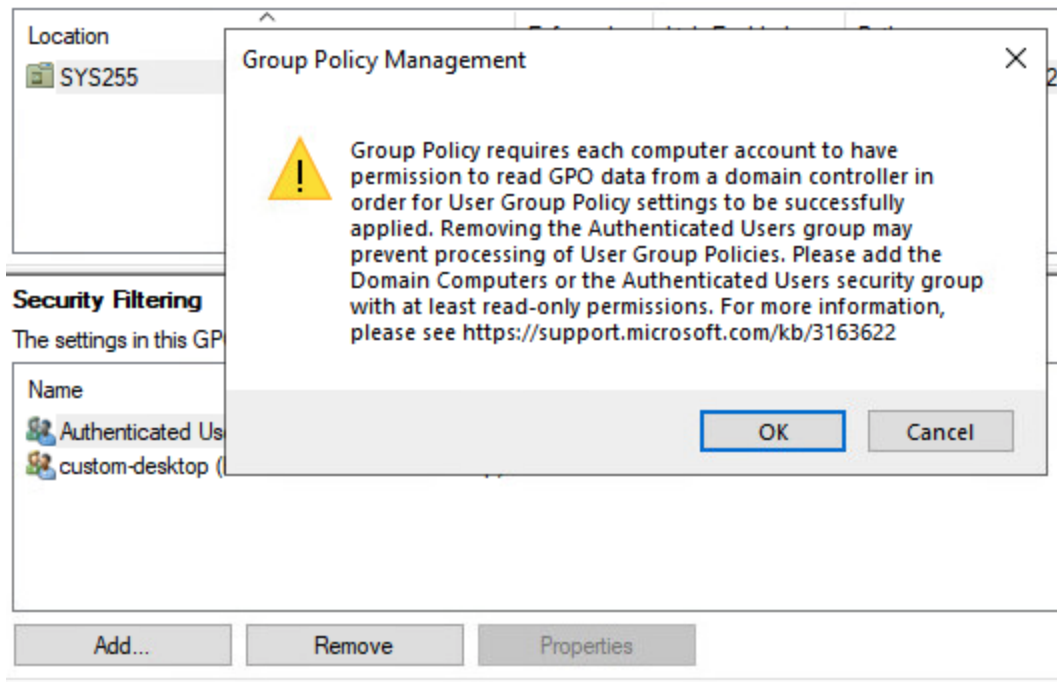


Step 2. Remove Authenticated Users from the Security Filter.

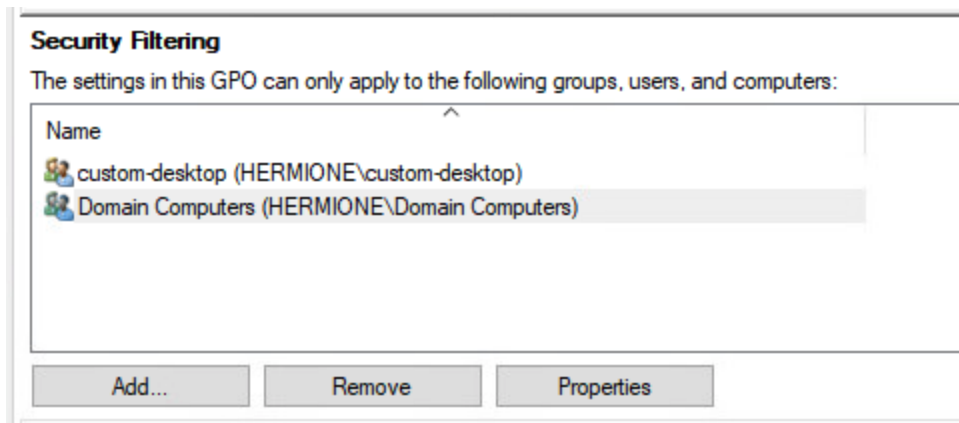
💡 For more information on this error message which was a source of consternation among Windows Admins back in 2016, see <https://go.microsoft.com/fwlink?linkid=843010>



LET US DARE



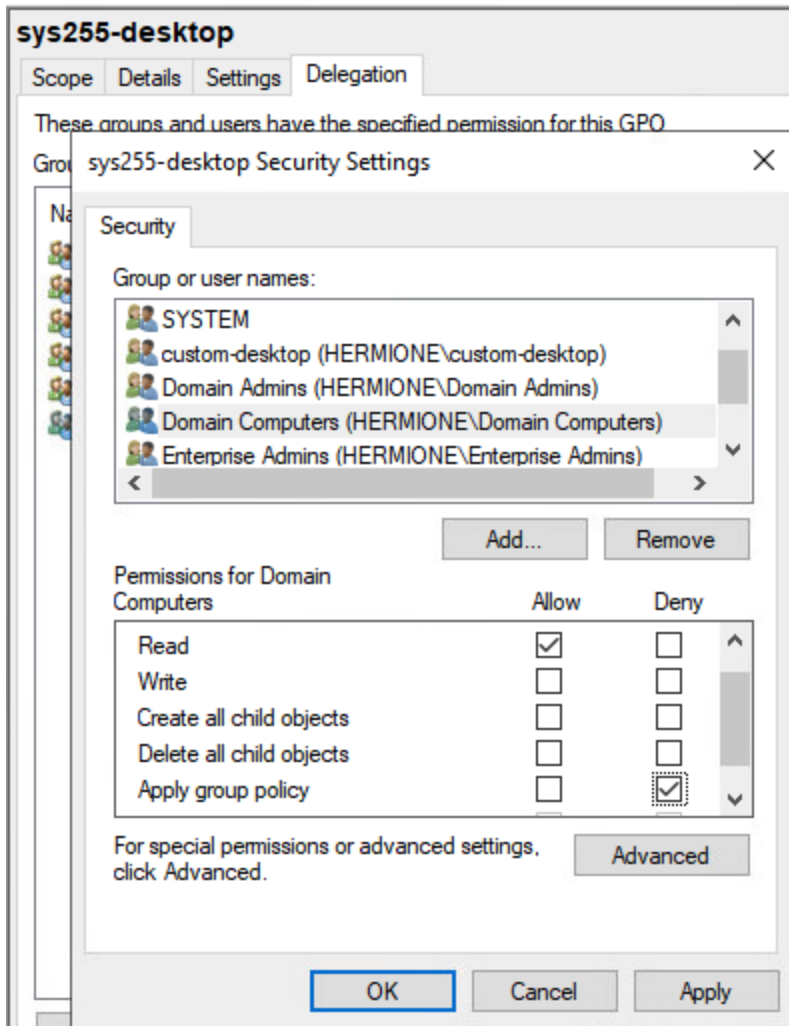
Step 3, Add Domain Computers



Step 4. Delegation tab -> Advanced (Uncheck Apply Group Policy, Select Deny)



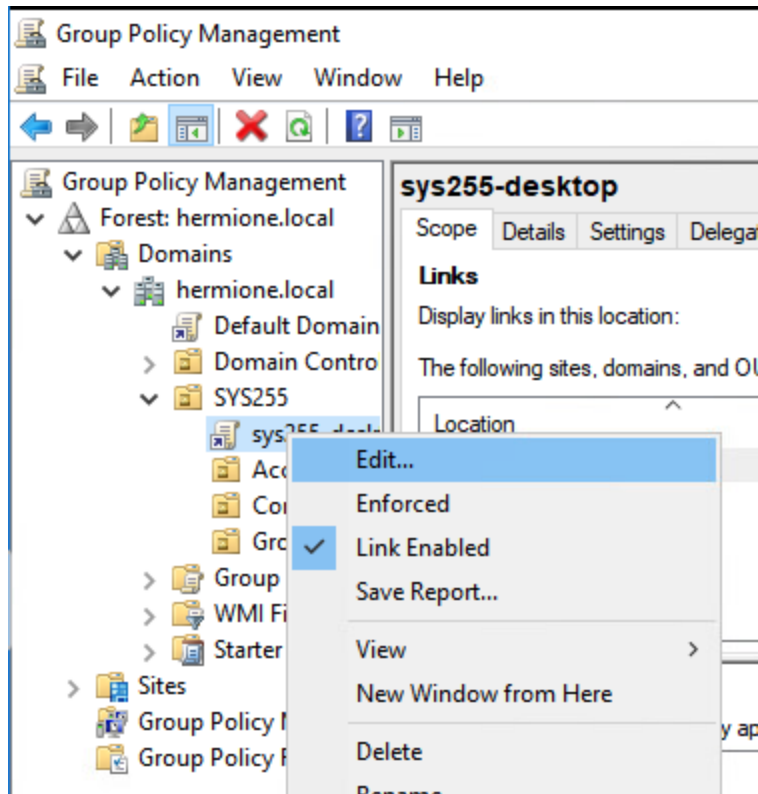
LET US DARE



Once we have defined who this policy applies to, we are now ready to author what the group policy does.



LET US DARE



💡 This is the bulk of the group policy editor on a Windows server where we can define computer and user settings. Remember: COMPUTER settings are applied when workstations turn on, where USER settings apply after users login.

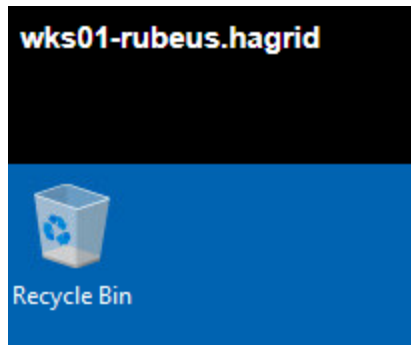
There are a handful of settings here that we can define and really control the experience of the workstation in this domain. This is commonly used to control things such as, but not limited to: desktop backgrounds, browser settings, password policies, network shares, printers, redirected folders, Microsoft Bitlocker, application allowed list policies, logon scripts, etc.

Nuking the Recycle Bin

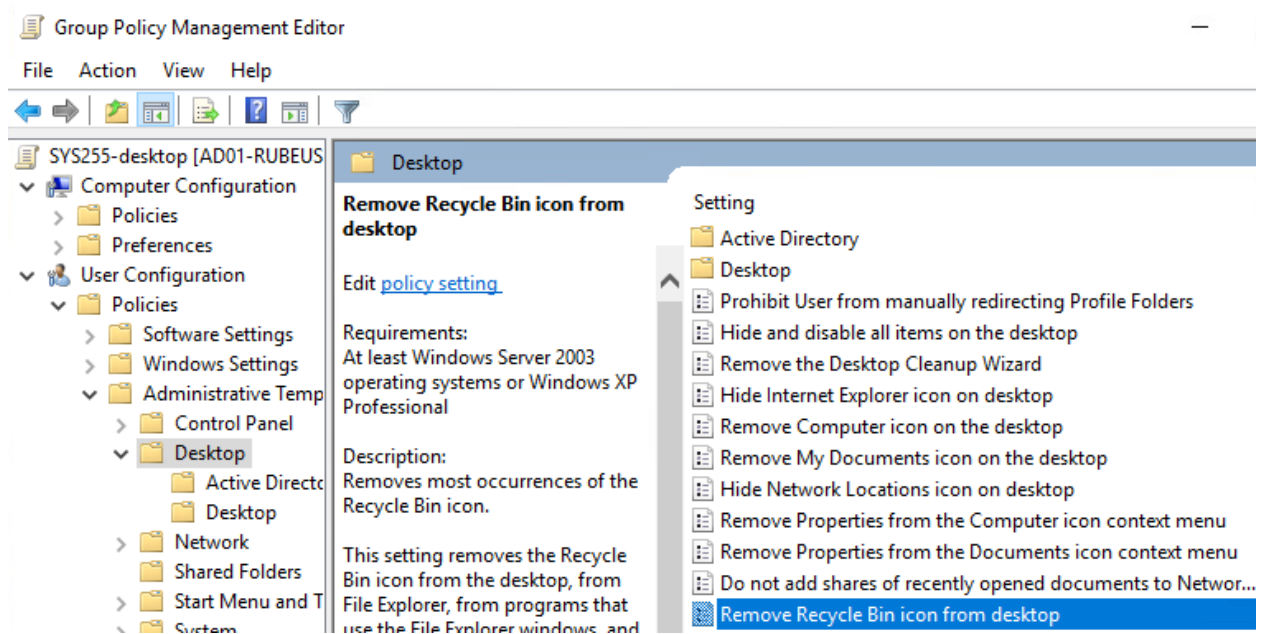
Your users are revolting against the Recycle Bin, so let's remove it.



LET US DARE



Find the Remove Recycle Bin icon setting under User Configuration, and click Edit Policy Setting in the group policy editor.



Enable the Remove Recycle Bin Icon from Desktop setting. Note: Frequently in AD GPO settings, its wording can be tricky, where you enable/allow the removal of a feature/function.



LET US DARE

Remove Recycle Bin icon from desktop

Remove Recycle Bin icon from desktop

Previous Setting Next Setting

☐ Not Configured Comment:

☒ Enabled

☐ Disabled

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options:

Help:

Removes most occurrences of the Recycle Bin icon.

This setting removes the Recycle Bin icon from the desktop, from File Explorer, from programs that use the File Explorer windows, and from the standard Open dialog box.

This setting does not prevent the user from using other methods to gain access to the contents of the Recycle Bin folder.

Note: To make changes to this setting effective, you must log off and then log back on.

Click Apply. Ok, and close the Group Policy editor.



LET US DARE

Deliverable 1. Login to WKS01 as Alice, and your desktop should not include the Recycle Bin. Provide a screenshot showing both your VM name, the lack of Recycle Bin, and the results of gpresult /r (using Alice's account).

wks01-rubeus.hagrid

Select Windows PowerShell

Created on [9/ 27/ 2020 at 4:17:09 PM

RSOP data for RUBEUS\alice on WKS01-RUBEUS : Logging Mode

```
-----
OS Configuration:      Member Workstation
OS Version:            10.0.17763
Site Name:             N/A
Roaming Profile:       N/A
Local Profile:         C:\Users\alice
Connected over a slow link?: No
```

USER SETTINGS

```
-----
CN=alice,OU=Accounts,OU=SYS255,DC=rubeus,DC=local
Last time Group Policy was applied: 9/27/2020 at 4:16:34 PM
Group Policy was applied from:      ad01-rubeus.rubeus.local
Group Policy slow link threshold:   500 kbps
Domain Name:                       RUBEUS
Domain Type:                       Windows 2008 or later
```

Applied Group Policy Objects

SYS255-desktop

The following GPOs were not applied because they were filtered out

```
-----
Local Group Policy
Filtering: Not Applied (Empty)
```

The user is a part of the following security groups



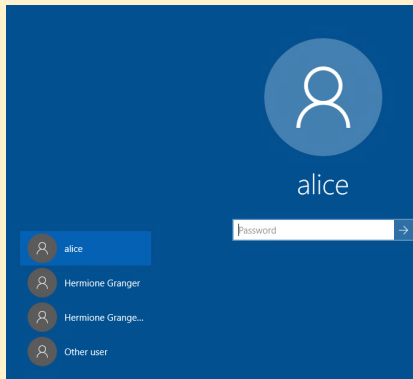
LET US DARE

Creating a Computer Policy

💡 Unlike User policies that are associated with the logged on user, Computer policies are applied before login and affect the entire system and thus any logged in users.

Disable Last Login

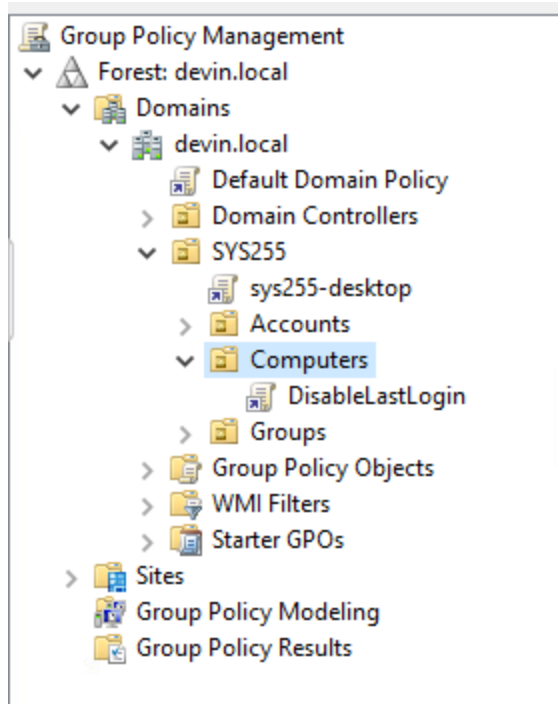
💡 The default display of previously logged on users is widely considered a security vulnerability, particularly in shared systems. The next policy will turn off the default display of previously logged in users:



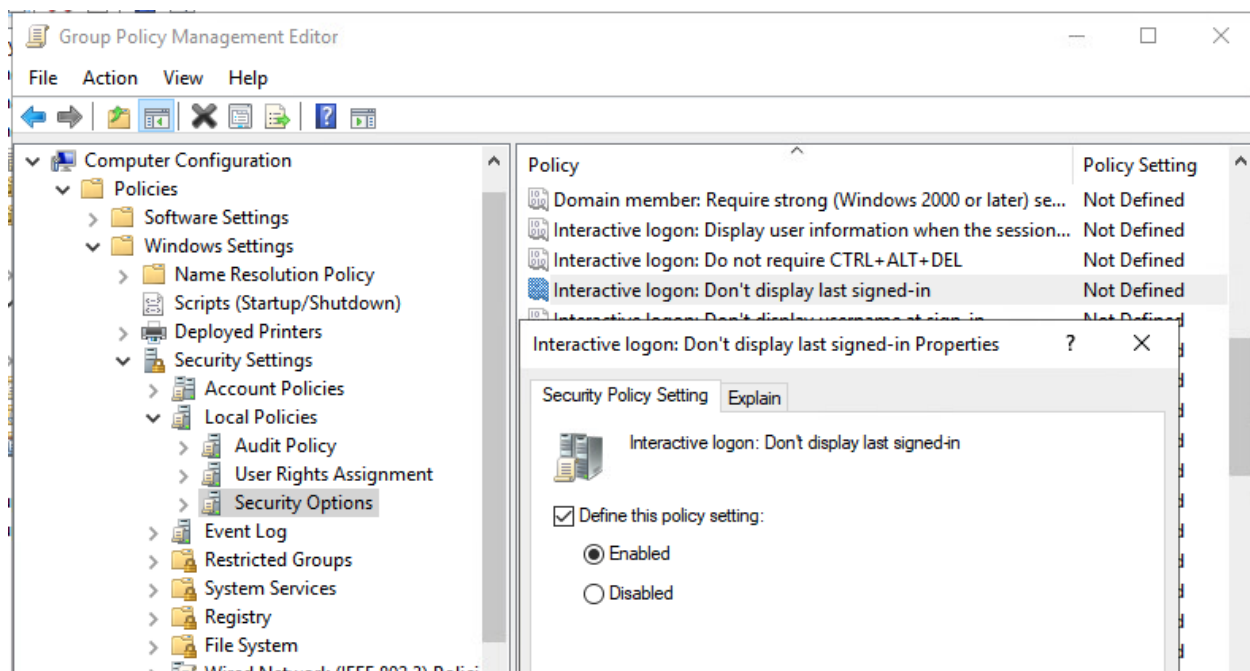
Create and Link a new GPO within the SYS255\Computers OU called *DisableLastLogin*.



LET US DARE



The Security Filter on this policy should be applied to Domain Computers (not Authenticated Users) similar to earlier. Then edit the policy so that the "Do not display last user name" is enabled.

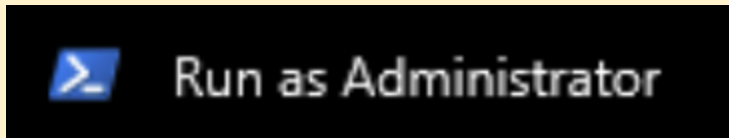


Deliverable 2: On WKS01, from an elevated domain administrative command prompt, issue the following commands:

- `gpupdate /force`
- `gpresult /scope computer /r`

Provide a screenshot showing the DisableLastLogin Policy was applied.

💡 Even though you may be logged into WKS01 as the -adm AD power account, you still need to elevate your command prompt or powershell session to “Run as Administrator”. Try right-clicking over the shortcut for command or powershell.



LET US DARE

wks01-rubeus.hagrid

```
Select Administrator: Windows PowerShell

Created on 9/6/2020 at 9:04:05 PM

Recy
RSOP data for on WKS01-RUBEUS : Logging Mode
-----
OS Configuration:      Member Workstation
OS Version:            10.0.17763
GoSite Name:           Default-First-Site-Name
ChRoaming Profile:
Local Profile:
Connected over a slow link?: No

COMPUTER SETTINGS
-----
Wire
CN=WKS01-RUBEUS,OU=Computers,OU=SYS255,DC=rubeus,DC=local
Last time Group Policy was applied: 9/6/2020 at 9:03:33 PM
Group Policy was applied from:      ad01-rubeus.rubeus.local
Group Policy slow link threshold:   500 kbps
Domain Name:                        RUBEUS
Domain Type:                        Windows 2008 or later

Applied Group Policy Objects
-----
DisableLastLogin
Default Domain Policy

The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

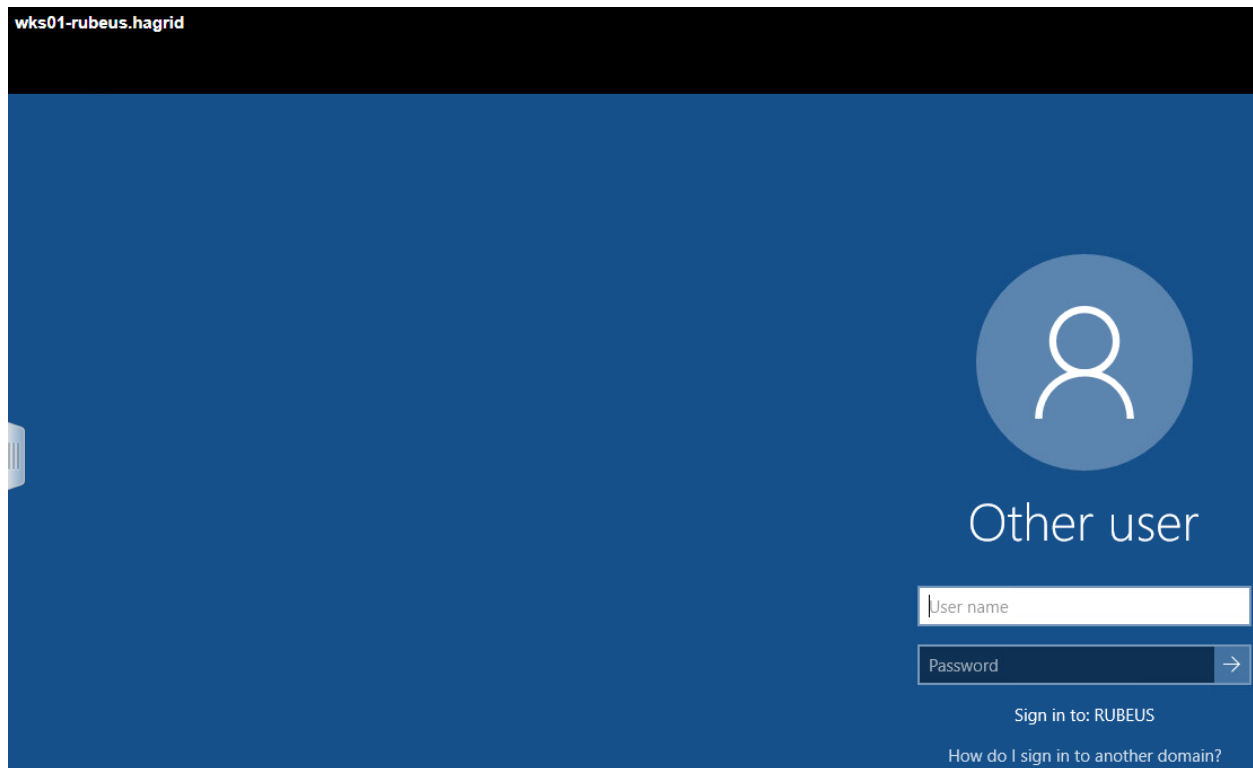
The computer is a part of the following security groups
-----
BUILTIN\Administrators
Everyone
BUILTIN\Users
NT AUTHORITY\NETWORK
NT AUTHORITY\Authenticated Users
This Organization
WKS01-RUBEUS$
Domain Computers
Authentication authority asserted identity
System Mandatory Level

PS C:\Windows\system32>
```



LET US DARE

Deliverable 3. Sign out of WKS01, and provide a screenshot showing the changes to the login screen. You should no longer see evidence of the last user who had logged in.



Deliverable 4: For your Tech Journal Entry - Create a detailed plan of how to prepare for next week's assessment. This plan should include a Current Network Diagram (example tool: <https://app.diagrams.net>) containing at least devices, hostnames, IPs, services, and "cabling".



LET US DARE