Security Lab

Lab 4: Enterprise Group Policy for Security

Systems Security Management

Document Sections

Lab Purpose – General discussion of the purpose of the lab

Lab Goal – What completing this lab should impart to you

Lab Instructions – Instructions for carrying out the lab

Lab Deliverables – What you have to submit to your instructor

Lab Rubric – How this assignment will be graded

Lab Resources – Any useful resources for completing the lab deliverables

Lab Purpose

As we learned in Module 10 and in Lab 3, Microsoft's Active Directory Domain Services is an Enterprise-level authentication and authorization platform. Lab 3 barely scratched the surface of what you can do in AD. To take your learning a step further we will work with one of the most powerful parts of AD: Group Policy. Group Policy is designed to provide system and network administrators with a centralized tool to enforce specific configuration settings on desktop, laptop, tablet, and server systems. These configuration settings

The purpose of this lab is to familiarize you with various aspects of account and computer-based security using Group Policy. This lab has four (4) parts:

1. Group Policy
2. Organizational Unit Security Design
3. Security Settings in Group Policy
4. Research and Recommend Security Settings

<u>Group Policy</u>

Despite the name Group Policy, groups actually have little to do with how group policy is enforced. Group Policy is a tool within Active Directory that gives System Administrators the ability to have fine-grained control over the systems and other computers they are responsible for. Group Policy includes settings for desktops, laptops, tablets, and servers running Windows operating systems that run the gamut from security settings all the way to controlling which applications you can run, Internet Explorer configuration settings, or even control how your desktop looks and operates. As such, it is an extremely powerful tool that, when used properly, can increase security and manageability of an enterprise computing environment.

<u>Organizational Unit Security Design</u>

The primary way a system administrator will apply group policy is by attaching a Group Policy Object (GPO) to an Organizational Unit (OU) or folder within Active Directory. Security Groups can be used as a security setting on the GPO so that the policies contained within are only applied to users or computers that are members of the specific security group. Otherwise, the default behavior of group policy is to apply the policy to any user or computer object contained inside of the OU. So, if you wanted a policy to only apply to users in the Sales department, you would create a Sales OU, assign the GPO to the OU, and place the user accounts of the people who should have these policies inside the OU. This is one of the main reasons to really plan for security in addition to organizational hierarchy when creating your active directory. Does this mean that OUs are required? Not at all. You can easily assign the GPO to the root folder of the active directory (which you will do in this lab) and it will apply to all users and computers in AD.

Security Settings in Group Policy

You will work with just a few of the hundreds of possible security settings in Group Policy during this lab. You will start with reviewing default password policies for the AD domain, then add a new GPO and a few other settings that are commonly used. Feel free to spend extra time after completing the lab trying different settings to see what they do.

Research and Recommend Security Settings

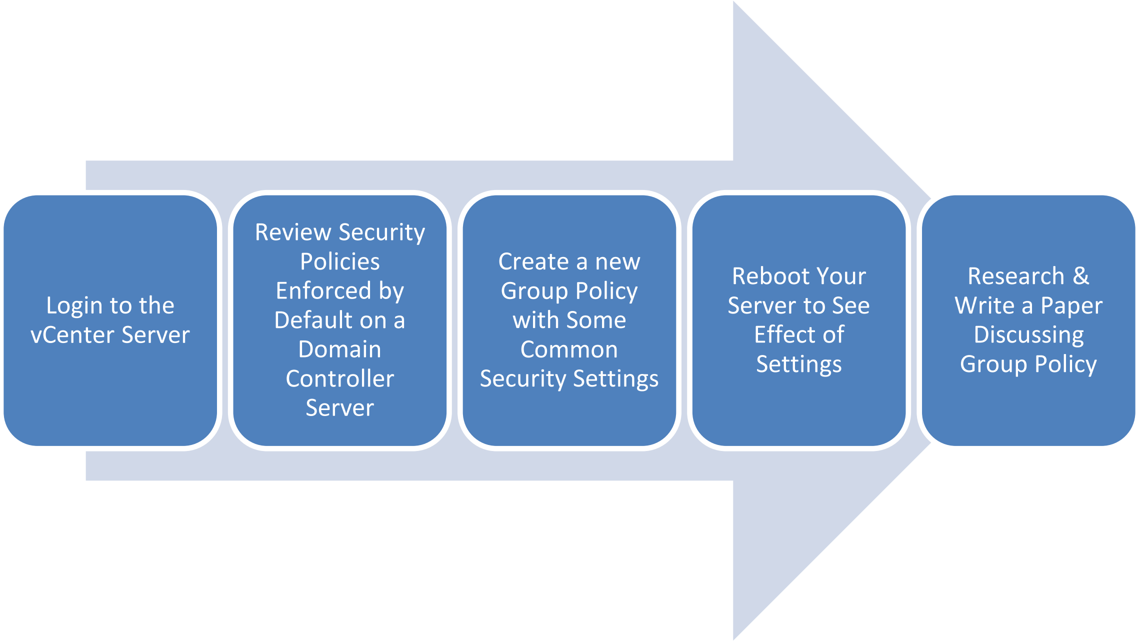
After you have completed the server portion of this lab and have seen some of what you can do to help secure networks and systems using GPOs, you will need to research a minimum of three additional group policy settings that can be applied to improve the security of systems. Be prepared to write a paper explaining each of the policies, including possible configuration options, how the policy works and what it does, and why an organization should use the policy settings.

Lab Goal

Upon completion of this lab, you should have:

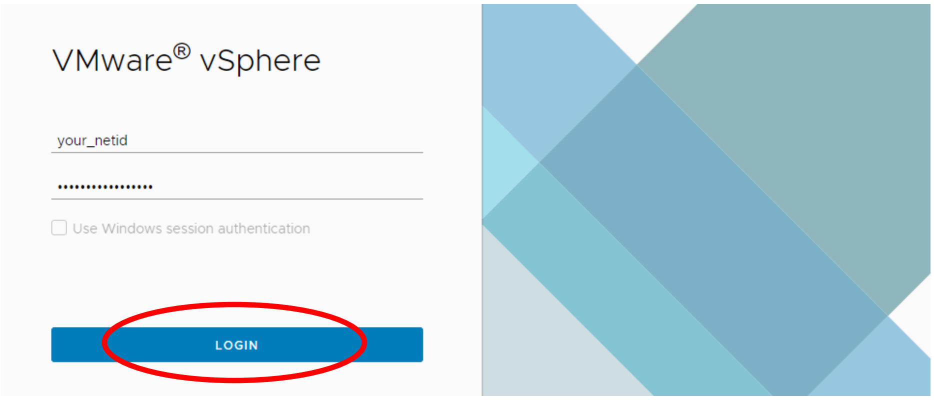
- Introduced you to Group Policy for Active Directory
- Further reinforce why designing security into an AD design is important
- Increase your awareness and understanding of several common security settings in Group Policy that can be enforced
- Provide hands-on experience creating group policies and seeing how they affect an operating system when applied.
- Provide experience researching other possible security settings that can be enforced in Group Policy

Lab Instructions


Login to the vCenter Server
Review Security Policies Enforced by Default on a Domain Controller Server
Create a new Group Policy with Some Common Security Settings
Reboot Your Server to See Effect of Settings
Research & Write a Paper Discussing Group Policy

1. Login to the vCenter Server

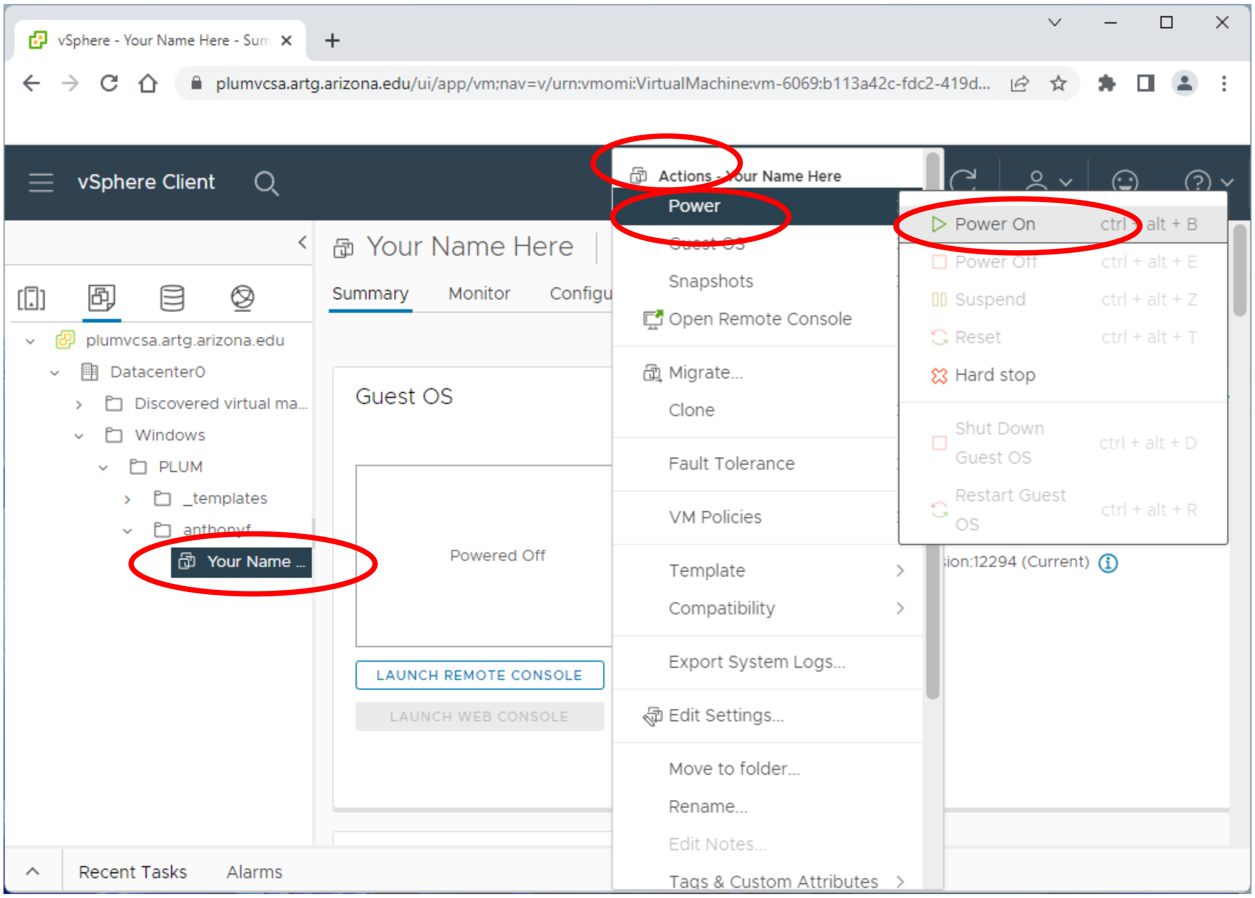
1) Connect to the UA VPN, then open your web browser and navigate to https://plumvcsa.artg.arizona.edu/ui/



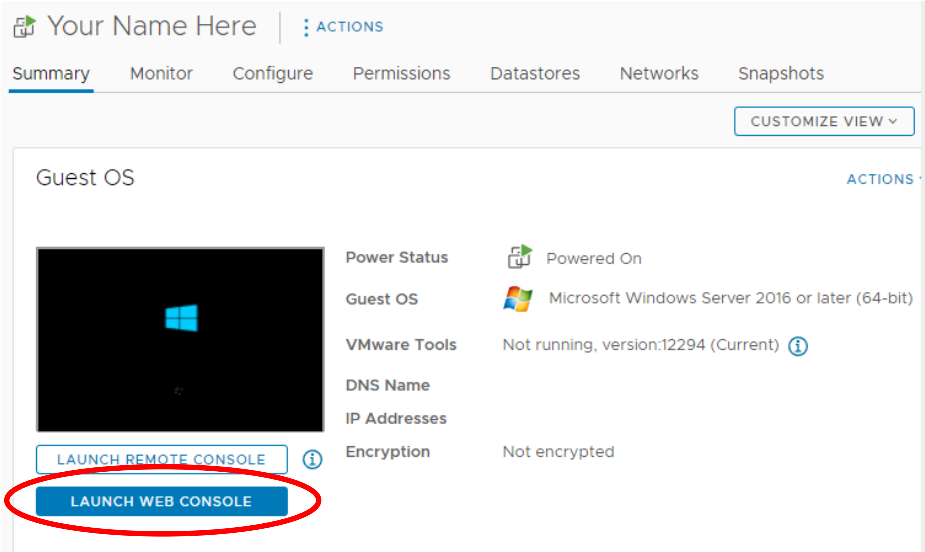
2) On the login page, you will enter your NetID and password.
3) Click **Login** to continue.

2. Review Security Policies Enforced by Default on a Domain Controller Server

1) Now we will power on the server and do some initial configuration.

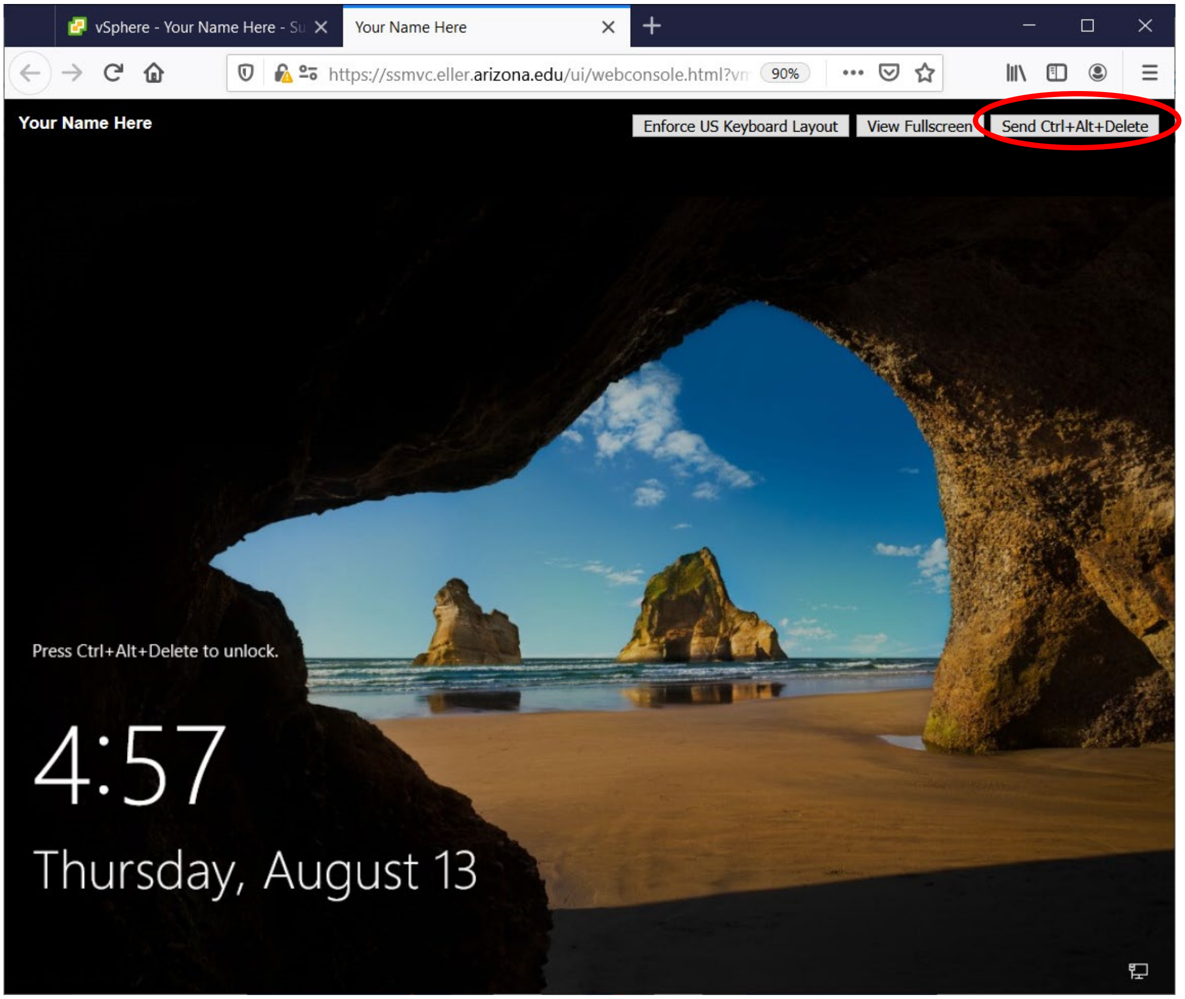


2) Click on the **name of your server**, then click on the **Actions** menu and choose **Power**, then **Power On** to boot up your server.



Power Status Powered On
Guest OS Microsoft Windows Server 2016 or later (64-bit)
VMware Tools Not running, version:12294 (Current)
DNS Name
IP Addresses
Encryption Not encrypted

3) As your server is powering up, click on the **Launch Web Console** link. This will open the server console window in a new browser tab.

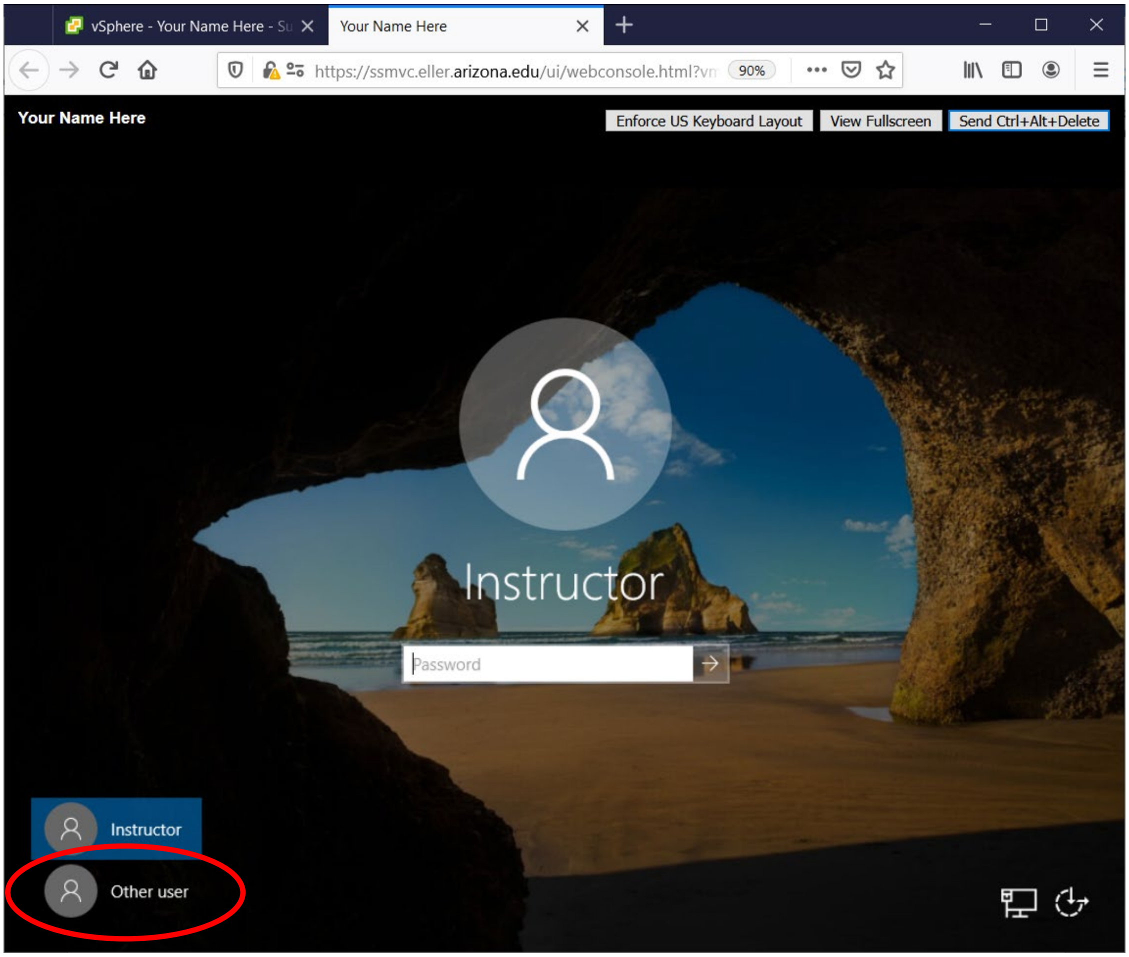

vSphere - Your Name Here - Su
Your Name Here
https://ssmvc.eller.arizona.edu/ui/webconsole.html?vm
90%
Your Name Here
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

Press Ctrl+Alt+Delete to unlock.

4:57

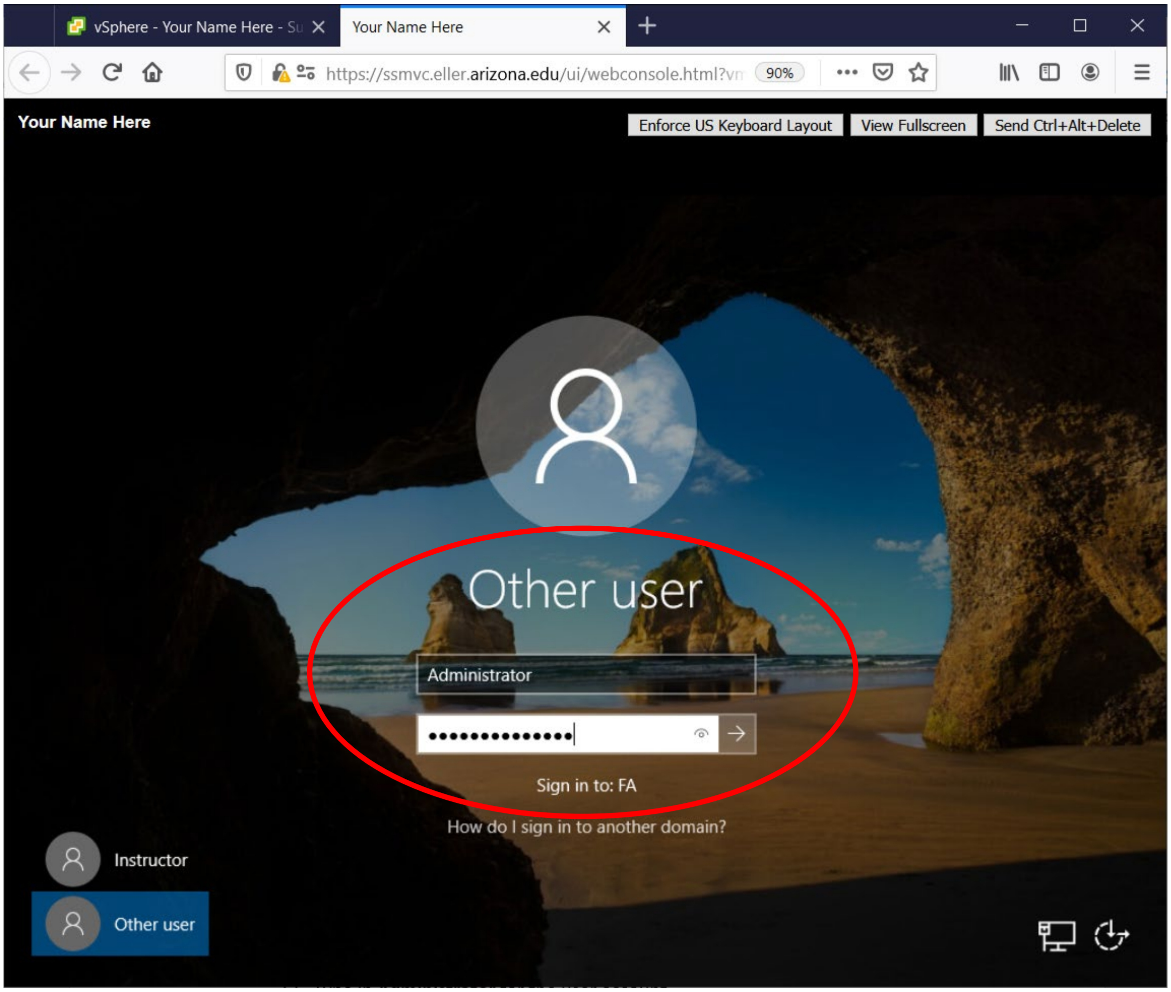
Thursday, August 13

4) You will now need to login to your server. Click on the **Send Ctrl+Alt+Delete** button in the upper right-hand portion of the browser window (highlighted above).

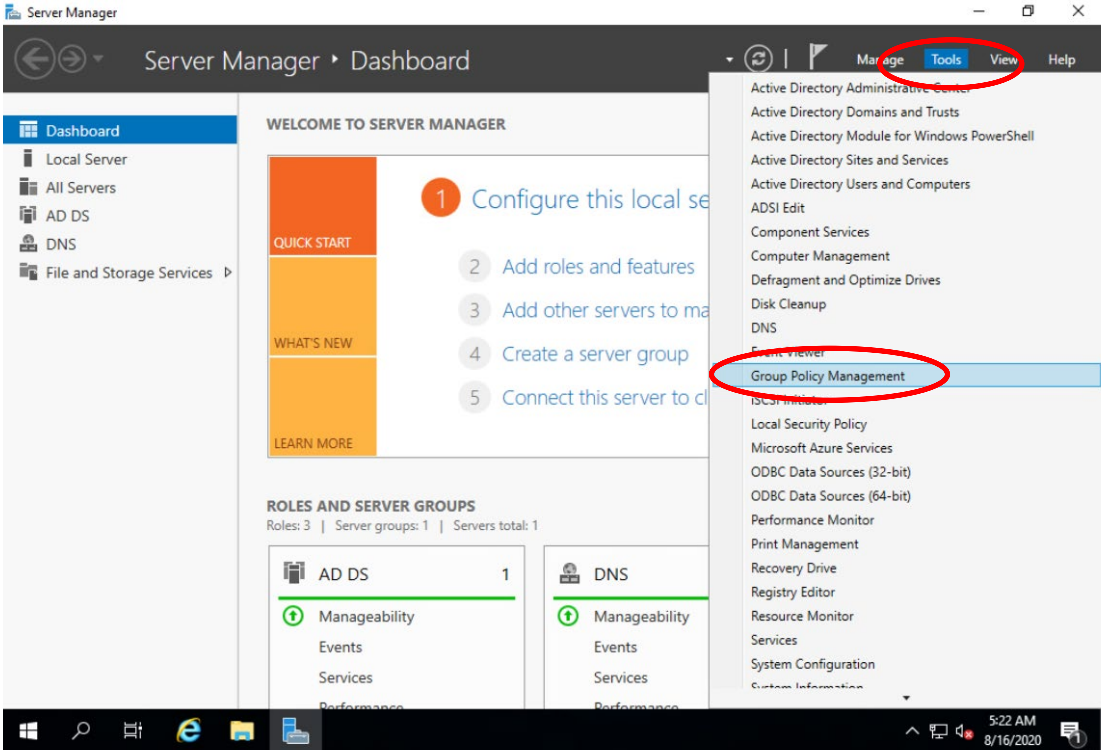

vSphere - Your Name Here - Su
Your Name Here
https://ssmvc.eller.arizona.edu/ui/webconsole.html?vn
90%
Your Name Here
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Instructor
Password
Instructor
Other user

5) If you see **Instructor** as the login name, you will need to switch over to the **Administrator** account.

6) Click on **Other User**.

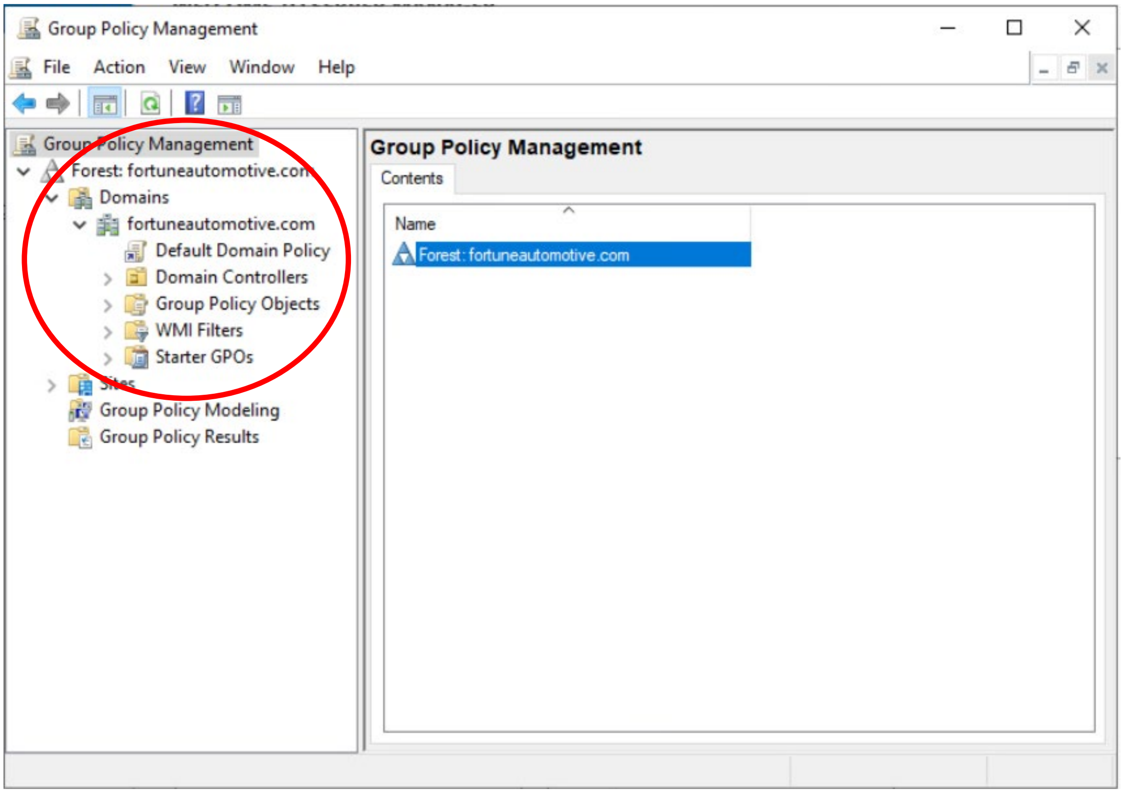

vSphere - Your Name Here - Su
Your Name Here
https://ssmvc.eller.arizona.edu/ui/webconsole.html?vn
90%
Your Name Here
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Other user
Administrator
Sign in to: FA
How do I sign in to another domain?
Instructor
Other user

7) Type in **Administrator** for the user account
8) Type in the **password** you created in lab 2 for this account (***if you cannot remember it, please contact your instructor to reset it for you***). Press the **Enter** key on your keyboard to continue.

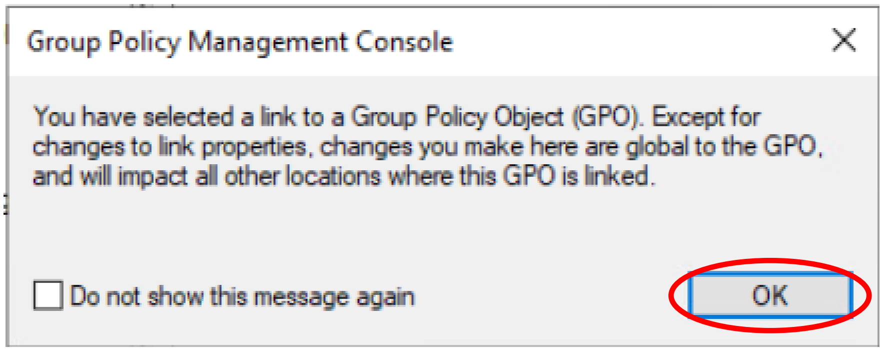


9) Once the login process finishes, the **Server Manager** should open automatically.

10) Click on the **Tools** Menu and select **Group Policy Management**.



11) Once Group Policy Management opens, **expand the options under Forest fortuneautomotive.com**. You will notice folders similar to the screenshot above. Note there is a shortcut to an object called **Default Domain Policy**. Because this policy is shown immediately under the domain name fortuneautomotive.com this indicates the policy is applied to all objects in the domain.

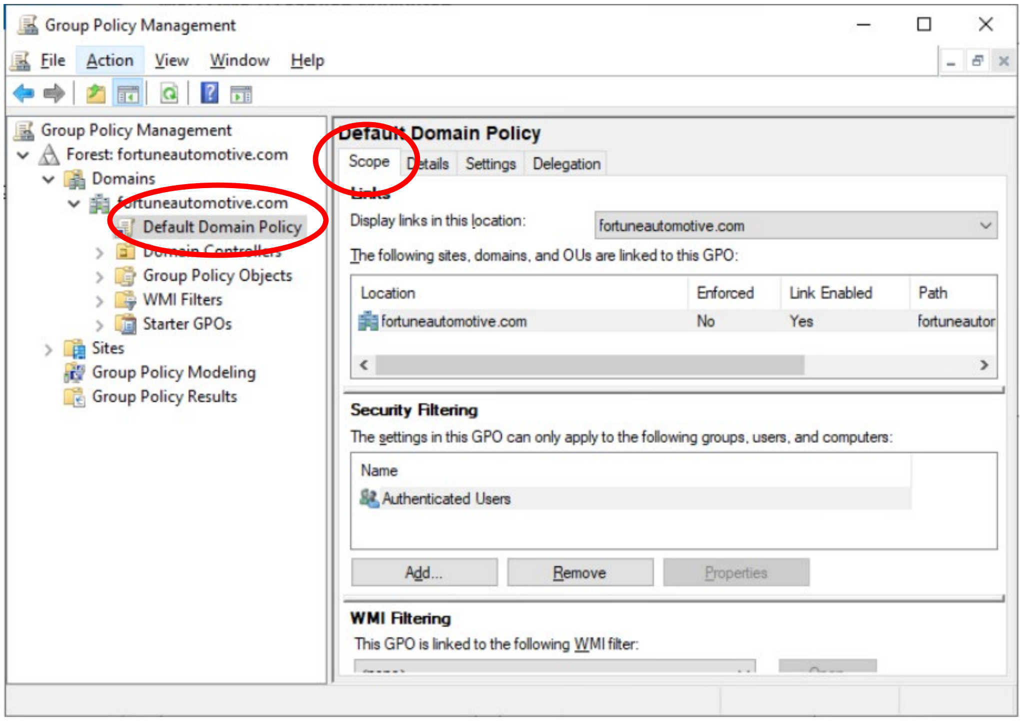


Group Policy Management Console

You have selected a link to a Group Policy Object (GPO). Except for changes to link properties, changes you make here are global to the GPO, and will impact all other locations where this GPO is linked.

☐ Do not show this message again

12) Click on the **Default Domain Policy**. This will immediately pop up a prompt that explains any changes you make to this specific policy will be applied everywhere the Group Policy Object (GPO) is linked in AD. Click **OK** to continue.



Default Domain Policy

Links

Display links in this location: fortuneautomotive.com

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

Location	Enforced	Link Enabled	Path
fortuneautomotive.com	No	Yes	fortuneautor

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

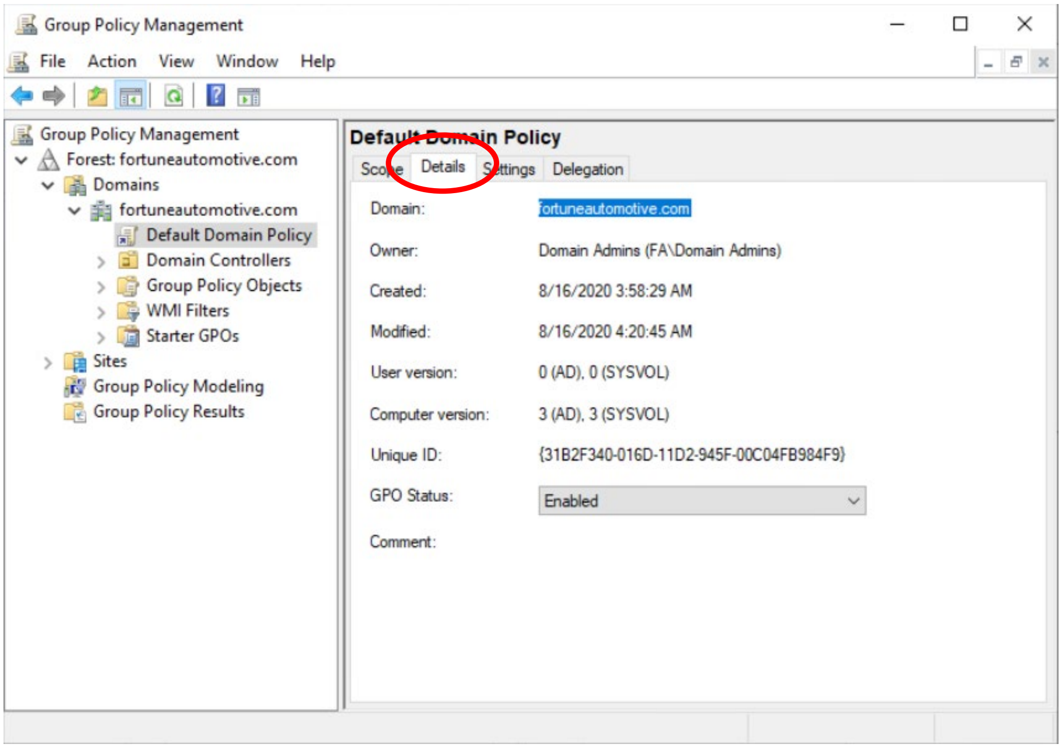
Name
Authenticated Users

WMI Filtering

This GPO is linked to the following WMI filter:

13) The **Scope** tab provides some initial information about this policy. This tab explains where the GPO is linked (as previously noted at the domain fortuneautomotive.com) and what security is applied to this GPO (in this case Authenticated Users). What this **security filter** means is the GPO settings will be

applied to any authenticated users in this domain, so all users should have these settings applied to their computers by default. You can further restrict this to specific Security Groups, so if you wanted a policy to only apply to Human Resources department, you would remove Authenticated Users and Add the security group you have for Human Resources. Once the settings are saved, this GPO would only be applied to HR users and not, for example, Sales users.



Domain: fortuneautomotive.com

Owner: Domain Admins (FA\Domain Admins)

Created: 8/16/2020 3:58:29 AM

Modified: 8/16/2020 4:20:45 AM

User version: 0 (AD), 0 (SYSVOL)

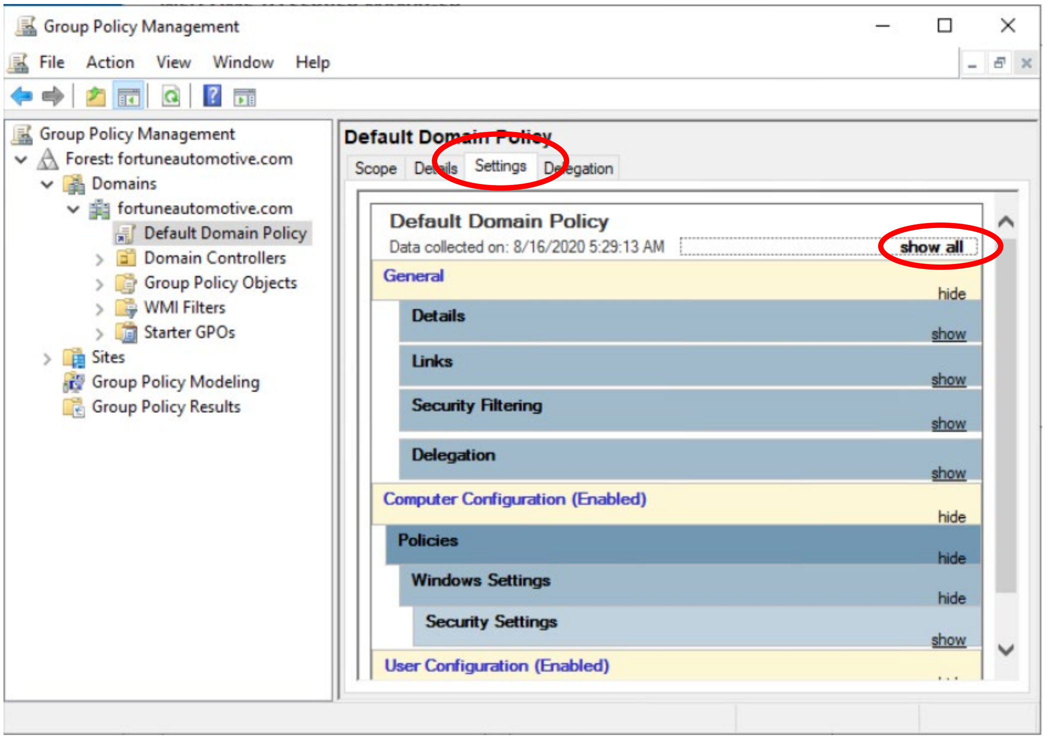
Computer version: 3 (AD), 3 (SYSVOL)

Unique ID: {31B2F340-016D-11D2-945F-00C04FB984F9}

GPO Status: Enabled

Comment:

14) The **Details** tab shows basic information about the domain. Note the GPO Status is set to Enabled. This means all policies contained within this GPO are applied and active. This can be set to Disabled (to prevent settings from being applied) or you can restrict the GPO to apply User or Computer settings only. For the purposes of this lab, leave this set to **Enabled**.



Default Domain Policy

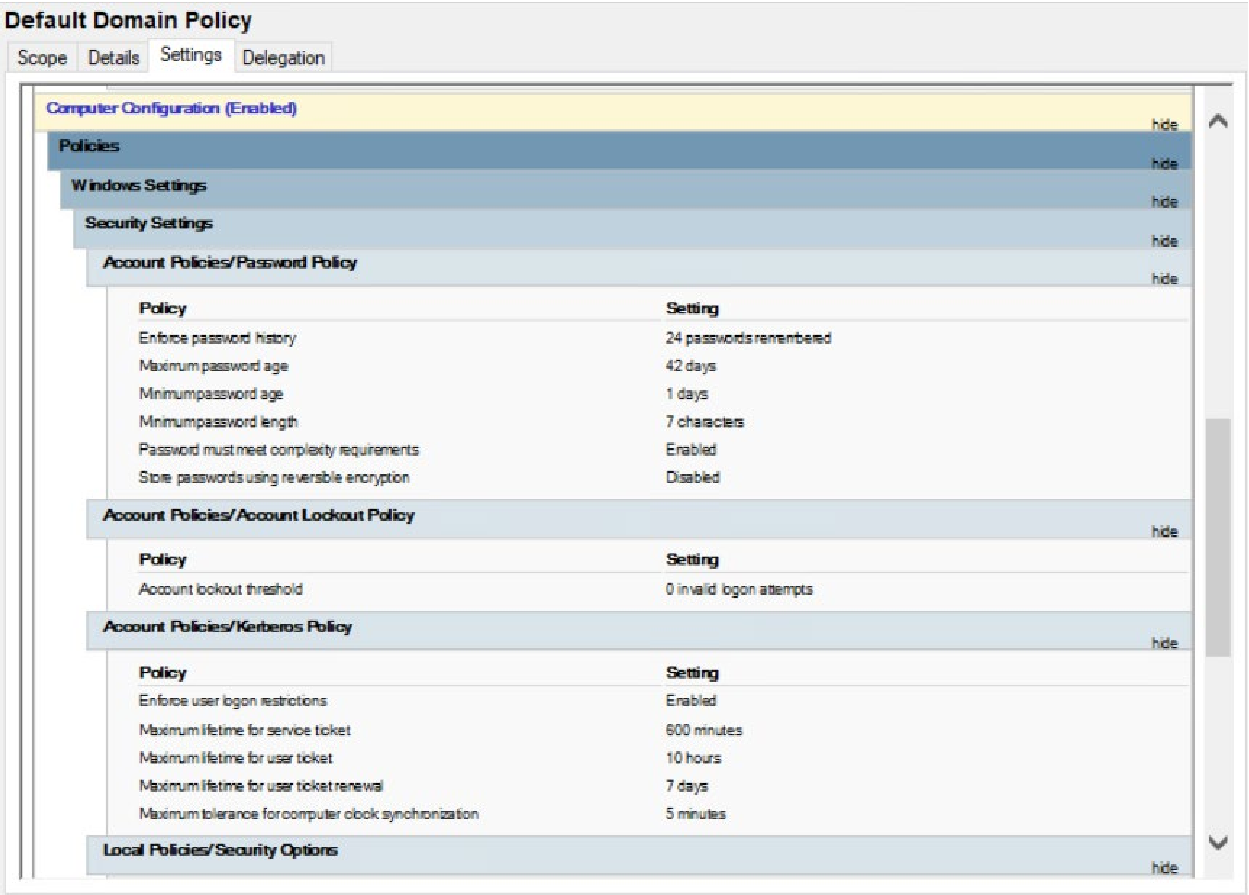
Data collected on: 8/16/2020 5:29:13 AM

General
- Details
- Links
- Security Filtering
- Delegation

Computer Configuration (Enabled)
- Policies
  - Windows Settings
    - Security Settings

User Configuration (Enabled)

15) The **Settings** tab will show you the policies that are included in this specific GPO. Let's look at this in more detail. Click on the **Show All** option in the upper right side of this window.



Default Domain Policy

Computer Configuration (Enabled) hide

Policies hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy hide

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy hide

Policy	Setting
Account lockout threshold	0 invalid logon attempts

Account Policies/Kerberos Policy hide

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

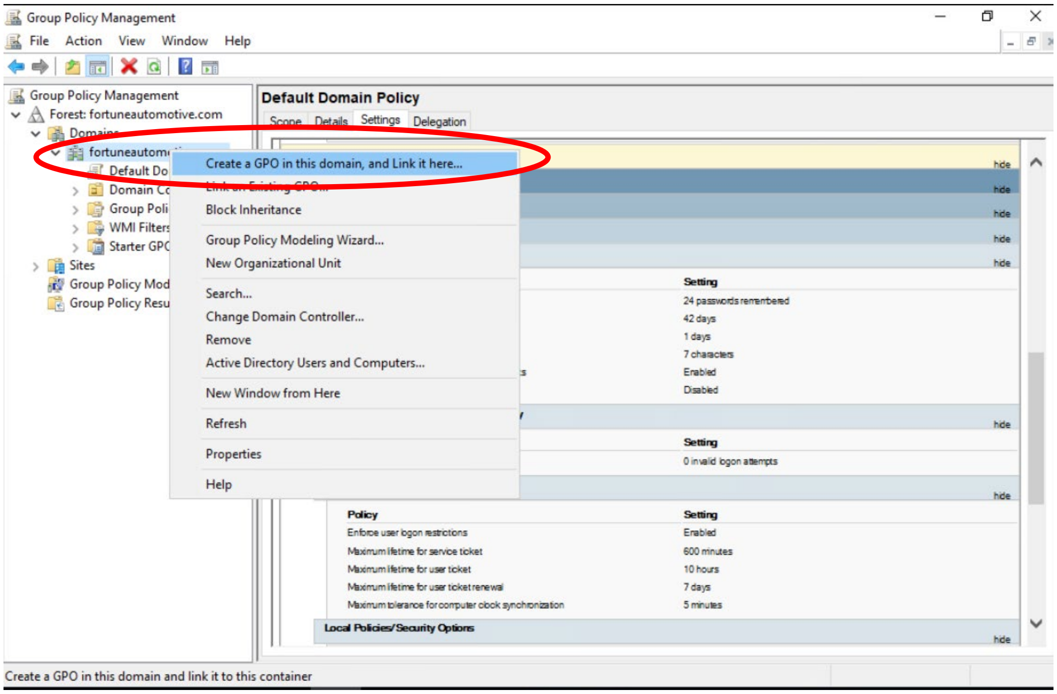
Local Policies/Security Options hide

16) You will see the page now has a scroll bar. Looking at this immediately you can see some security settings enabled by default. These policies include **Password Policy, Account Lockout Policy, Kerberos Policy, Security Options, and others**. Take a look at these settings and think about what security levels they provide.

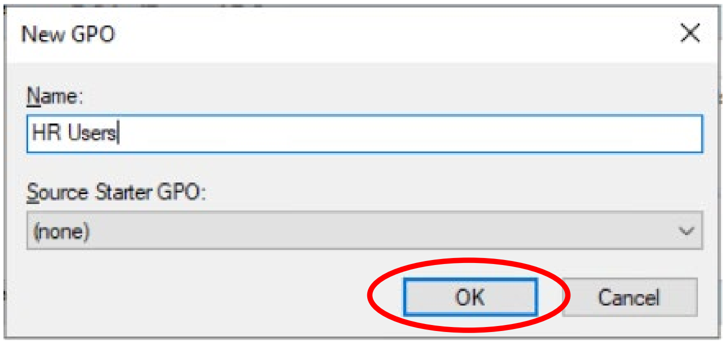
17) While these are the default policies, they can be changed or overwritten. You will find different organizations will change these in different ways based on the security policies the company decided to implement. For example, some organizations may change the **Account Lockout Policy** from **0 attempts** (meaning accounts will not be locked after a bad password is entered) to **3 attempts** (giving users 3 chances to login before the account is locked out for a period of time).

3. Create a New Group Policy with Some Common Security Settings

1) Now that you have seen what a GPO looks like, let's create one of our own.


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: fortuneautomotive.com
Domains
fortuneautomotive.com
Default Do
Domain Co
Group Poli
WMI Filters
Starter GPC
Sites
Group Policy Mod
Group Policy Resu
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Active Directory Users and Computers...
New Window from Here
Refresh
Properties
Help
Default Domain Policy
Scope Details Settings Delegation
Setting
24 passwords remembered
42 days
1 days
7 characters
Enabled
Disabled
Setting
0 invalid logon attempts
Policy
Setting
Enforce user logon restrictions
Enabled
Maximum lifetime for service ticket
600 minutes
Maximum lifetime for user ticket
10 hours
Maximum lifetime for user ticket renewal
7 days
Maximum tolerance for computer clock synchronization
5 minutes
Local Policies/Security Options
hide
Create a GPO in this domain and link it to this container

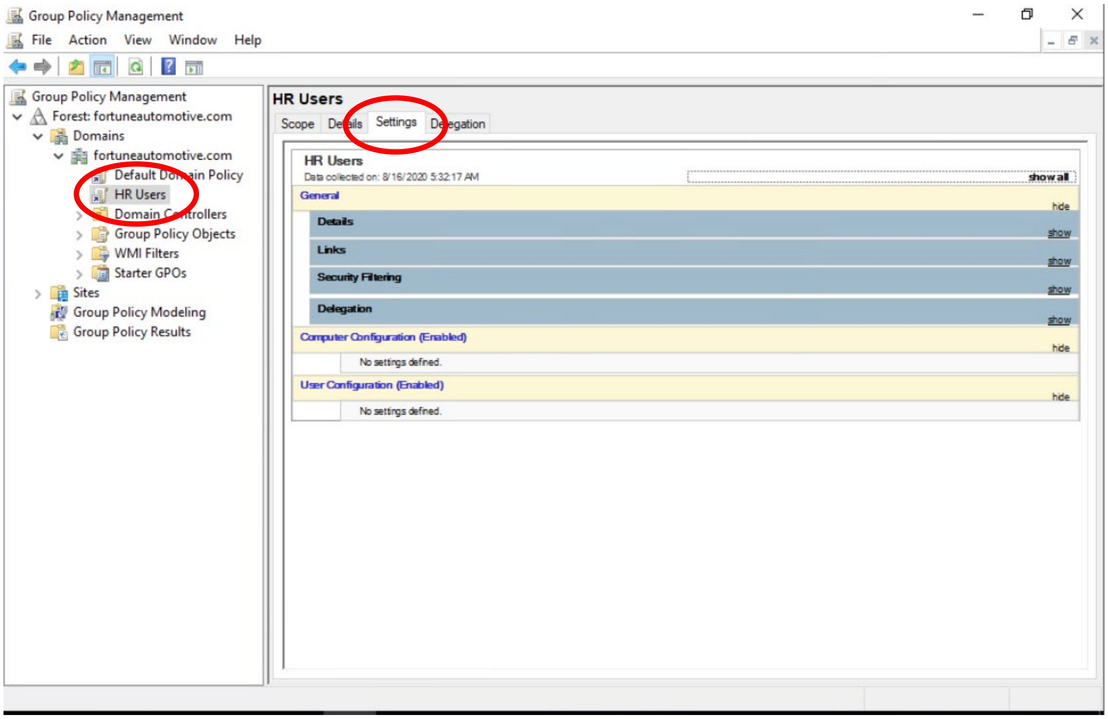
2) Right click on the **fortuneautomotive.com** domain and choose **Create a GPO in this domain, and Link it here…**



Name: HR Users

Source Starter GPO: (none)

3) In the **New GPO** window, give the GPO a name of **HR Users**. Leave **Source State GPO** to **(none)** and click **OK**.



HR Users

Data collected on: 8/16/2020 5:32:17 AM

General

Details

Links

Security Filtering

Delegation

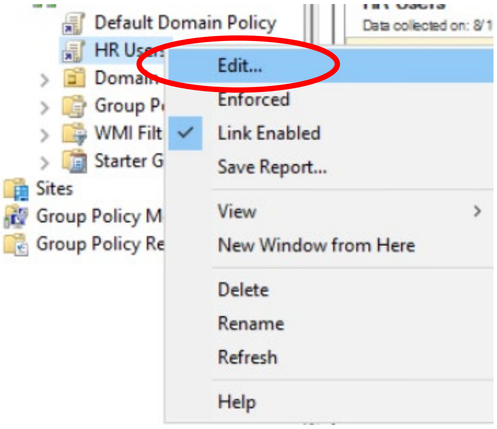
Computer Configuration (Enabled)

No settings defined.

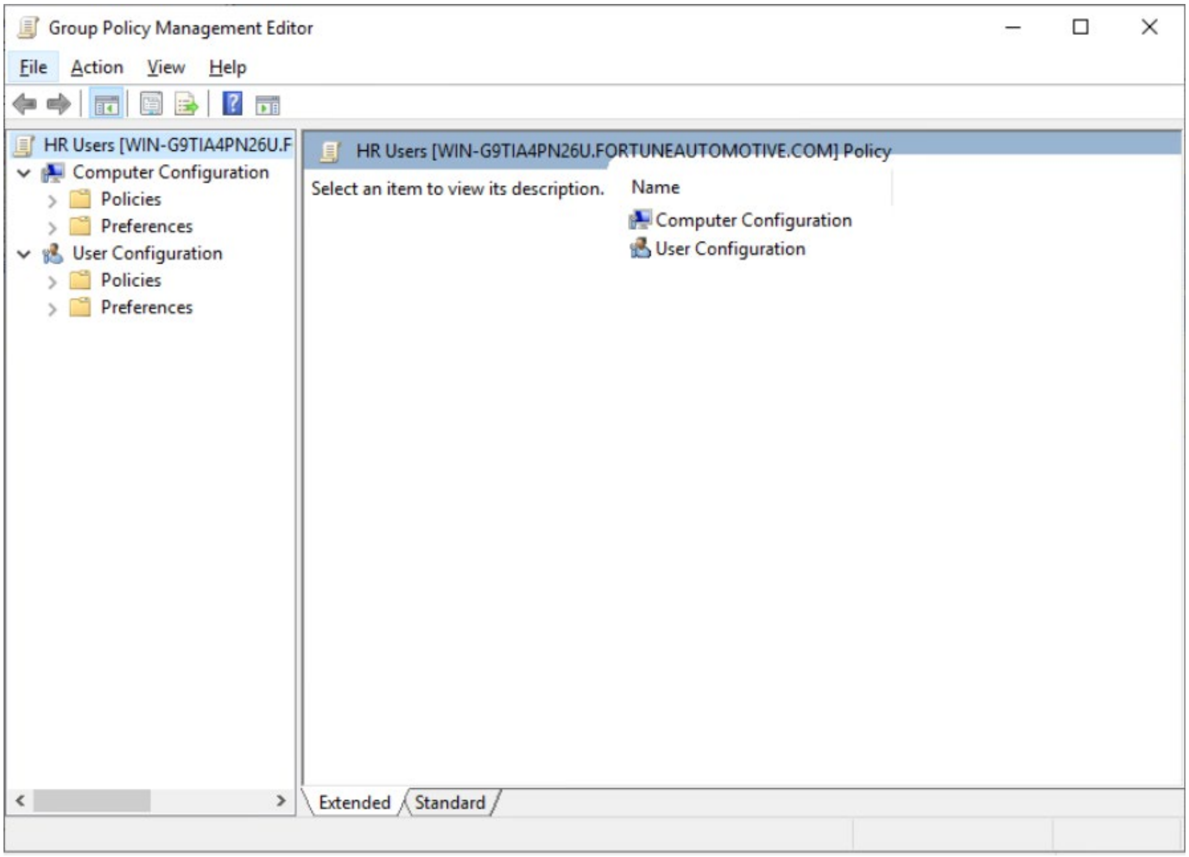
User Configuration (Enabled)

No settings defined.

4) Click on the **HR Users** GPO that you just created. If necessary, click on the **Settings** tab. You will see that no settings have been created in this GPO yet.

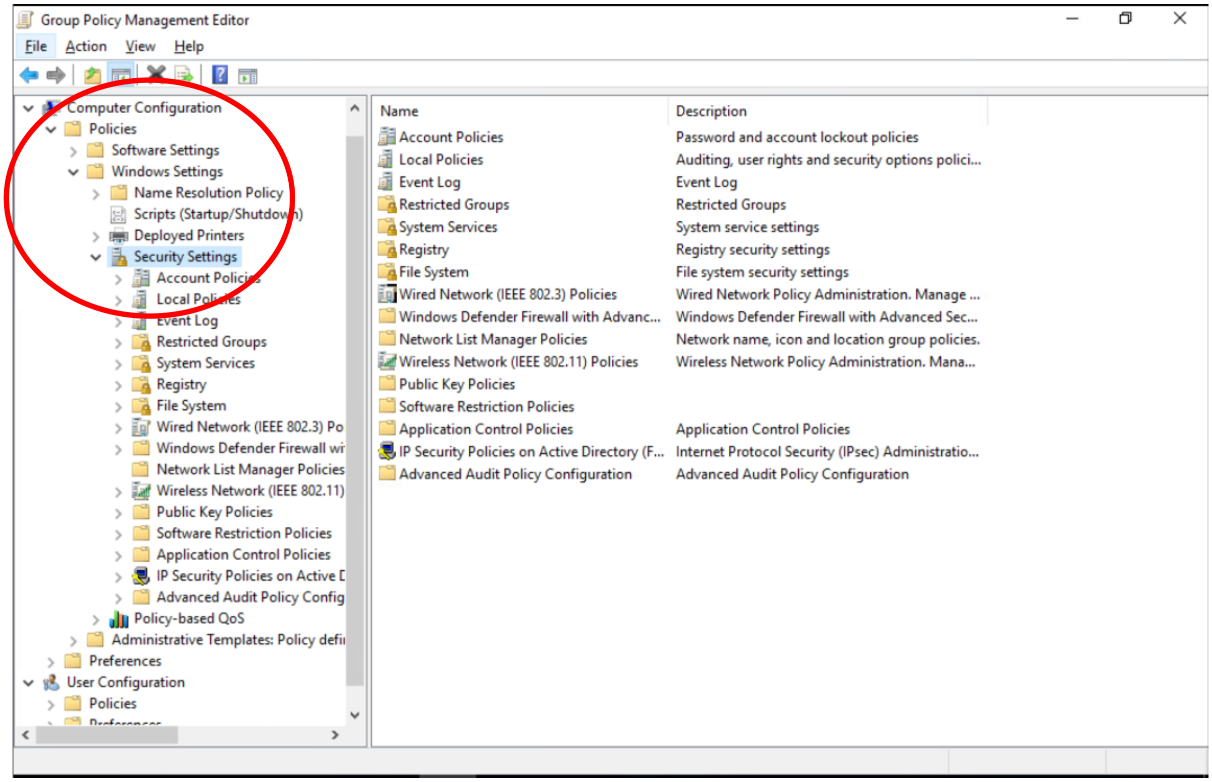


5) Right click on **HR Users** and select **Edit…** from the menu.



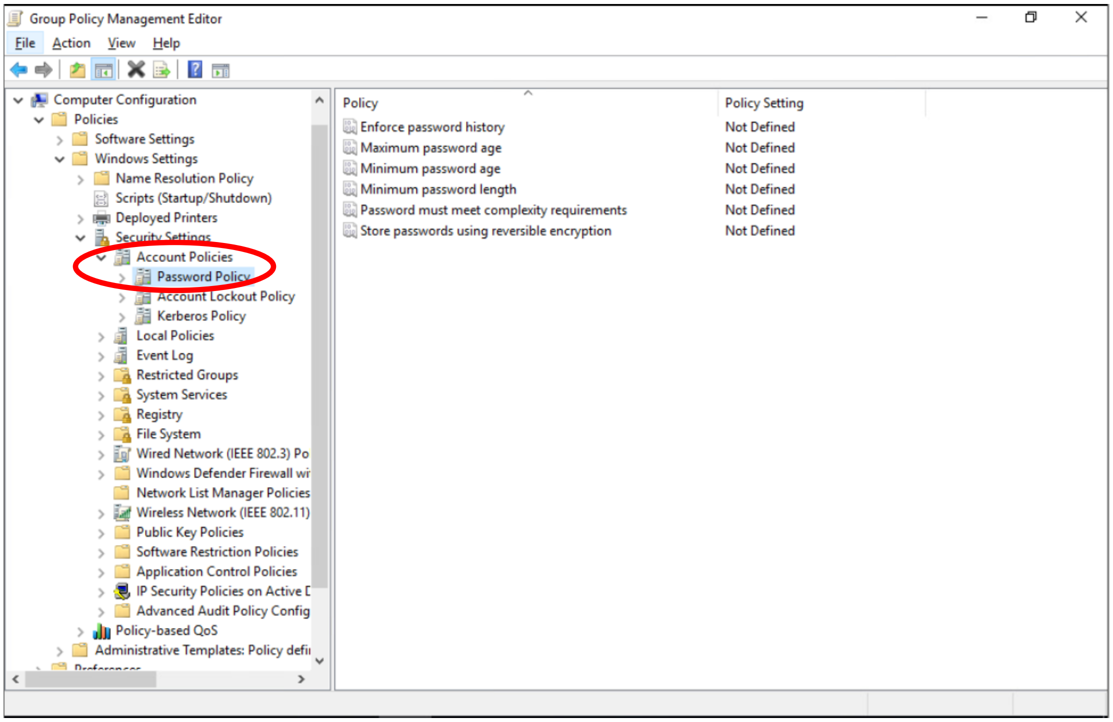
6) You will now see the Group Policy Management Editor window appear. On the left-side of the screen you will see Computer Configuration and User Configuration.

   a. Computer Configuration will allow you to select group policies that will apply only to Computer objects in AD. Computer policies will be applied to a computer at boot time. User Configuration will allow you to select group policies that will apply only to User objects in AD. User policies will be applies to users when they log in.
   b. The types of policies in each are different and serve different purposes. You can have both types of policies in a single GPO. For this lab we will look at both policy types.


Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Po
Windows Defender Firewall wi
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active D
Advanced Audit Policy Config
Policy-based QoS
Administrative Templates: Policy defi
Preferences
User Configuration
Policies
Preferences

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Event Log	Event Log
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File system security settings
Wired Network (IEEE 802.3) Policies	Wired Network Policy Administration. Manage ...
Windows Defender Firewall with Advanc...	Windows Defender Firewall with Advanced Sec...
Network List Manager Policies	Network name, icon and location group policies.
Wireless Network (IEEE 802.11) Policies	Wireless Network Policy Administration. Mana...
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Active Directory (F...	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

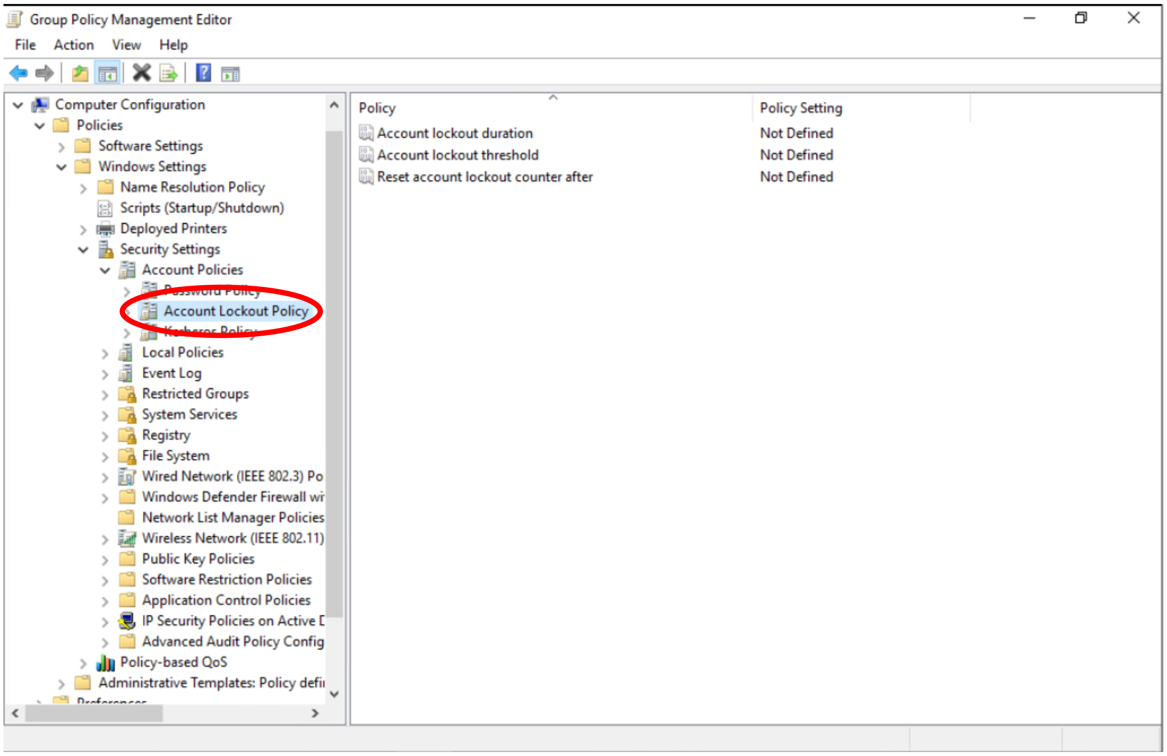
7) Expand the Policies folder under Computer Configuration until you get to Security Settings. Highlight **Security Settings** and you will see over a dozen sections where security policies can be defined.


Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Po
Windows Defender Firewall wi
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active D
Advanced Audit Policy Config
Policy-based QoS
Administrative Templates: Policy defi
Preferences

Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	Not Defined
Password must meet complexity requirements	Not Defined
Store passwords using reversible encryption	Not Defined

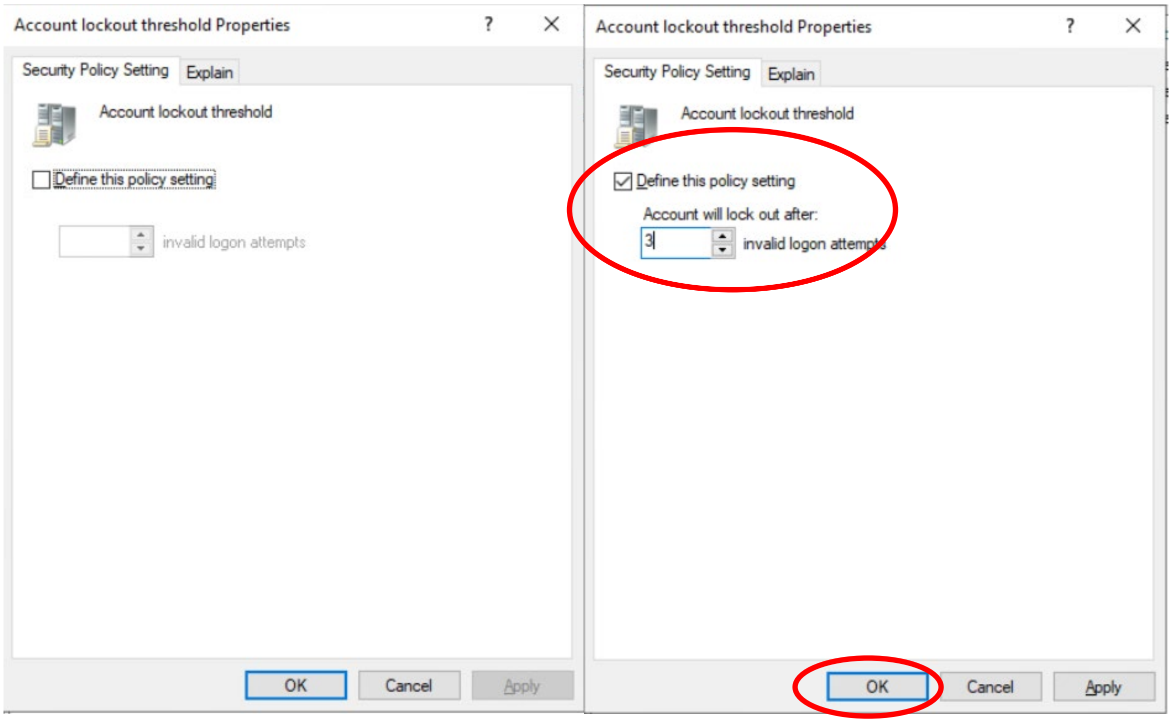
8) Expand **Account Policies** in the left-hand side of the window and highlight **Password Policy** so you can see the options.

9) The possible Password policies should look familiar because they were included in the Default Domain Policy.


Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Po
Windows Defender Firewall wi
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active D
Advanced Audit Policy Config
Policy-based QoS
Administrative Templates: Policy defi
Preferences

Policy	Policy Setting
Account lockout duration	Not Defined
Account lockout threshold	Not Defined
Reset account lockout counter after	Not Defined

10) Now highlight the **Account Lockout Policy** in the left-hand side window. In the Default Domain Policy, the only setting enabled was the Account Lockout Threshold. Double click on the Account Lockout Threshold policy.



Account lockout threshold Properties

Security Policy Setting | Explain

Account lockout threshold

□ Define this policy setting

invalid logon attempts

Account lockout threshold Properties

Security Policy Setting | Explain

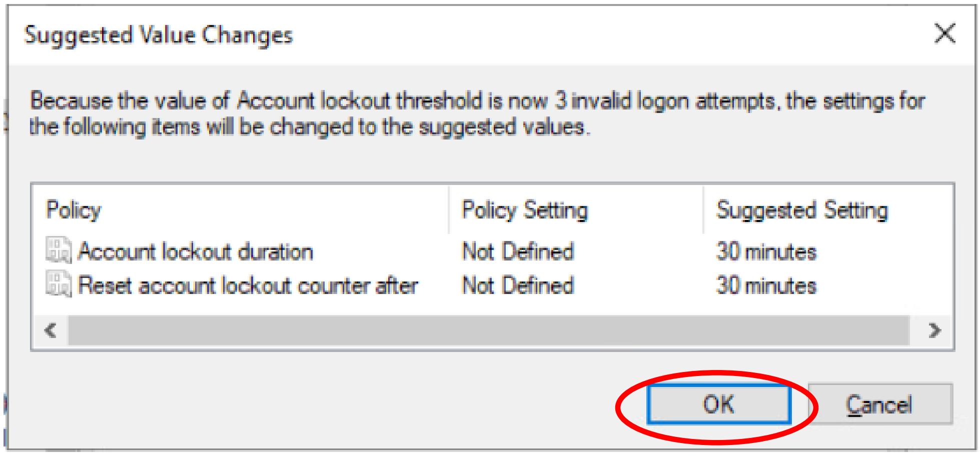
Account lockout threshold

☑ Define this policy setting

Account will lock out after:

3 invalid logon attempts

11) This will open a properties window so you can change the threshold settings. Since this setting is not defined in your policy, it will appear the same as the screenshot on the left. Check the box to **Define this policy setting** and change the number from 0 to **3 for invalid logon attempts**. Click OK to save this setting and close the Properties window.



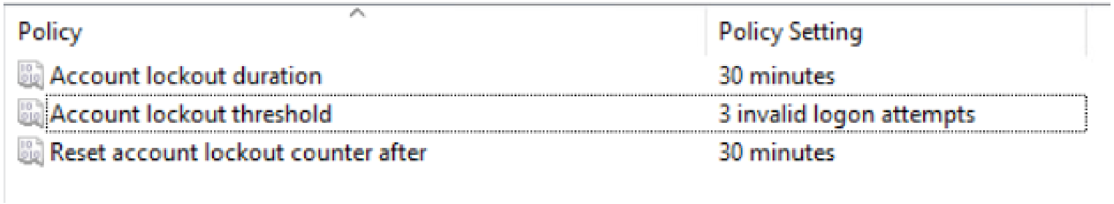
Suggested Value Changes

Because the value of Account lockout threshold is now 3 invalid logon attempts, the settings for the following items will be changed to the suggested values.

Policy	Policy Setting	Suggested Setting
Account lockout duration	Not Defined	30 minutes
Reset account lockout counter after	Not Defined	30 minutes

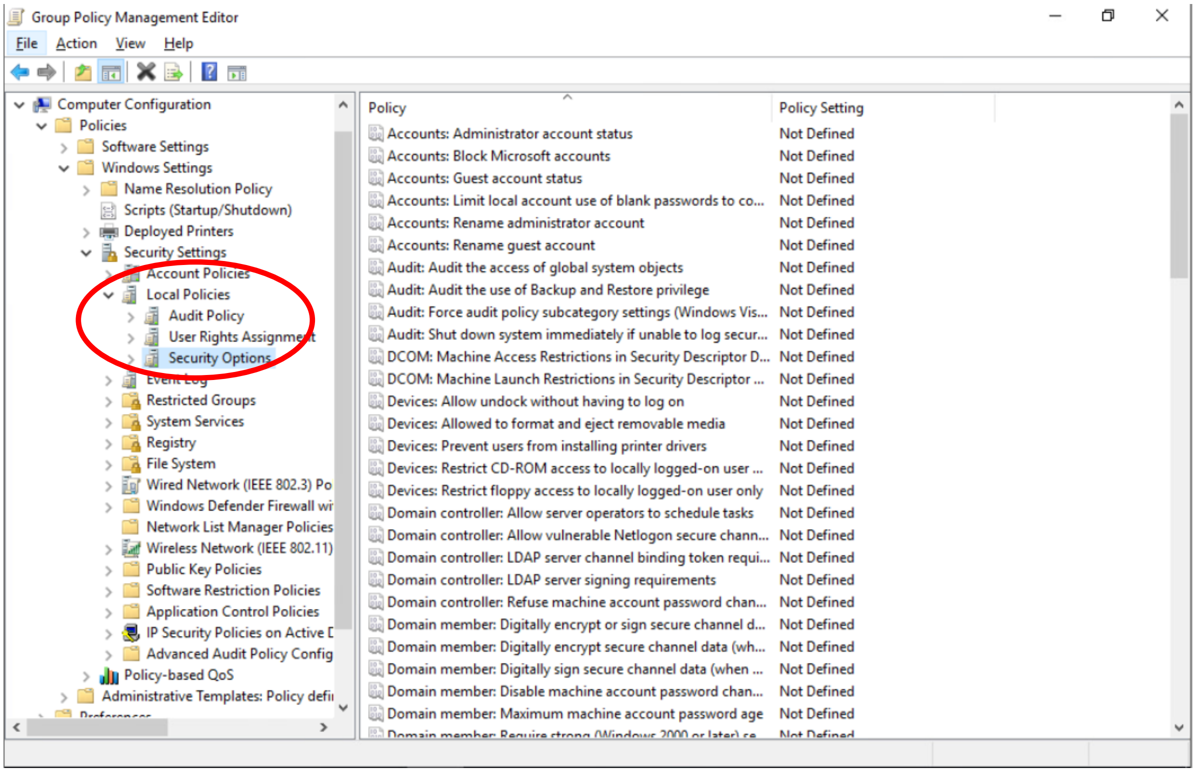
12) You will now be immediately presented with a pop-up window with Suggested Value Changes. You will notice the other two policies listed with their current policy setting and what the GPO would recommend for the settings to be changed to. If you do not make these changes, then once an account is locked out after 3 bad logon attempts, the account would remain locked out until an

Administrator re-enabled the account for the user. With the suggested setting of 30 minutes, this would mean the account would remain locked out for 30 minutes and would reset the lockout counter after the 30 minutes had passed. Click **OK** to continue.



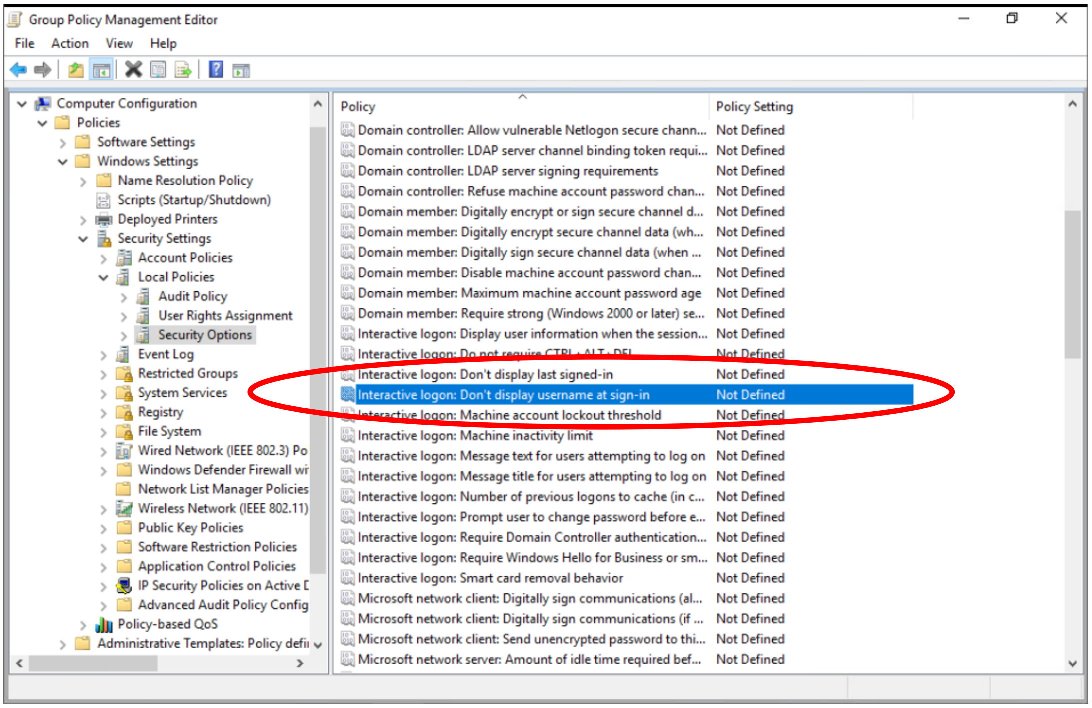
Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

13) Notice that all three policies have now been enabled with the settings above.


Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Po
Windows Defender Firewall wi
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active D
Advanced Audit Policy Config
Policy-based QoS
Administrative Templates: Policy defi
Preferences

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Not Defined
Domain member: Digitally encrypt secure channel data (wh...	Not Defined
Domain member: Digitally sign secure channel data (when ...	Not Defined
Domain member: Disable machine account password chan...	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) se...	Not Defined

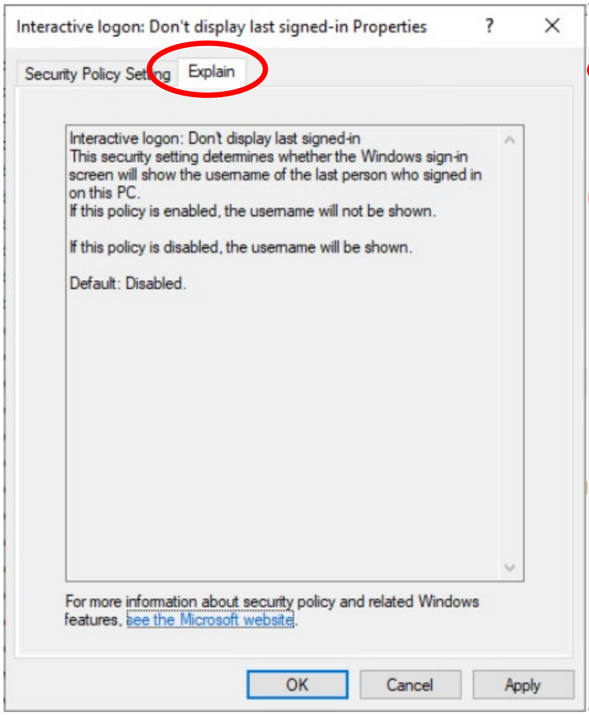
14) In the left-hand side of the window, expand the **Local Policies** section and highlight **Security Options**.



- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Po
        - Windows Defender Firewall wi
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11)
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Active D
        - Advanced Audit Policy Config
      - Policy-based QoS
    - Administrative Templates: Policy defi

Policy	Policy Setting
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Not Defined
Domain member: Digitally encrypt secure channel data (wh...	Not Defined
Domain member: Digitally sign secure channel data (when ...	Not Defined
Domain member: Disable machine account password chan...	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) se...	Not Defined
Interactive logon: Display user information when the session...	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Don't display last signed-in	Not Defined
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in c...	Not Defined
Interactive logon: Prompt user to change password before e...	Not Defined
Interactive logon: Require Domain Controller authentication...	Not Defined
Interactive logon: Require Windows Hello for Business or sm...	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (al...	Not Defined
Microsoft network client: Digitally sign communications (if ...	Not Defined
Microsoft network client: Send unencrypted password to thi...	Not Defined
Microsoft network server: Amount of idle time required bef...	Not Defined

1) You will notice there are lots of policy options to choose from. Let's pick three easy ones to see the results of. Start by double clicking on the **Interactive logon: Don't display last signed-in** policy.

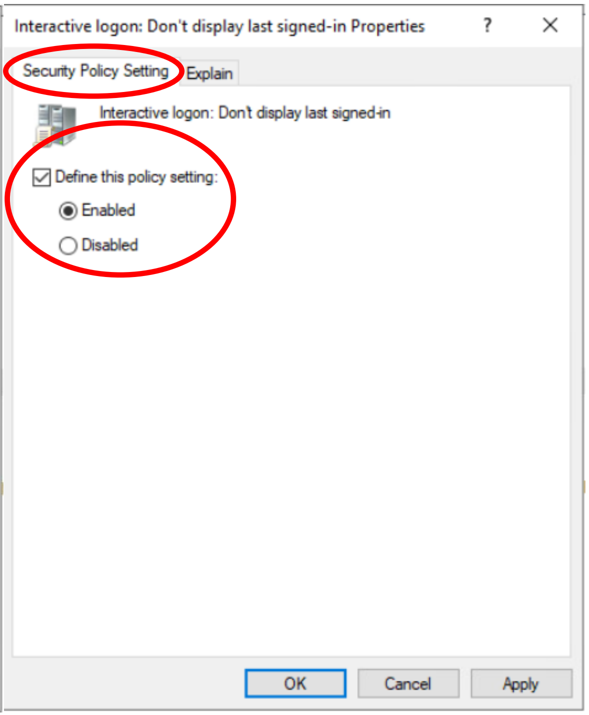


Interactive logon: Dont display last signed-in
This security setting determines whether the Windows sign-in screen will show the username of the last person who signed in on this PC.
If this policy is enabled, the username will not be shown.

If this policy is disabled, the username will be shown.

Default: Disabled.

For more information about security policy and related Windows features, see the Microsoft website.



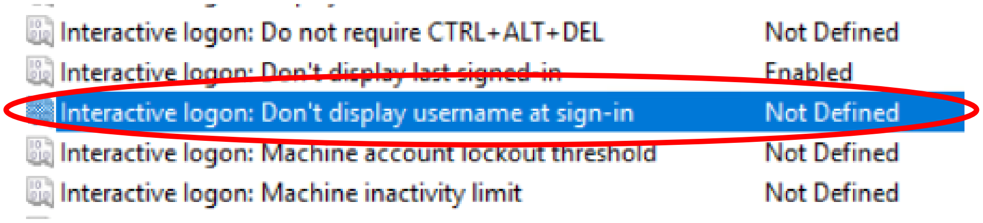
Interactive logon: Dont display last signed-in

☑ Define this policy setting:

● Enabled

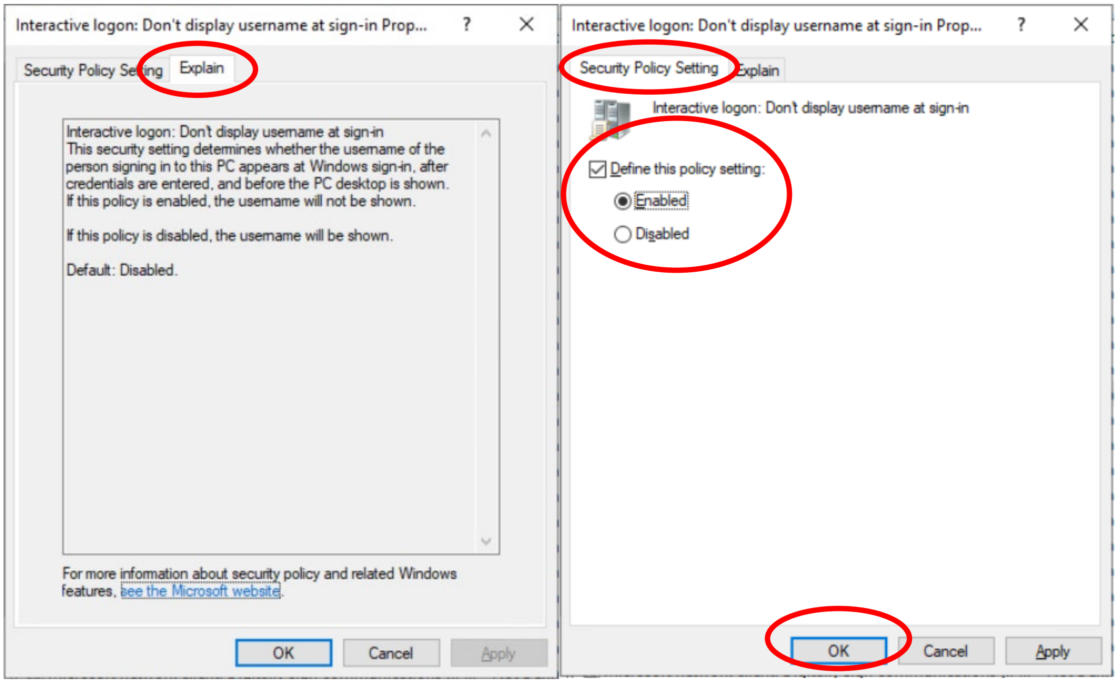
○ Disabled

2) Click on the **Explain** tab to learn more about this policy. Once you have finished reading the policy information, click on the **Security Policy Setting** tab, check the box to **Define this policy setting**, and choose **Enabled**. Click **OK** when finished.



Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Don't display last signed-in	Enabled
Interactive logon: Don't display username at sign-in	Not Defined
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined

3) Now double click on the Interactive logon: **Don't display username at sign-in**.



Interactive logon: Don't display username at sign-in Prop...

Interactive logon: Dont display username at sign-in
This security setting determines whether the username of the person signing in to this PC appears at Windows sign-in, after credentials are entered, and before the PC desktop is shown.
If this policy is enabled, the username will not be shown.

If this policy is disabled, the username will be shown.

Default: Disabled.

For more information about security policy and related Windows features, see the Microsoft website.

Interactive logon: Don't display username at sign-in Prop...

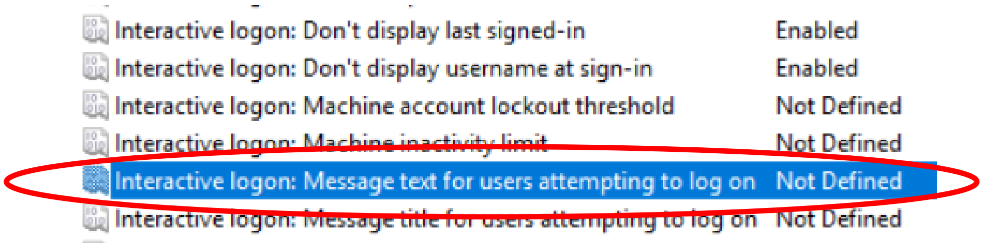
Interactive logon: Dont display username at sign-in

☑ Define this policy setting:

● Enabled

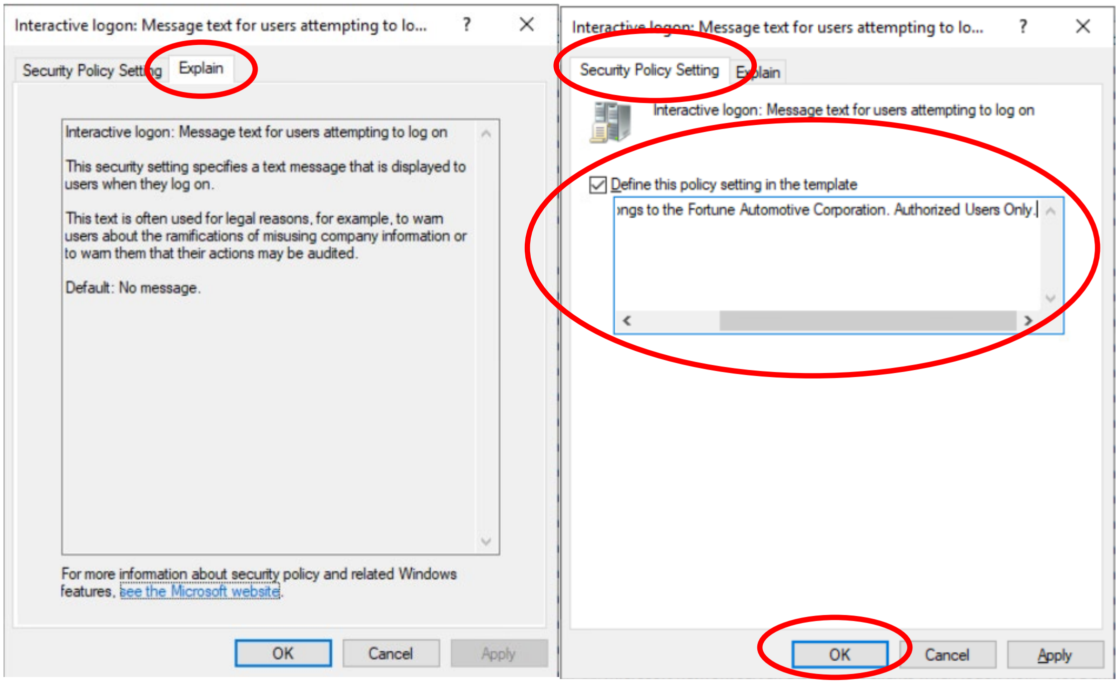
○ Disabled

4) Click on the **Explain** tab to learn more about this policy. Once you have finished reading the policy information, click on the **Security Policy Setting** tab, check the box to **Define this policy setting**, and choose **Enabled**. Click **OK** when finished.



Interactive logon: Don't display last signed-in	Enabled
Interactive logon: Don't display username at sign-in	Enabled
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined

5) Now double click on the Interactive logon: **Message text for users attempting to log on**.



Interactive logon: Message text for users attempting to lo...

Interactive logon: Message text for users attempting to log on

This security setting specifies a text message that is displayed to users when they log on.

This text is often used for legal reasons, for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.

Default: No message.

For more information about security policy and related Windows features, see the Microsoft website.

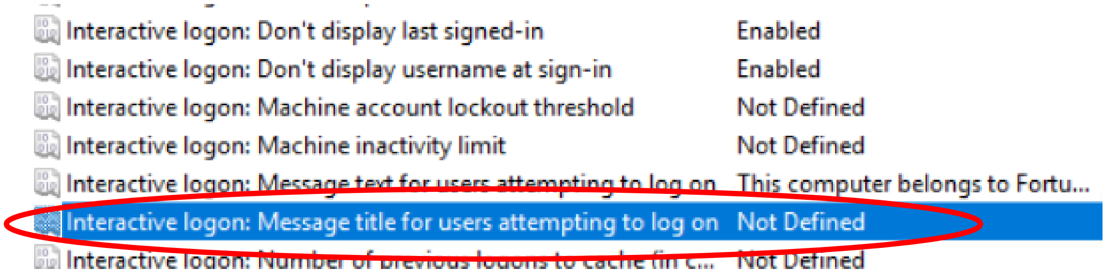
Interactive logon: Message text for users attempting to lo...

Interactive logon: Message text for users attempting to log on

☑ Define this policy setting in the template

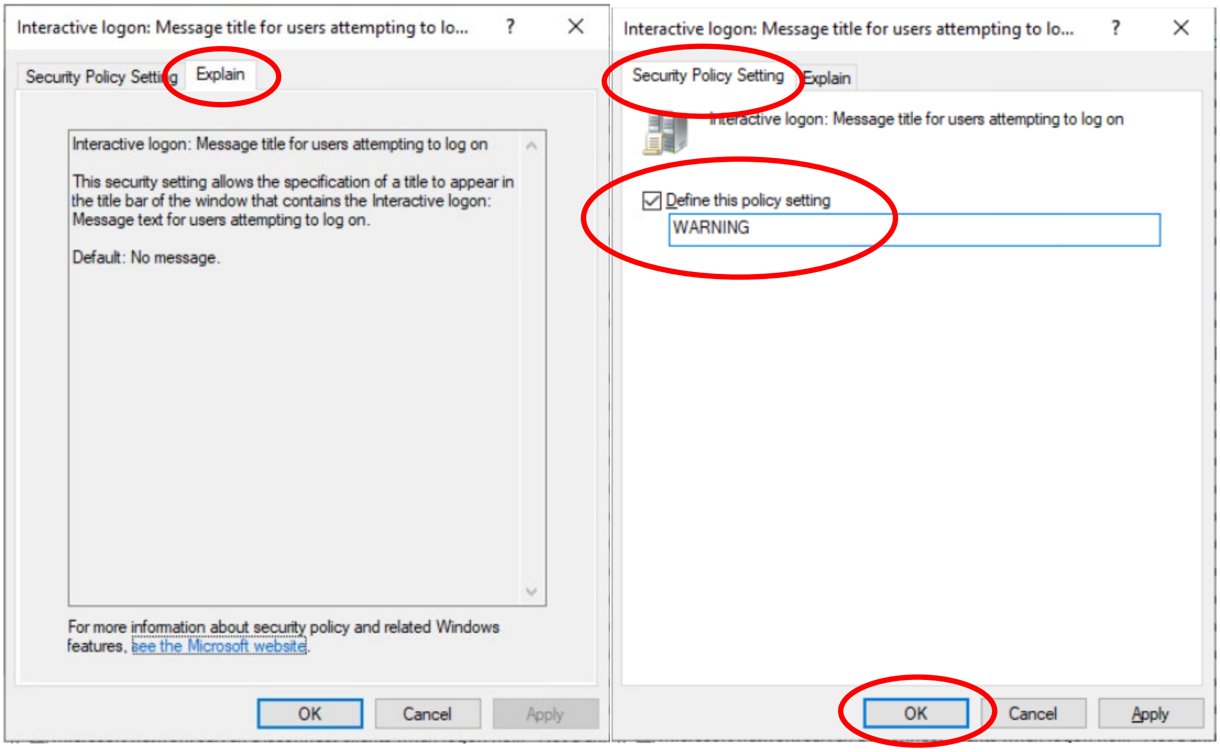
ngs to the Fortune Automotive Corporation. Authorized Users Only.

6) Click on the **Explain** tab to learn more about this policy. Once you have finished reading the policy information, click on the **Security Policy Setting** tab, check the box to **Define this policy setting in the template** and type the following message in the box: ***This computer belongs to the Fortune Automotive Corporation. Authorized Users only***. Click **OK** to save this policy setting.



Interactive logon: Don't display last signed-in	Enabled
Interactive logon: Don't display username at sign-in	Enabled
Interactive logon: Machine account lockout threshold	Not Defined
Interactive logon: Machine inactivity limit	Not Defined
Interactive logon: Message text for users attempting to log on	This computer belongs to Fortu...
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in c...	Not Defined

7) Now for the final setting. Double click on the policy setting for **Interactive logon: Message title for users attempting to log on**.



Interactive logon: Message title for users attempting to lo...
?
Security Policy Setting
Explain
OK
Cancel
Apply

Interactive logon: Message title for users attempting to log on

This security setting allows the specification of a title to appear in the title bar of the window that contains the Interactive logon: Message text for users attempting to log on.

Default: No message.

For more information about security policy and related Windows features, see the Microsoft website.

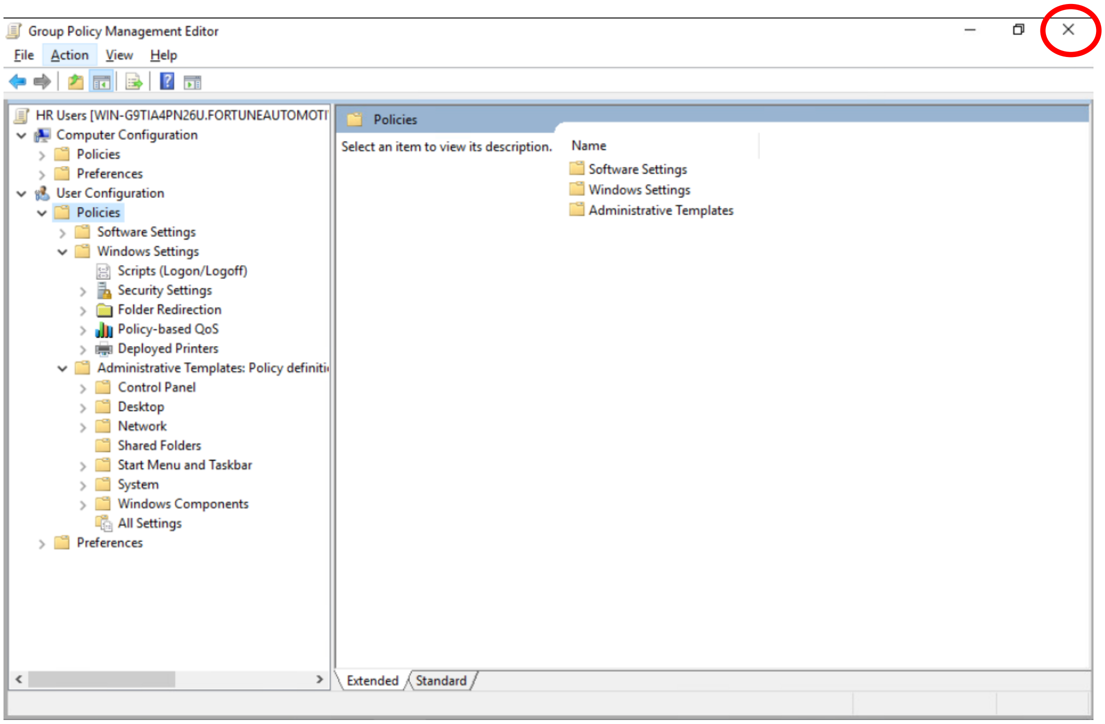
Interactive logon: Message title for users attempting to log on

☑ Define this policy setting

WARNING

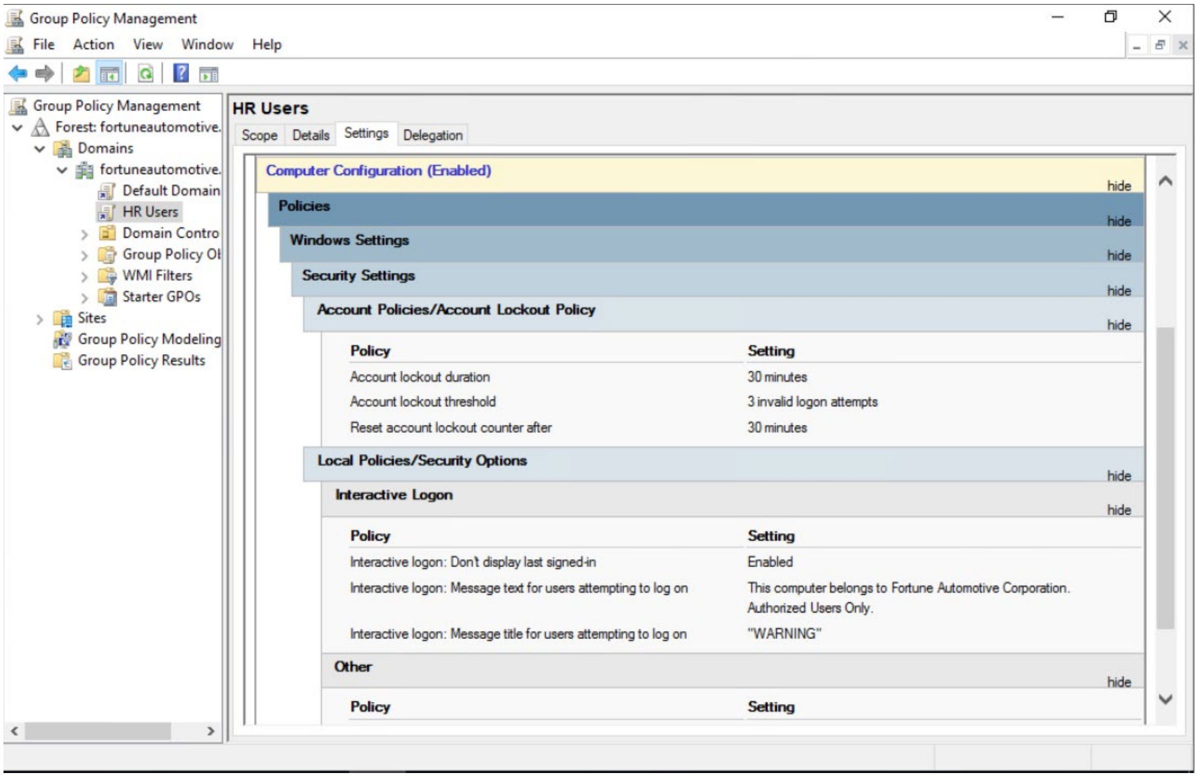
8) Click on the **Explain** tab to learn more about this policy. Once you have finished reading the policy information, click on the **Security Policy Setting** tab, check the box to **Define this policy setting** and type the following message in the box: ***WARNING***. Click **OK** to save this policy setting.

9) With these three policies set you are accomplishing two things. The first policy makes it so the last user who logged on to this computer will not appear automatically when you press CTRL+ALT+DEL to logon. This prevents someone from knowing what you user account naming convention is and what a valid user account will be. This is half of the information needed to breach a system. The second and third policies will immediately present the user with a disclaimer when they attempt to log on. Note that in the real world, these messages should be crafted by an organization's legal and HR departments.



10) Take some time to look around the Computer Configuration settings and possible User Configuration settings. You will notice there are few security-related policies in User Configuration. This is because most of the User-based policies are designed to control the look and feel of the Windows desktop operating systems. Most organizations use these settings to create a standardized desktop for all users. The reason for this is so a user can move from one computer to another and always have the same experience. Feel free to open a few policies and read about what they do. We will not be enabling any of these settings in this lab.

11) Once you have finished looking at the possible settings, you can close the Group Policy Management Editor window by clicking on the **X** in the upper-right corner.



HR Users

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

Local Policies/Security Options

Interactive Logon

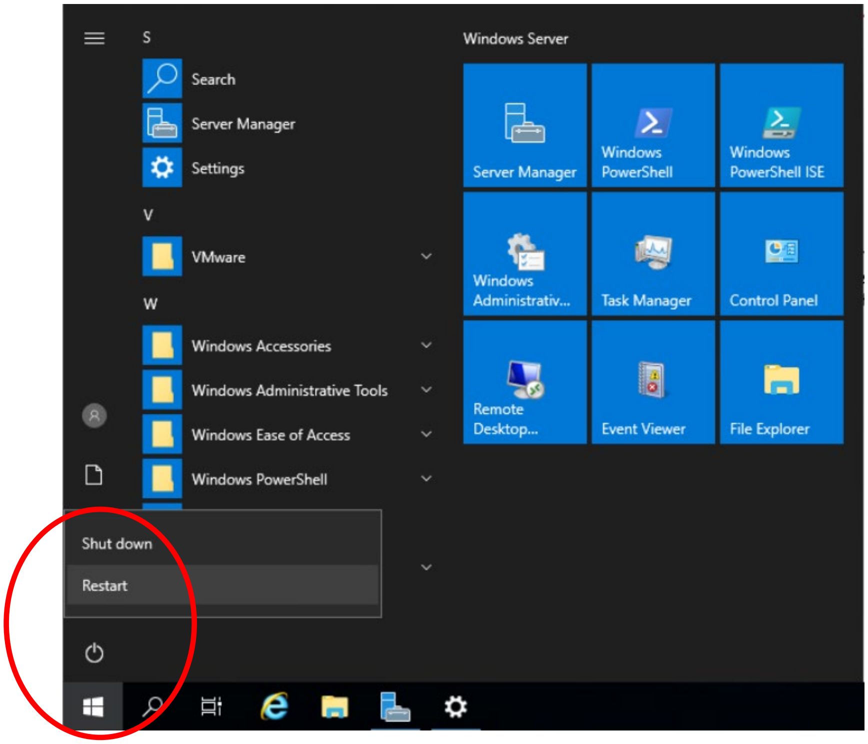
Policy	Setting
Interactive logon: Don't display last signed-in	Enabled
Interactive logon: Message text for users attempting to log on	This computer belongs to Fortune Automotive Corporation. Authorized Users Only.
Interactive logon: Message title for users attempting to log on	"WARNING"

Other

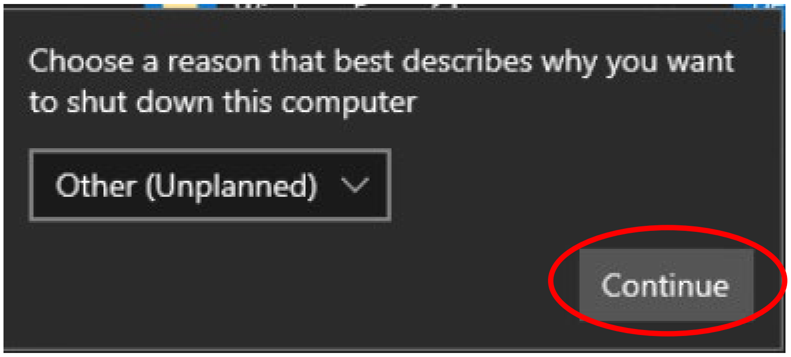
Policy	Setting

12) To see the settings you just created, you need to refresh the window. If you hit **F5**, it will eventually refresh (you will get a few error messages before it does. Otherwise, just click on the **Default Domain Policy** in the left-hand side of the window, then click back on **HR Users**. Click on the **Show All** option in the upper right corner to see the policies you just created.

4. Reboot Your Server to See Effect of Settings



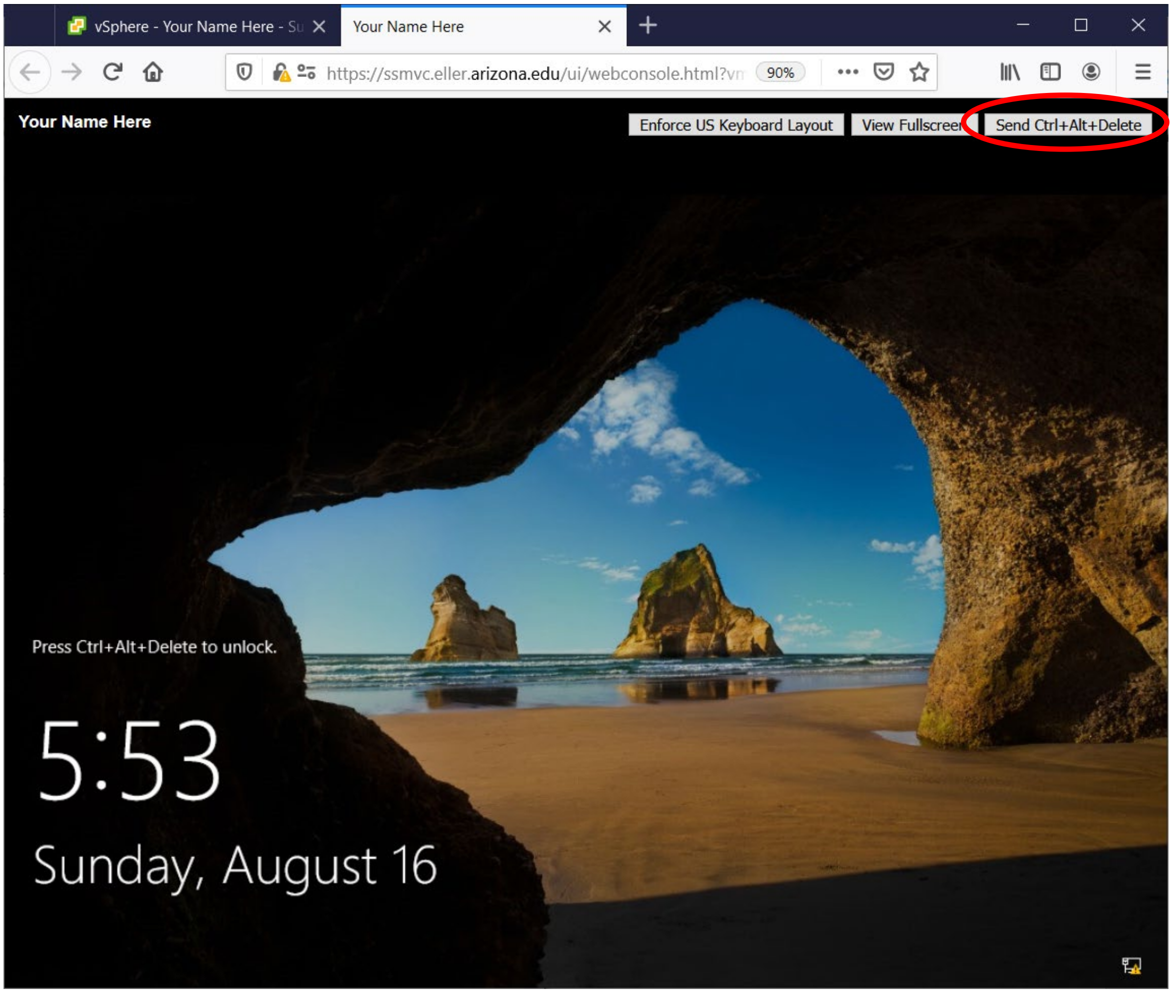
1) Now to see the changes, you should reboot the server.
   a. Click on the **Start** button in the lower left corner.
   b. Click on the **power** button and choose **Restart**.



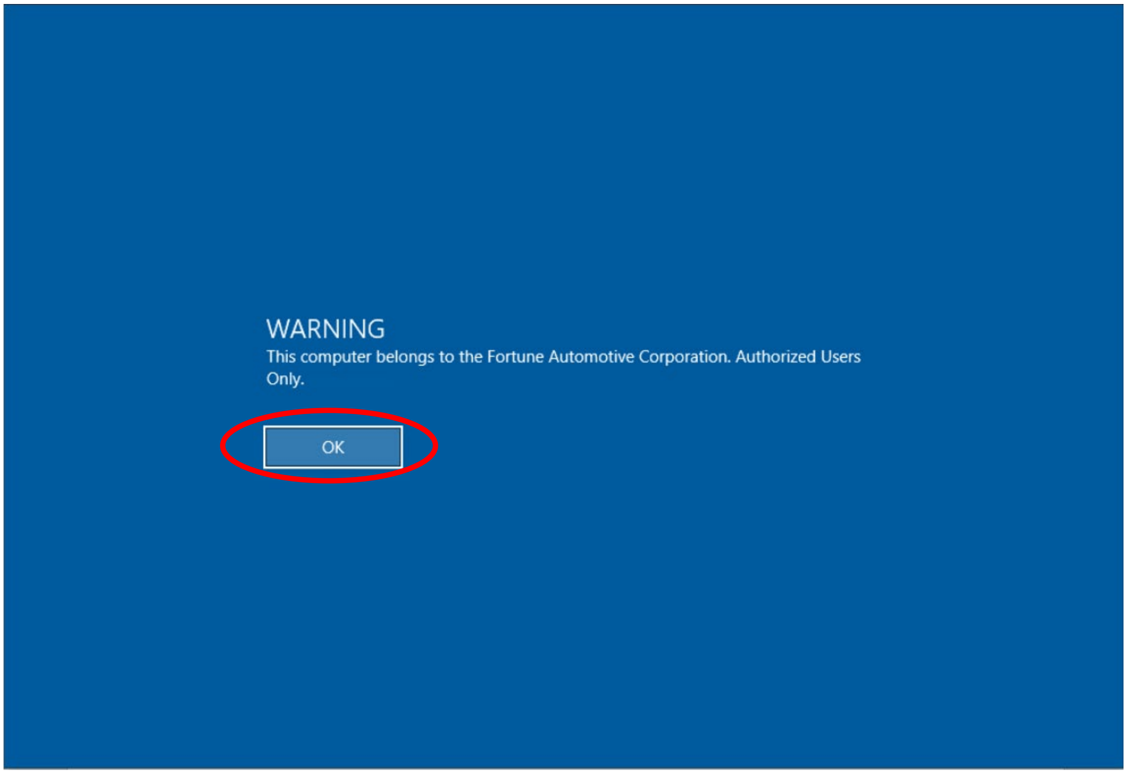
Choose a reason that best describes why you want to shut down this computer

Other (Unplanned)

2) Choose any reason from the list and click **Continue** to restart the server.

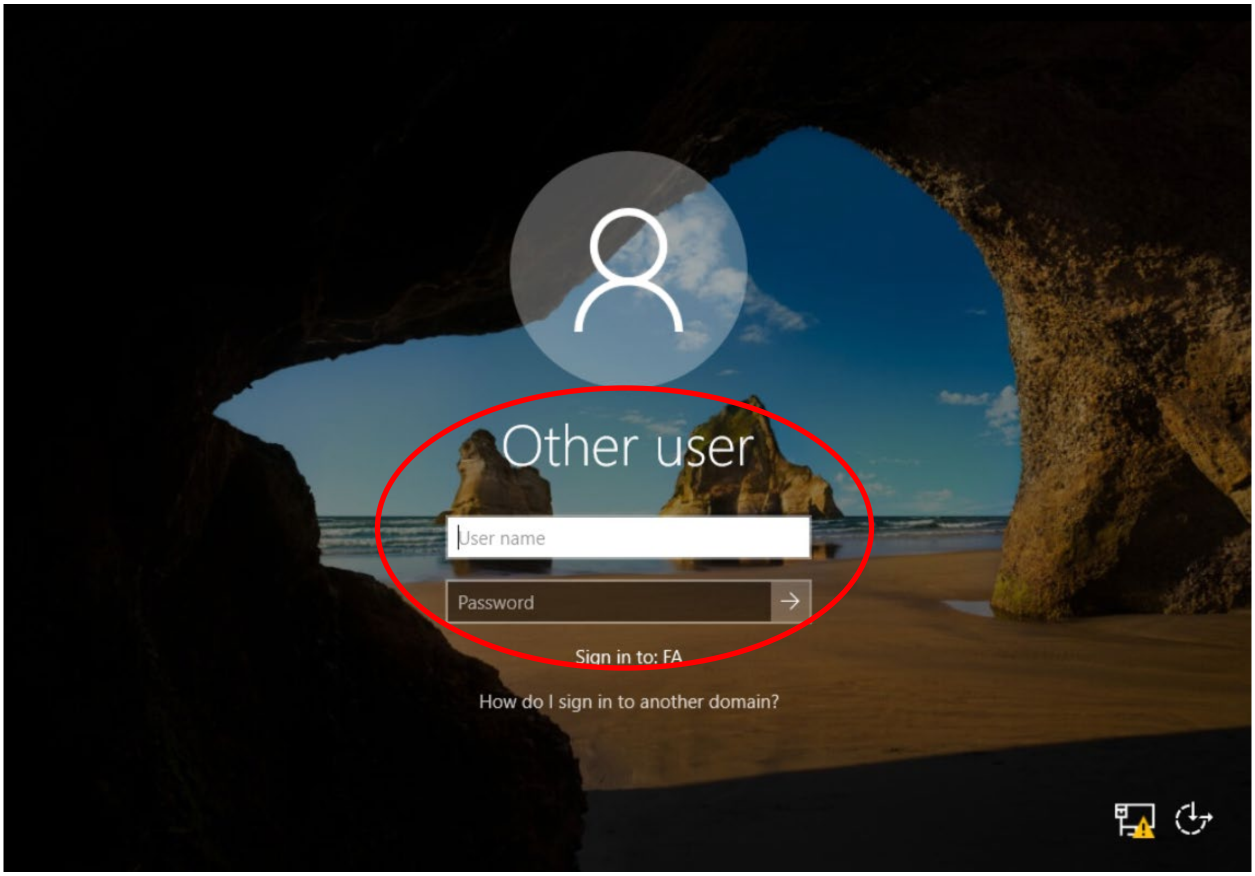

vSphere - Your Name Here - Su
Your Name Here
https://ssmvc.eller.arizona.edu/ui/webconsole.html?vn
90%
Your Name Here
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Press Ctrl+Alt+Delete to unlock.
5:53
Sunday, August 16

3) When the server boots back up, click on the **Send Ctrl+Alt+Delete** button in the upper right-hand portion of the browser window (highlighted above).

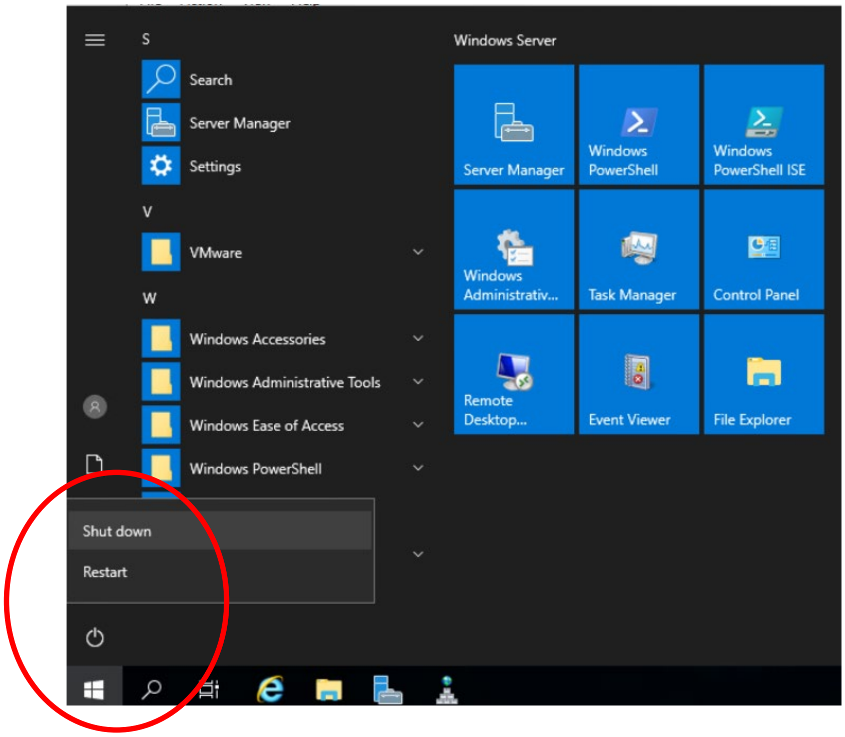


WARNING
This computer belongs to the Fortune Automotive Corporation. Authorized Users Only.

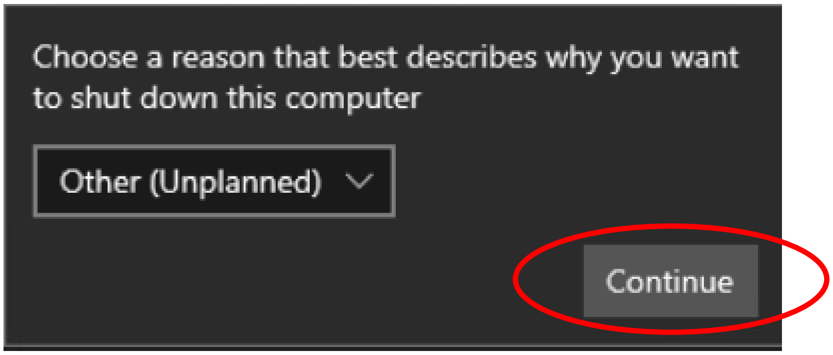
4) You should be immediately presented with the WARNING disclaimer message you created. Click **OK** to continue to the login prompt.



5) You will immediately notice that you are presented with the Other User log on screen. You will need to **type your username (Administrator) and password** to log on. This is the result of the first policy you configured.
6) Once you have logged on you can choose to play with other Computer and User Configuration settings to see what they do. When you are finished, shut down your server.

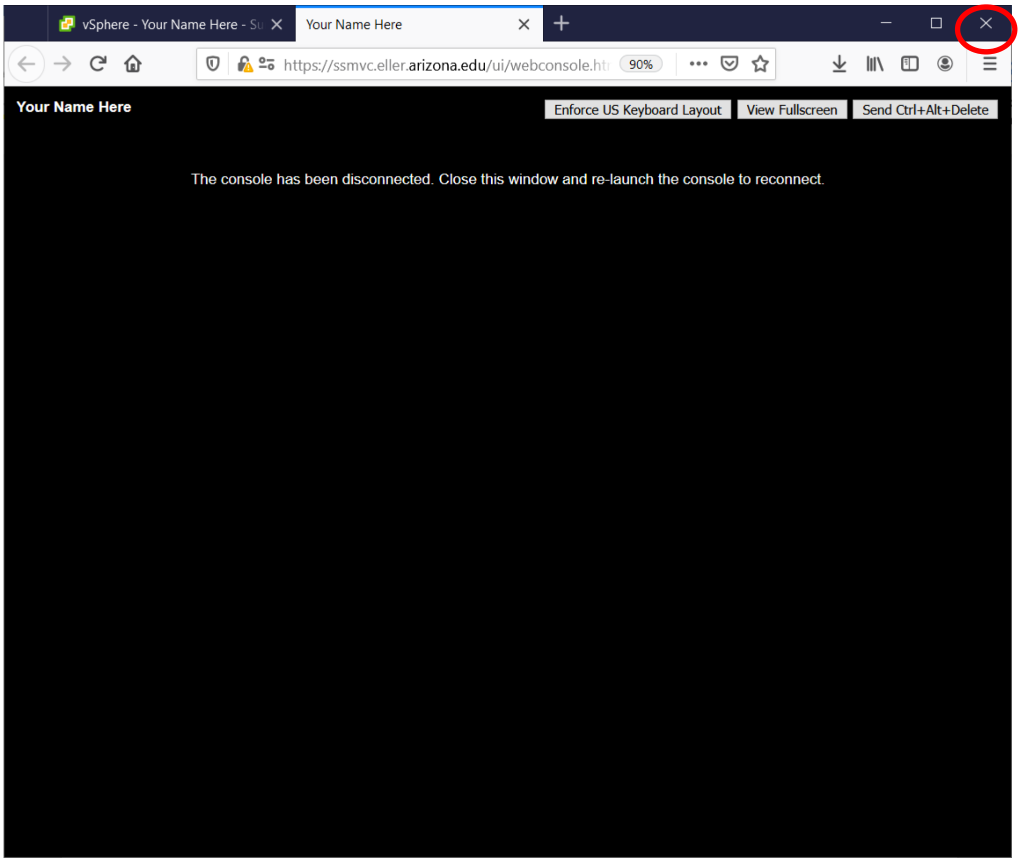


7) Click on the **Start** button in the lower left corner of the screen to bring up the Start screen. In the lower left corner you will see a power button. Click on the **power** button and choose **Shut down** from the menu.


Choose a reason that best describes why you want to shut down this computer

Other (Unplanned)

8) You will be asked to select a reason for the shutdown. **Choose any option** and click **Continue** to shut down the server.


vSphere - Your Name Here - Su
Your Name Here
https://ssmvc.eller.arizona.edu/ui/webconsole.ht
90%
Your Name Here
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete

The console has been disconnected. Close this window and re-launch the console to reconnect.

9) When the server is completely shut down the screen will be black with the statement “The console has been disconnected”. Close the window for your server by clicking on the **X** in the upper right-hand corner of the open tab.

5. Research & Write a Paper Discussing Group Policy

1) Now that you have a basic understanding of group policy and what it can do, you will need to do some additional research into other possible group policy security settings.
2) Google and Microsoft TechNet are good websites to help you research what is possible.
3) Write a paper explaining a minimum of 3 security group policy settings **that are not used or discussed in either the Default Domain Policy or the HR Users policy you created.** ***This would include <u>any</u> Password policies.***
4) See Lab Deliverables for more information.

Lab Deliverables

At this point you should have the following:

a. A new Group Policy Object configured with a few basic security settings and assigned to the root of your active directory.
b. An understanding of how group policy can be used and some of the settings that are possible for both computer objects and user objects within Active Directory.
c. A written paper explaining a minimum of 3 additional security settings that can be applied using group policy. These security settings should not be used in either the Default Domain Policy or your HR Users policy.
    i. Explain what each policy will do when enabled and disabled
    ii. Including specific information on what settings are possible and what setting is recommended to be used and why.
d. Your paper should be written using Times New Roman, 12 point font, double spaced.
e. Your paper must include a cover page, a body (including introduction and conclusion), and a reference page with a minimum of 3 references.
    i. Citations are REQUIRED for any direct quotes or paraphrased materials used in your paper. Failure to do so will result in a loss of up to 25% of the total points.
    ii. The paper must be formatted properly. Do NOT use a list or outline format for your paper. This is an incomplete paper and will result in a loss of points.

Submit the following via the D2L assignments section for the lab:

- Your completed paper.

Lab Rubric

Lab #4 will be graded in two parts: your active directory GPO and your paper. Here is the breakdown for how your lab will be graded:

Sections	Additional Information
Following Instructions (10%)	Please make certain you follow the instructions for the Lab Deliverable.
Group Policy Object Creation (25%)	You must create the HR Users GPO as instructed in this lab with the minimum set of policies as outlined in these instructions.
Group Policy Security Settings Discussion (40%)	The content of your paper must include a discussion of 3 or more possible security settings that can be applied to a computer or server via GPO. You must explain what the setting will do, how it will do it, what happens when enabled and disabled, what options are available with each, what setting is recommended, and why an organization would use these settings.
References (25%)	You must provide a minimum of 3 references and use proper citations with direct quotes and paraphrased materials.

Lab Resources

- Google
- Microsoft TechNet