Lab – Configure Windows Local Security Policy (Instructor Version)

Introduction

In this lab, you will configure Windows Local Security Policy. Windows Local Security Policy is used to configure a variety of security requirements for stand-alone computers that are not part of an Active Directory domain. You will modify password requirements, enable auditing, configure some user rights, and set some security options. You will then use Event Manager to view logged information.

Recommended Equipment

- A computer with Windows installed.

Note: Accessing the Local Security Policy tool is slightly different, depending on the version of Windows. But after it is open, the configurations are the same for the remaining steps in this lab.

Step 1: Review the security requirements.

A customer needs to have six stand-alone Windows computers at a branch office configured according to the security policy for the organization. These computers are not part of an Active Directory domain. The policies must be manually configured on each computer.

The security policy is as follows:

- Passwords must be at least 8 characters.
- Passwords must be changed every 90 days.
- A user may change their password once a day.
- A user must use a unique password for at least 8 changes of the password.
- A password must consist of three of the following four elements:
  - At least one lower case alpha character.
  - At least one upper case alpha character.
  - At least one numerical character.
  - At least one symbol character.
- Users are locked out of the computer after 5 attempts to enter the correct password. A user must wait 5 minutes for the lookout counter to reset.
- Each security setting for Audit Policy should be enabled.
- After 30 minutes of inactivity, the user will be automatically logged out. (Windows 8.1 and 8.0 only)
- Users must login before removing a laptop from the docking station
- At login, users should be presented with the following title and text:
  - Title: **Caution:**
  - Text: **Your activity is monitored. This computer is for business use only.**
- Users will receive a reminder to change the password 7 days before it expires.

The Windows Local Security Policy tool provides many more settings that are beyond the scope of this course.

Step 2: Open the Windows Local Security Policy tool.

a. To access Local Security Policy in Windows 7 and Vista, use the following path:

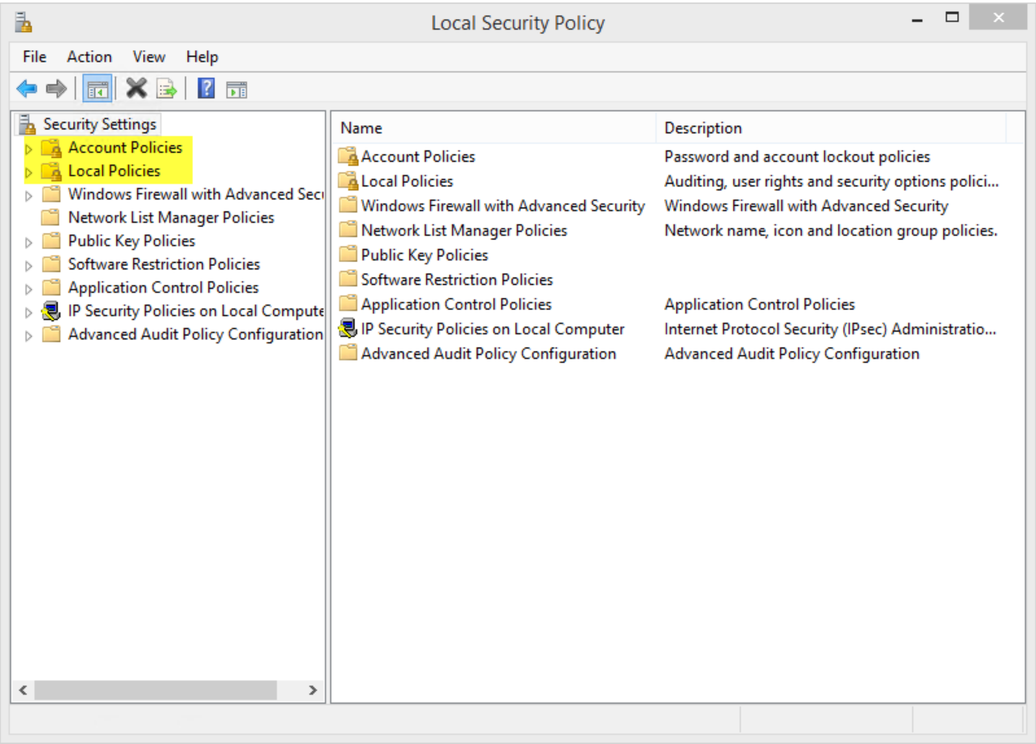
   Start > Administrative Tools > Local Security Policy

b. To access Local Security Policy in Windows 8 and 8.1, use the following path:

   Search > secpol.msc and then click **secpol**.

c. The **Local Security Policy** window opens. This lab will focus on the **Account Policies** and **Local Policies**, as highlighted in the figure below. The rest of the **Security Settings** are beyond the scope of this course.

   Note: Screenshots from Windows 8.1 are used throughout this lab.



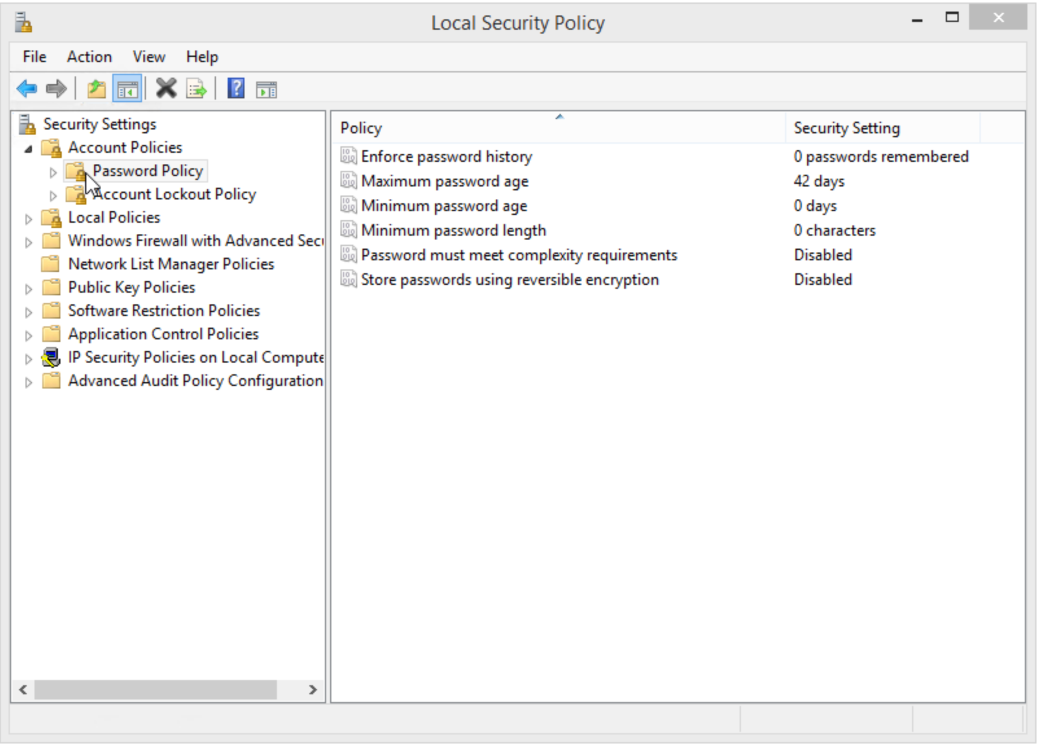
- Security Settings
  - Account Policies
  - Local Policies
  - Windows Firewall with Advanced Secu
  - Network List Manager Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Compute
  - Advanced Audit Policy Configuration

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

Step 3: Configure the Password Policy security settings.

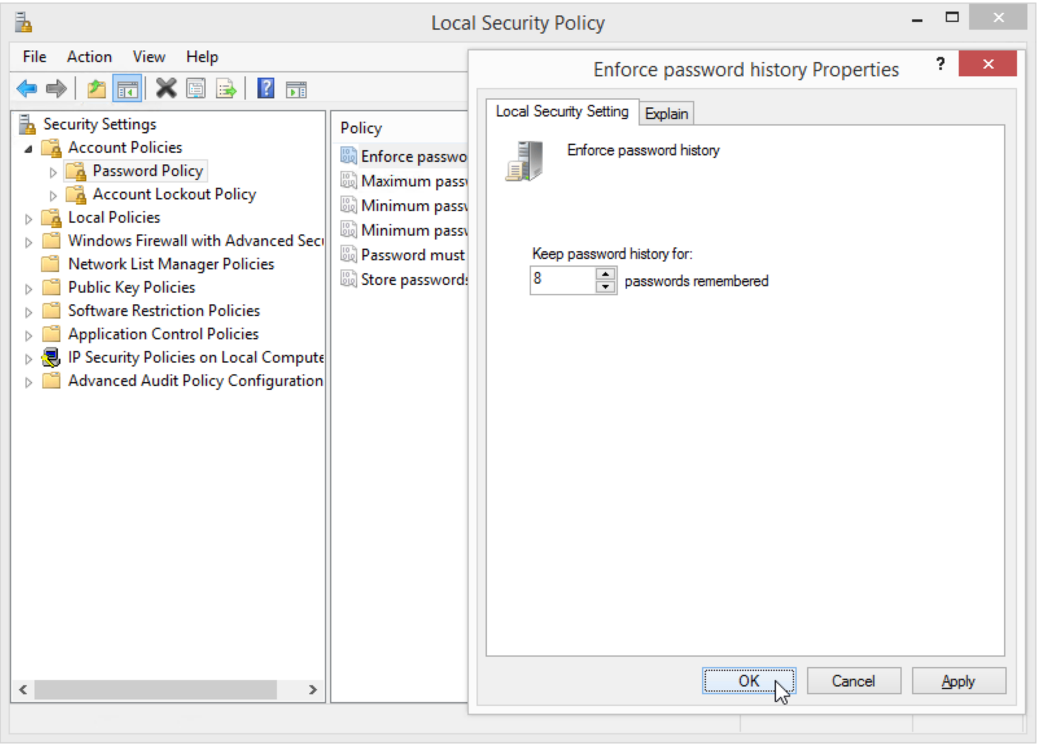
The first six requirements of the company’s security policy are configured in the **Account Policies** section of the **Local Security Policy** tool.

a. Click the arrow next to **Account Policies** to expand it, and then click **Password Policy**. Six policies are displayed in the right panel with their associated default security settings.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

b. The first policy, **Enforce password history**, is used to set the number of unique passwords the user must enter before being allowed to reuse a password. According to the organization's security policy in Step 1, the security setting for this policy should be **8**. Double-click **Enforce password history** to open the **Enforce password history Properties** window. Set the value to **8**.



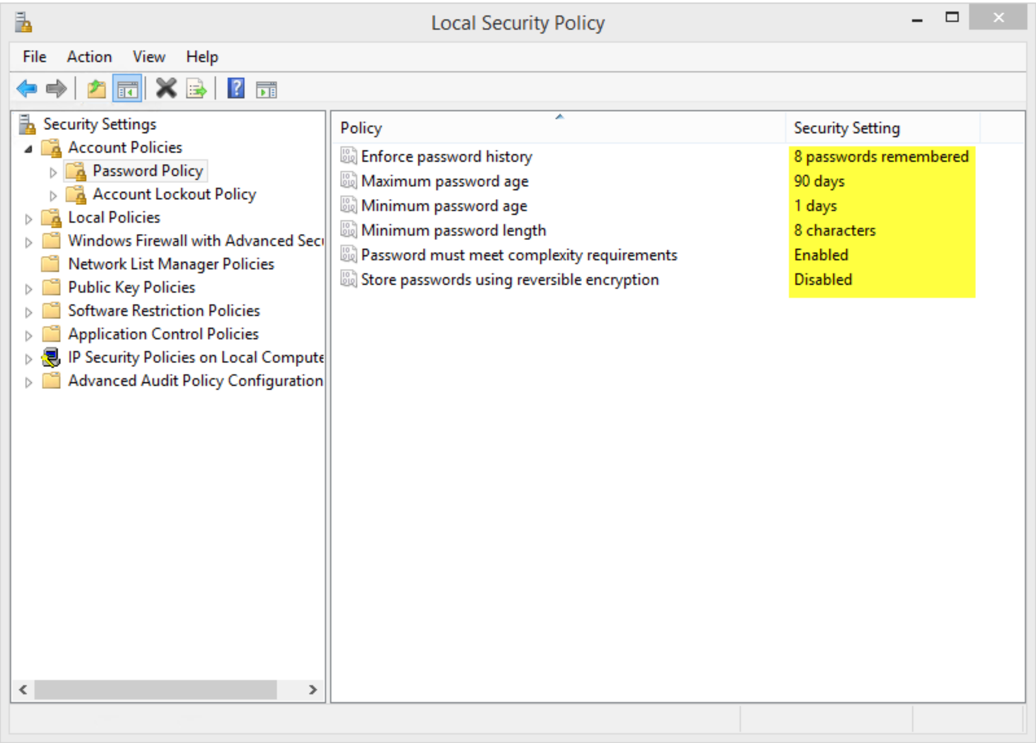
Keep password history for:
8 passwords remembered

c. Using the security policy requirements in Step 1, fill in the values you should set in **Local Security Policy** for the remaining **Password Policy** security settings.

Policy	Security Setting
Enforce password history	8
Maximum password age	90
Minimum password age	1
Minimum password length	8
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Note: The **Store passwords using reversible encryption** security setting should always be disabled. Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords. For this reason, this policy should never be enabled unless application requirements outweigh the need to protect password information.

d. Double-click on each of the policies and set the values according to your entries in the table above. When done, your configuration should look like the following:


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Enforce password history	8 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Step 4: Configure the Account Lockout Policy security settings.

a. According the security policy in Step 1, how many times is a user allowed to attempt to login before the account is locked?

5 attempts

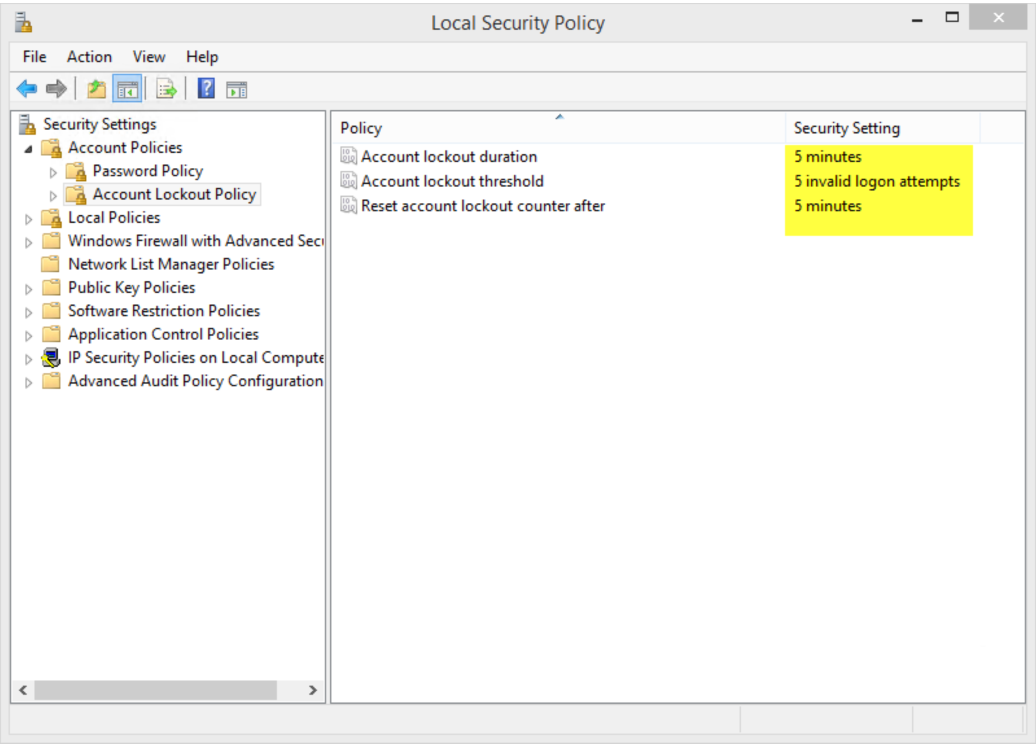
b. How long should the user have to wait before attempting to log back in?

____

5 minutes

c. Use the **Account Lockout Policy** security settings in **Local Security Policy** to configure the policy requirements. When done, your configuration should look like the following.

Hint: You will need to configure the **Account lockout threshold** first.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

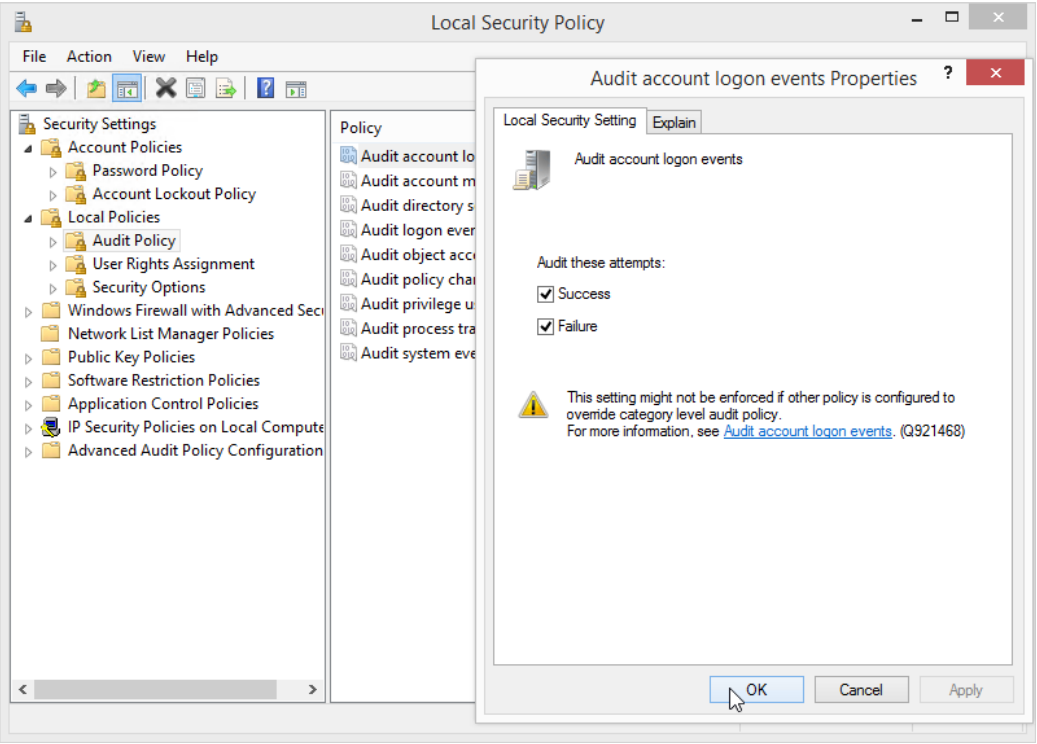
Policy	Security Setting
Account lockout duration	5 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	5 minutes

Step 5: Configure the Audit Policy security settings.

a. In **Local Security Policy**, expand the **Local Policies** menu, and then click **Audit Policy**.

b. Double-click **Audit account logon events** to open the **Properties** window. Click the **Explain** tab to learn about this security setting.

c. Click the **Security Setting** tab, and then click the check boxes for **Success** and **Failure**. Click **OK** to close the **Properties** window and apply the security settings.



Audit account logon events Properties

Audit account logon events

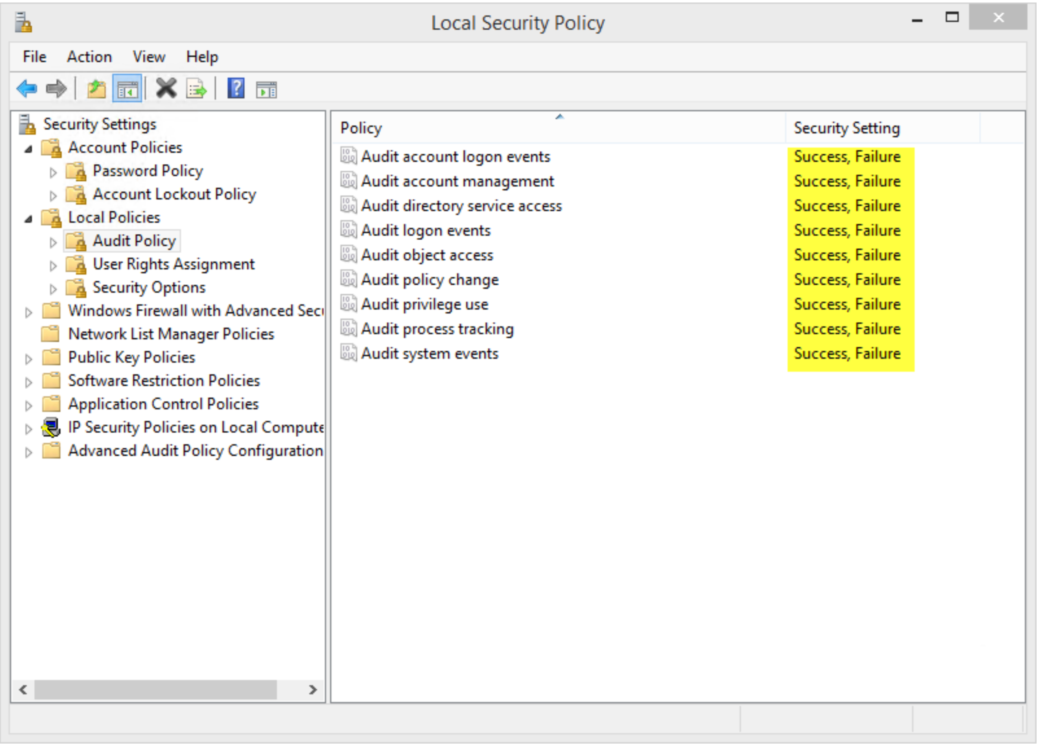
Audit these attempts:

☑ Success

☑ Failure

This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit account logon events. (Q921468)

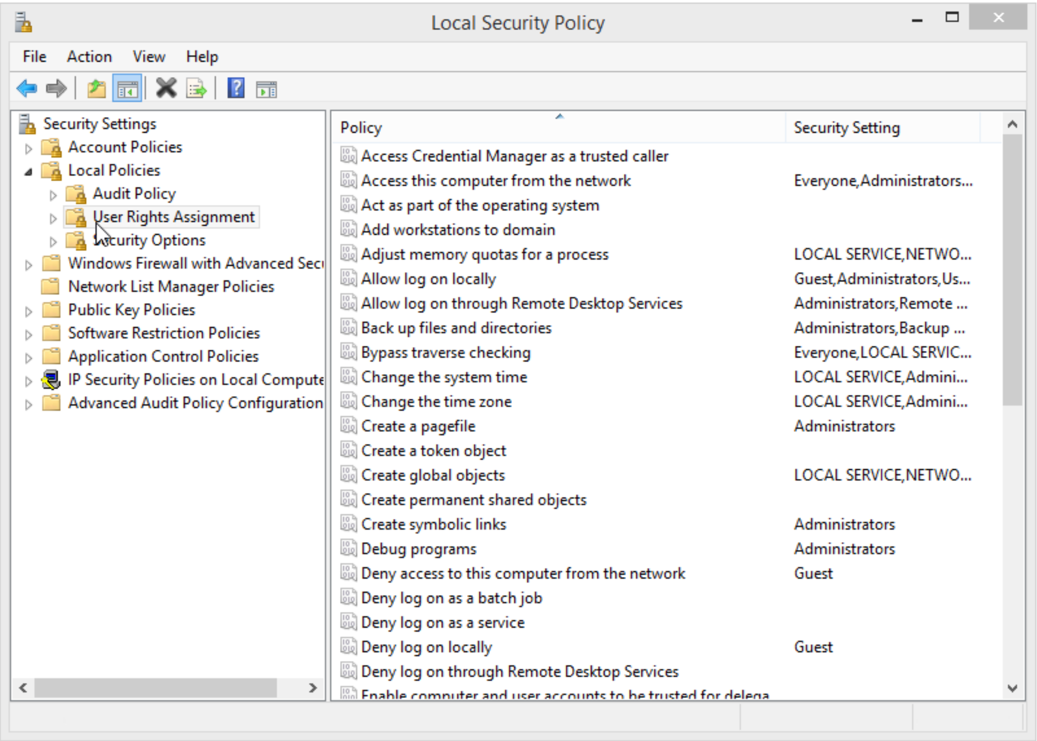
d. Continue modifying the rest of the **Audit Policy** security settings. Click the **Explain** tab for each and read what it does. Click the **Success** and **Failure** check boxes in each **Properties** window. After you are done, your **Audit Policy** configuration should look like the following:


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	Success, Failure
Audit system events	Success, Failure

Step 6: Configure additional Local Policies security settings

a. In **Local Security Policy**, click **User Rights Assignment** under **Local Policies** to view the security settings.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Access Credential Manager as a trusted caller	
Access this computer from the network	Everyone,Administrators...
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	LOCAL SERVICE,NETWO...
Allow log on locally	Guest,Administrators,Us...
Allow log on through Remote Desktop Services	Administrators,Remote ...
Back up files and directories	Administrators,Backup ...
Bypass traverse checking	Everyone,LOCAL SERVIC...
Change the system time	LOCAL SERVICE,Admini...
Change the time zone	LOCAL SERVICE,Admini...
Create a pagefile	Administrators
Create a token object	
Create global objects	LOCAL SERVICE,NETWO...
Create permanent shared objects	
Create symbolic links	Administrators
Debug programs	Administrators
Deny access to this computer from the network	Guest
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	Guest
Deny log on through Remote Desktop Services	
Enable computer and user accounts to be trusted for delega	

b. Although none of the security settings need to be modified to meet the security policy requirements, spend some time viewing the default settings. Are there any you would recommend changing? Why?

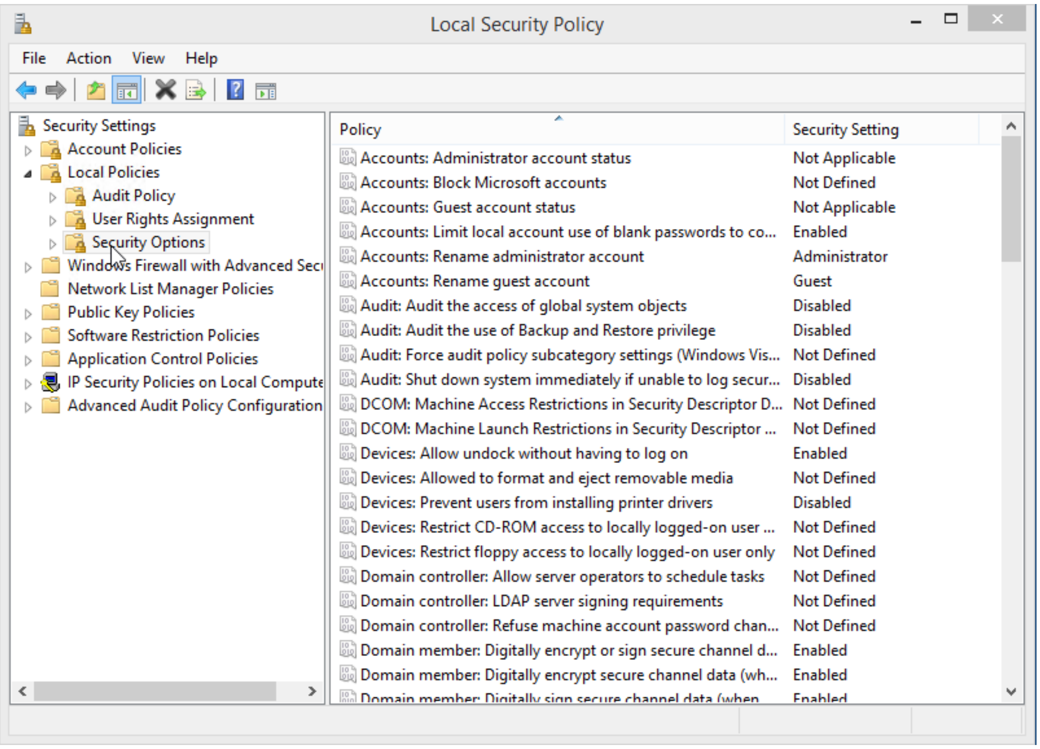
____

____

____

Answers will vary. The student may not understand all the settings. However, the student should be able to provide at least one example of a **User Rights Assignment** security setting that should be changed. Although the computer is stand-alone, this does not mean that it is not on a network. Stand-alone, in this case, means the computer is not a part of an Active Directory domain. Therefore, many of the **User Rights Assignment** settings could be changed to better protect the computer on the LAN. For example, the **Access this computer from the network** security setting defaults to allow everyone network access. The student might recommend that only the **Administrator** group be allowed access.

c. In **Local Security Policy**, click **Security Options** under **Local Policies** to view the security settings.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Accounts: Administrator account status	Not Applicable
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Applicable
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Disabled
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	Enabled
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Disabled
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: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Enabled
Domain member: Digitally encrypt secure channel data (wh...	Enabled
Domain member: Digitally sign secure channel data (when	Enabled

d. Using the remaining security policy requirements in Step 1, list the policy and security setting values you need to change in **Security Options** in the table below. The first one is done for you.

Policy	Security Setting
Interactive logon: Machine inactivity limit (Windows 8.1 and 8.0 only)	1800 seconds
Devices: Allow undock without having to log on	Disabled
Interactive logon: Message title for users attempting to log on	Caution:
Change the Interactive logon: Message text for users attempting to log on	Your activity is monitored. This computer is for business use only.
Interactive logon: Prompt user to change password before expiration	7 days

Step 7: Test the password policy security settings.

a. Test your password policy security settings by attempting to change the password. Try a new password that does not meet the length or complexity requirements.

In Windows 7 and Vista, use the following path:

Control Panel > User Accounts > Change your password

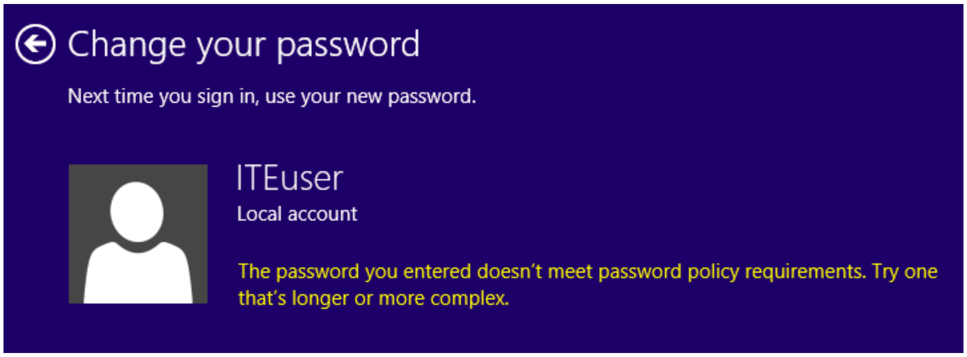
In Windows 8.1, use the following path:

Control Panel > User Accounts > Make changes to my account in PC settings > Sign-in options, and then click **Change** under **Password**.

In Windows 8.0, use the following path:

Control Panel > User Accounts > Make changes to my account in PC settings, and then click **Change your password**.

b. You should be presented with a message that your new password does not meet password policy requirements, such as this message in Windows 8.1:



Change your password

Next time you sign in, use your new password.

ITEuser

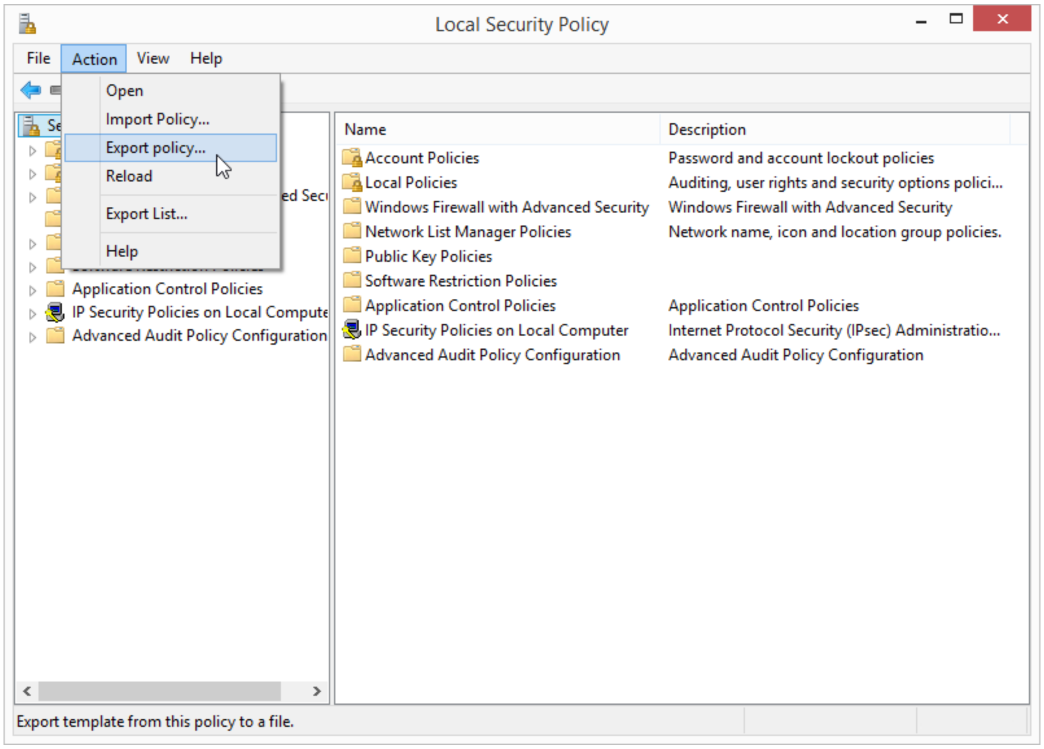
Local account

The password you entered doesn't meet password policy requirements. Try one that's longer or more complex.

Step 8: Export and import security policy settings.

The customer has another 5 stand-alone computers that must meet the same security policy requirements. Instead of manually configuring the settings each computer, export the settings on this computer.

a. From the menu bar in **Local Security Policy**, click **Action > Export policy...**



Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Firewall with Advanced Security	Windows Firewall with Advanced Security
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

Export template from this policy to a file.

b. Choose a name for the **.inf** file and save it to a location of your choice.

c. Copy the security policy **.inf** file to a flash drive. Take the flash drive to another computer. Insert the flash drive, open **Local Security Policy**, and click **Action > Import Policy...** Locate the **.inf** on the flash drive and open it to apply the security policy to the new computer.