Lab – Configure Windows Local Security Policy (Instructor Version)

**Instructor Note**: Red font color or gray highlights indicate text that appears in the instructor copy only.

# 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.

# Instructions

## 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 log in before removing a laptop from a docking station.
* At log in, 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.

## Configure the Password Policy security settings.

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.

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

* + - 1. To access Local Security Policy, click **Start** and search for **Local Security Policy**.
      2. In the Local Security Policy window, expand the **Account Policies** and click **Password Policy**. Six policies are displayed in the right panel with their associated default security settings.
      3. 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 the previous part, 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**.
      4. Using the security policy requirements in the previous part, 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.

* + - 1. Double-click each of the policies and set the values according to your entries in the table above.

## Configure the Account Lockout Policy security settings.

#### Questions:

According to the security policy in an earlier part, how many times is a user allowed to attempt to login before the account is locked?

Type your answers here.

5 attempts

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

Type your answers here.

5 minutes

Use the **Account Lockout Policy** security settings in **Local Security Policy** to configure the policy requirements.

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

## Configure the Audit Policy security settings.

* + - 1. In Local Security Policy, expand the Local Policies menu, and then click **Audit Policy**.
      2. Double-click **Audit account logon events** to open the **Properties** window. Click the **Explain** tab to learn about this security setting.
      3. Click the **Local 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.
      4. 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.

## Configure additional Local Policies security settings

* + - 1. In Local Security Policy, click **User Rights Assignment** under Local Policies to view the security settings.
      2. Although none of the security settings need to be modified to meet the security policy requirements, spend some time viewing the default settings.

#### Question:

Are there any you would recommend changing? Explain.

Type your answers here.

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.

* + - 1. In Local Security Policy, click **Security Options** under Local Policies to view the security settings.
      2. For the remaining security policy requirements in an earlier part, 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 | 1800 seconds |
| Devices: Allow undock without having to log on | Disabled |
| Interactive logon: Message title for users attempting to log on | Caution: |
| 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 |

## Test the password policy security settings.

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.

Click **Start** > **Settings** > **Accounts** > **Sign-in options**, and then click **Change** under **Password**.

You should be presented with a message that your new password does not meet password policy requirements.

## 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.

* + - 1. From the menu bar in Local Security Policy, select **Security Settings** > click **Action** > **Export policy...**
      2. Choose a name for the **.inf** file and save it to a location of your choice.
      3. 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.

End of Document