INFORMATION TECHNOLOGY SUPPORT SERVICE

Level - I

LEARNING GUIDE 33

Unit of Competence:	Protect Application or System Software
Module Title:	Protecting Application or System Software
LG Code:	ICT ITS1 M09 LO1 – LG33
TTLM Code:	ICT ITS1 TTLM 1019v1

LO 1: Ensure User Accounts are Controlled

Instruction Sheet	Learning Guide 33

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics –

- User Account Control
- User Account Configuration
- Notifications Displayed at Logon
- Utilities Used to Check Strength of Passwords
- Accessing Information Services

This guide will also assist you to attain the learning outcome stated in the cover page. Specifically, upon completion of this Learning Guide, you will be able to –

- Modify default user settings to ensure that they conform to security policy
- Previously created user settings are modified to ensure they conform to updated security policy
- Ensure legal notices displayed at logon are appropriate
- Appropriate utilities are used to check strength of passwords and consider tightening rules for password complexity
- Emails are monitored to uncover breaches in compliance with legislation
- information services are accessed to identify security gaps and take appropriate action using hardware and software or patches

Learning Instructions:

1. Read the specific objectives of this Learning Guide.
2. Follow the instructions described below 3 to 6.
3. Read the information written in the information "Sheet 1, Sheet 2, Sheet 3 and Sheet 4" in page 3, 14, 20, 25 and 33 respectively.
4. Accomplish the "Self-Check 1, Self-Check 2, Self-Check 3, Self-Check 4 and Self-Check 5" in page 12, 18, 23, 30 and 37 respectively.
5. If you earned a satisfactory evaluation from the "Self-Check" proceed to "Operation Sheet 1, Operation Sheet 2 and Operation Sheet 3 " in page 39
6. Do the "LAP test" in page 45

Information Sheet - 1	User Account Control

1.1. User Access

We do want our users to access the system; it's just that we want them to have the appropriate access. The control of user access can take many forms and apply at several levels. Once a computer is physically accessed, the user usually logs on to gain access to applications. These applications will access data in files and folders.

We can simplify the process down to 3 things.

- Physical access
- Authentication
- Authorisation

1.1.1. Physical Access

The first layer of management and security is the physical access to the computer. To prevent unauthorised access, a company may make use of:

- locks on the front doors
- locks on each floor
- locks on offices, etc
- security guards
- cameras
- keys on computer systems.

Only those who have permission and keys will be able to access a computer in the company's premises. The Internet, however, presents issues concerning access to corporate information or systems because physical restrictions cannot be imposed.

1.1.2. Authentication

Authentication is the process of verifying the identity of people who are attempting to access the network or system. Typically, a user identifies himself to the system, then is required to provide a second piece of information to prove their identity. This information is only known by the user or can only be produced by the user.

The most common method used to authenticate users is the ***Username and Password*** method. Using this method a user identifies itself with a username. They are then prompted for a password. The combination of name and password are then compared by the system to its data on configured users and if the combination matches the system's data the user is granted access.

Other authentication methods include:

- ***Username with static passwords*** - the password stays the same until changed by the user at some time

- ***Usernames with dynamic passwords*** - the password is constantly changed by a password generator synchronized with the user and system.
- ***Other challenge response systems* -** this may involve PINs, questions to the user requiring various answers or actions
- ***Certificate Based*** - this requires the user to have an electronic certificate or token. This may also need to be digitally signed by a trusted authority.
- ***Physical devices*** - these include the use of smartcards and biometrics. Generally, the entire authentication process occurs on the local workstation, thus eliminating the need for a special server.

Whatever method is used is determined by the organisational policy and security requirements.

1.1.3. Authorisation

Once a user has been authenticated (that is their identity validated) they are granted access to the network or system. For the user to then access data or an application or execute some task or command they need be authorised to do so. The authorisation process determines what the user can do on the network. In other words it enforces the organisation policy as applicable to the user.

The Network and System administrators are responsible for the technical configuration of network operating systems, directory services and applications. Part of the configuration includes security settings that authorise user access. The administrators use an organisational policy to determine these settings.

1.2. User Account

A user account is a collection of information that tells Windows which *files and folders you can access*, *what changes you can make to the computer*, and *your personal preferences*, such as your desktop background or screen saver. User accounts let you share a computer with several people, while having your own files and settings. Each person accesses his or her user account with a username and password.

There are three types of accounts. Each type gives users a different level of control over the computer:

- **Standard Accounts** are for everyday computing.
- **Administrator Accounts** provide the most control over a computer, and should only be used when necessary.
- **Guest Accounts** are intended primarily for people who need temporary use of a computer.

1.2.1. Standard User Account

A standard user account lets you use most of the capabilities of the computer. You can use most programs that are installed on the computer and change settings that affect your user account. However, you can't install or uninstall some software and hardware, you can't delete files that are required for the computer to work, and you can't change settings that affect other users or the security of the computer. If you're using a standard account, you might be prompted for an administrator password before you can perform certain tasks.

Why use a Standard User Account instead of an Administrator Account?

The ***standard account*** can help protect your computer by preventing users from making changes that affect everyone who uses the computer, such as deleting files that are required for the computer to work. We recommend creating a standard account for each user.

When you are logged on to Windows with a standard account, you can do almost anything that you can do with an ***administrator account***, but if you want to do something that affects other users of the computer, such as installing software or changing security settings, Windows might ask you to provide a password for an administrator account.

1.2.2. Administrator Account

An administrator account is a ***user account*** that lets you make changes that will affect other users. Administrators can change security settings, install software and hardware, and access all files on the computer. Administrators can also make changes to other user accounts.

When you set up Windows, you'll be required to create a user account. This account is an administrator account that allows you to set up your computer and install any programs that you would like to use. Once you have finished setting up your computer, we recommend that you use a ***standard user account*** for your day-to-day computing. It's more secure to use a standard user account instead of an administrator account because it can prevent a person from making changes that affect everyone who uses the computer.

1.2.3. Guest Account

A guest account allows people to have temporary access to your computer. People using the guest account can't install software or hardware, change settings, or create a password. You have to turn on the guest account before it can be used.

1.3. User Profiles

User profile is a collection of settings that make the computer look and work the way you want it to. It contains your settings for desktop backgrounds, screen savers, pointer preferences, sound settings, and other features. Your user profile ensures that your personal preferences are used whenever you log on to Windows.

A user profile is different from a user account, which you use to log on to Windows. Each user account has at least one user profile associated with it.

1.4. User Account Control

User Account Control (UAC) is a feature in Windows that can help you stay in control of your computer by informing you when a program makes a change that requires administrator-level permission. UAC works by adjusting the permission level of your user account. If you're doing tasks that can be done as a ***standard user***, such as reading e-mail, listening to music, or creating documents, you have the permissions of a standard user—even if you're logged on as an administrator.

When changes are going to be made to your computer that requires administrator-level permission, UAC notifies you. If you are an administrator, you can click Yes to continue. If you are not an administrator, someone with an administrator account on the computer will have to enter their password for you to continue. If you give permission, you are temporarily given the rights of an administrator to complete the task and then your permissions are returned back to that of a standard user. This makes it so that even if you're using an administrator account, changes cannot be made to your computer without you knowing about it, which can help prevent ***malicious software (malware)*** and ***spyware*** from being installed on or making changes to your computer.

When your permission or password is needed to complete a task, UAC will notify you with one of four different types of dialog boxes.

Table 1-1: The different types of dialog boxes used to notify you and guidance on how to respond to them.

Icon	Type	Description
🛡	A setting or feature that is part of Windows needs your permission to start.	This item has a ***valid digital signature*** that verifies that Microsoft is the publisher of this item. If you get this type of dialog box, it's usually safe to continue. If you are unsure, check the name of the program or function to decide if it's something you want to run.
?	A program that is not part of Windows needs your permission to start.	This program has a valid digital signature, which helps to ensure that the program is what it claims to be and verifies the identity of the publisher of the program. If you get this type of dialog box, make sure the program is the one that you want to run and that you

		trust the publisher.
!	A program with an unknown publisher needs your permission to start.	This program ***doesn't have a valid digital signature*** from its publisher. This doesn't necessarily indicate danger, as many older, legitimate programs lack signatures. However, you should use extra caution and only allow a program to run if you obtained it from a trusted source, such as the original CD or a publisher's website. If you are unsure, look up the name of the program on the Internet to determine if it is a known program or malicious software.
✖	You have been blocked by your ***system administrator*** from running this program.	This program has been ***blocked*** because it is known to be ***untrusted***. To run this program, you need to contact your system administrator.

We recommend that you log on to your computer with a standard user account most of the time. You can browse the Internet, send e-mail, and use a word processor, all without an administrator account. When you want to perform an administrative task, such as installing a new program or changing a setting that will affect other users, you don't have to switch to an administrator account; Windows will prompt you for permission or an administrator password before performing the task. We also recommend that you create standard user accounts for all the people who use your computer.

In this version of Windows, you can adjust how often UAC notifies you when changes are made to your computer. If you want to be informed when any change is made to your computer, choose to always be notified.

1.4.1. User Account Control settings

User Account Control (UAC) notifies you before changes are made to your computer that requires administrator-level permission. The default UAC setting notifies you when programs try to make changes to your computer, but you can control how often you are notified by UAC by adjusting the settings.

Table 1-2: The description of the UAC settings and the potential impact of each setting to the security of your computer.

Setting	Description	Security Impact
Always Notify	• You will be notified before programs make changes to your computer or to Windows settings that require the permissions of an administrator. • When you're notified, your desktop will be dimmed, and you must either approve or deny the request in the UAC dialog box before you can do anything else on your computer. The dimming of your desktop is referred to as the secure desktop because other programs can't run while it's dimmed.	• This is the most secure setting. • When you are notified, you should carefully read the contents of each dialog box before allowing changes to be made to your computer.
Notify me only when programs try to make changes to my computer	• You will be notified before programs make changes to your computer that requires the permissions of an administrator. • You will not be notified if you try to make changes to Windows settings that require the permissions of an administrator. • You will be notified if a program outside of Windows tries to make changes to a Windows setting.	• It's usually safe to allow changes to be made to Windows settings without you being notified. However, certain programs that come with Windows can have commands or data passed to them, and malicious software can take advantage of this by using these programs to install files or change settings on your computer. You should always be careful about which programs you allow to run on your computer.
Notify me only when programs try to make changes to my computer (do not dim my desktop)	• You will be notified before programs make changes to your computer that requires the permissions of an administrator. • You will not be notified if you try to make changes to Windows settings that require the permissions of an administrator. • You will be notified if a program outside of Windows tries to make changes to a Windows setting.	• This setting is the same as "Notify only when programs try to make changes to my computer," but you are not notified on the secure desktop. • Because the UAC dialog box isn't on the secure desktop with this setting, other programs might be able to interfere with the dialog's visual appearance. This is a small security risk if you already have a malicious program running on your computer.

Never Notify	• You will not be notified before any changes are made to your computer. If you are logged on as an administrator, programs can make changes to your computer without you knowing about it. • If you are logged on as a standard user, any changes that require the permissions of an administrator will automatically be denied. • If you select this setting, you will need to restart the computer to complete the process of turning off UAC. Once UAC is off, people that log on as administrator will always have the permissions of an administrator.	• This is the least secure setting. When you set UAC to never notify, you open up your computer to potential security risks. • If you set UAC to never notify, you should be careful about which programs you run, because they will have the same access to the computer as you do. This includes reading and making changes to protected system areas, your personal data, saved files, and anything else stored on the computer. Programs will also be able to communicate and transfer information to and from anything your computer connects with, including the Internet.

1.4.2. Why is User Account Control necessary?

The most important rule for controlling access to resources is to provide the least amount of access privileges required for users to perform their daily tasks. Many tasks do not require administrator privileges. However, because previous versions of Windows created all user accounts as administrators by default, users logged on to their computers with an administrator account. Without User Account Control (UAC), when a user is logged on as an administrator, that user is automatically granted full access to all system resources.

However, most users do not require such a high level of access to the computer. Often users are unaware that they are logged on as an administrator when they browse the Web, check e-mail, and run software. While logging on with an administrator account enables a user to install legitimate software, the user can also unintentionally or intentionally install a malicious program. A malicious program installed by an administrator can fully compromise the computer and affect all users.

With the introduction of UAC, the access control model changed to help mitigate the impact of a malicious program. When a user attempts to start an administrator application, the User Account Control dialog box asks the user to click Yes or No before the user's full administrator access token can be used. If the user is not an administrator, the user must provide an administrator's credentials to run the program.

Because UAC requires an administrator to approve application installations, unauthorized applications cannot be installed automatically or without the explicit consent of an administrator.

1.4.3. How UAC Work

There are two levels of users: standard users and administrators. Standard users are members of the Users group and administrators are members of the Administrators group on the computer.

Both standard users and administrators access resources and run applications in the security context of standard users by default. When a user logs on to a computer, the system creates an access token for the user. This access token contains information about the level of access that the user is granted, including specific ***Security Identifiers*** (SIDs) and ***Windows privileges***. When an administrator logs on, two separate access tokens are created for the user: a standard user access token and an administrator access token. The standard user access token contains the same user-specific information as the administrator access token, but the administrative Windows privileges and SIDs are removed. The standard user access token can start standard user applications but cannot start applications that perform administrative tasks.

When the user needs to run applications that perform administrative tasks (administrator applications), the user is prompted to change or elevate the security context from a standard user to an administrator. This default user experience is called ***Admin Approval Mode***. In this mode, applications require specific permission to run as an administrator application.

Self-Check – 1	**Written Test**

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. __________________ is a collection of information that tells Windows which files and folders you can access, what changes you can make to the computer, and your personal preferences, such as desktop background or screen saver. **(1 pts)**
2. __________________ lets you use most of the capabilities of the computer. You can use most programs that are installed on the computer and change settings that affect your user account. **(1 pts)**
3. __________________ is a user account that lets you make changes that will affect other users change security settings, install software and hardware, and access all files on the computer. **(1 pts)**
4. ____________ allows people to have temporary access to your computer. **(1 pts)**
5. __________________ is a collection of settings that make the computer look and work the way you want it to. **(1 pts)**
6. __________________ is the process of verifying the identity of people who are attempting to access the network or system. **(1 pts)**
7. __________________ determines what the user can do on the network. In other words it enforces the organization policy as applicable to the user. **(1 pts)**
8. The most common method used to authenticate users is __________________
9. Why use a Standard User Account instead of an Administrator Account? **(2 pts)**

   ____

   ____

   ____

   ____

10. List and describe authentication methods used to authenticate users. **(4 pts)**

   ____

   ____

   ____

   ____

   ____

11. _____________________ is a feature in Windows that can help you stay in control of your computer by informing you when a program makes a change that requires administrator-level permission. **(1 pts)**

12. List the four different types of dialog boxes that UAC will notify you when your permission or password is needed to complete a task. **(4 pts)**

    ____

    ____

    ____

    ____

13. List the UAC settings and the potential impact of each setting to the security of your computer. **(4 pts)**

    ____

    ____

    ____

    ____

14. When a user logs on to a computer, the system creates an access token for the user. This access token contains information about the level of access that the user is granted, including specific _____________________ and _____________________. **(2 pts)**

15. When the user needs to run applications that perform administrative tasks (administrator applications), the user is prompted to change or elevate the security context from a standard user to an administrator. This default user experience is called _____________________. **(1 pts)**

Note: **Satisfactory rating - 13 points** **Unsatisfactory - below 13 points**

You can ask your teacher for the copy of the correct answers.

Answer Sheet

Score = ___________

Rating: ___________

Name: ________________________________ Date: ________________

Short Answer Questions

1. _________________________
2. _________________________
3. _________________________
4. _________________________
5. _________________________
6. _________________________
7. _________________________
8. _________________________
9. ____
____
____
____
10. ____
____
____
____
11. _________________________
12. ____
____
____
____
13. ____
____
____
____

14._____________________ and _____________________

15._______________________

Information Sheet – 2	User Account Configuration

2.1. User Account Configuration

Network and System Administrators are responsible for configuring user accounts. Network operating systems and applications have many security options and setting relating to user access. How does an administrator determine the configuration and setting for user accounts?

Organisation policies and procedures provide the guidelines for administrators.

2.1.1. User Account Settings

The organisation's policies should make statements as to the degree of user control that is required. Network procedures should contain details as to how these policies may be implemented. For example, the policy may state that user passwords should not be less than six characters. The procedures will then describe how the administrator should configure the operating system to ensure that all passwords are at least six characters.

The administrator should review the policies to ensure that the procedures produce the desired outcomes. The procedures should describe in detail how to make use of the operating system facilities to configure user accounts in accordance with the security requirements.

The actual way you set these parameters will vary with each operating environment, however, here are some basic parameters covered by most operating systems to consider when setting up user account options:

- ***Password requirements*** - whether a password is required, minimum length, complexity, needs to be changed at intervals, etc
- ***Account lock out settings*** - disabling accounts that have made a number of bad logon attempts
- ***Access hours*** - the standard days and time that users will be permitted to access the network
- ***Account expiry dates*** - date when account will be disabled
- ***Logon restrictions*** - accounts can only be used at specified locations or workstations.
- ***Home directory information*** - a home directory is a folder that usually has the name of the user and the user has full permissions over.
- ***Logon scripts*** - these perform specific tasks or run specific programs when the user logs on

2.1.2. Configuring User Access

Once user account settings have been determined how do we know who should have accounts and what access should be set?

2.1.2.1. User Authorisations

Once again, organisational policy and procedures provide the necessary information for the administrators. There should be procedures in place that inform the appropriate people that a person requires a new user account or changes to an existing account or a deletion of accounts. The notification procedure should cover circumstances such as new employees joining the organisation, employees changing positions in the organisation and employees leaving the organisation. These notifications must come from authorised people in the organisation (managers, etc) as stated in the policy and procedures.

Notifications also need to specify what information, data, resources etc the account is permitted to access. The request for access must be authorised by an appropriate person in the organisation (usually department managers). The access permissions for users should be carefully planned and determined in writing by appropriate people who have the authority to allocate the access. Procedures should address:

- Which managers can authorise a new user
- Standards for user id and passwords
- Groups that users can belong to and authority required for each group
- Basic accesses that all users are allowed
- Authorisation requirements to access sensitive data
- Application accesses
- Ability to install additional software
- Email and internet accesses
- Special accesses that may be required.

2.1.2.2. Use of Groups

The most common way of administering access permissions is to create **groups** and put user accounts into appropriate groups. The group is then permitted or denied access as required. Using groups is an efficient way of managing authorisation because you only need to set access permission to a group and not individual accounts.

For example, a company may have thousands of users, but analysis of what those users want to do may show that there are twenty or more different combinations of access permissions required. By assigning users to groups and then allocating permissions to the group, the security administration is greatly simplified.

Once we have users allocated to groups we can explore other levels of controlling access. Allocating permissions to folders and files is a major security provision of network operating systems and one that is important to set up correctly. Can we go lower and look at the content of a specific file and restrict access there?

The restriction of file access is most applicable in controlling access to database files.

For example, imagine a Payroll system using a database in which the data is stored in tables. These tables have columns and rows of data. Let us think about two groups of user, the payroll department staff and the manager of a department. The payroll group are likely to be allowed full access to all the data although in a very large organisation there may be segregation of access.

But what about a department manager? This person may be allowed to see salary details for the staff that work in the department only.

In the table containing salary details there may be a row for every employee in the organisation. This means that we only want to show this manager the rows that relate to the one department. This would be secured with a filter that only displays staff in the department being examined.

Furthermore there may be information about an employee that even their manager may not be able to see, such as medical or financial information. This information may be restricted by controlling the columns returned in a report or query.

This type of security is really part of the application control rather than the network but it is still an important part of the overall security of the system and needs to be addressed by the organisational procedures.

2.1.2.3. Permissions and Rights

Permissions generally refer to file and directory access. The user account or group can be set with the following type of permissions:

- No access at all to files and directories
- Read only.
- Modify where the contents of files and directories may be accesses but changed or added to but not deleted
- Full Control or Supervisory where files and directories can be view modified and deleted.

Rights (or privileges) generally refer to the restriction on user accounts or group in performing some task or activity. For example a user account or group may be assigned administrator or supervisor rights meaning that the user can perform administration tasks like create, modify or delete user accounts. Care must be taken with rights to ensure security is not compromised.

2.2. Managing User Accounts

Once user accounts are configured we still need to manage the accounts as required by organisational policy. For example user accounts for contractors are active only for as long as the contractor are physically on site. This means that accounts need to be enabled and disabled. This activity should be addressed by procedures.

Note also that many networks on different OS’s allow’ ’guest’ and’ ’temporary’ accounts. These are usually set up for either read-only or short-term access to people who would not normally have access to the system. Great care must be taken in configuring or using these accounts firstly because they can allow anonymous and uncontrolled use of a system and secondly guest passwords can sometimes be guessed easily and provide a doorway for hackers/crackers.

Administrators need to review procedures to ensure that they remain current and address any changes to the organisation and the network.

Administrators need to be aware of user activities and practices when accessing the network. Organisational policy and procedures should address how users should access the network. In time users may develop shortcuts and practices that knowingly or unknowingly are in breech of policy and may compromise network security. For example a user may log on to the network on one workstation. Then to allow access for a colleague who has forgotten their password the users logs in on another workstation for the colleague. The result is two concurrently network connections for one user account but for two different people who have different user access requirements.

To manage user accounts appropriately administrators should

- Regularly review organisational policies and procedures to be aware of requirements and address any organisational or network changes
- Conduct regular checks to ensure the change management procedures are working for new, changed and deleted users
- Review and investigate current work practices regarding user network access
- Conduct information and training sessions for network users to reinforce appropriate practices and organisational policy
- Conduct regular audits of network access—verifying current users and deleting expired accounts

Managing user accounts can be a complex and tedious task but we can make things easier by ensuring appropriate policy and procedures are in place.

Self-Check – 2	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. ______________________should make statements as to the degree of user control that is required. **(1 pts)**
2. ______________________need to review procedures to ensure that they remain current and address any changes to the organisation and the network. **(1 pts)**
3. List and describe some basic parameters covered by most operating systems to consider when setting up user account options: **(6 pts)**
4. The most common way of administering ______________________ is to create groups and put user accounts into appropriate groups. **(1 pts)**
5. ______________________ generally refer to file and directory access. **(1 pts)**
6. List type of permissions the user account or group can be set with: **(4 pts)**
7. ______________________ generally refer to the restriction on user accounts or group in performing some task or activity. **(1 pts)**
8. List what administrators should do to manage user accounts appropriately. **(4 pts)**
9. Managing user accounts can be a complex and tedious task but we can make things easier by ensuring appropriate ___________________ are in place. **(1 pts)**

Note: **Satisfactory rating - 11 points** **Unsatisfactory - below 11 points**

You can ask your teacher for the copy of the correct answers.

Answer Sheet

Score = ___________

Rating: ___________

Name: ________________________________ Date: ________________

Short Answer Questions

1. ______________________
2. ______________________
3. ____

   ____

   ____

   ____

   ____

   ____

   ____
4. ______________________
5. ______________________
6. ____

   ____

   ____

   ____
7. ______________________
8. ____

   ____

   ____

   ____

   ____
9. ______________________

Information Sheet - 3	Notifications Displayed at Logon

3.1. Identifying Logon Restrictions

Often, authentication problems occur because administrators have configured logon restrictions to enforce the organization's security requirements. Logon restrictions include locking accounts after several incorrect attempts at typing a password, allowing users to log on only during specific hours, requiring users to change their passwords regularly, disabling accounts, and accounts that expire on a specific date. The sections that follow describe each of these types of logon restrictions.

3.1.1. Account Lockout

If a user provides incorrect credentials several times in a row (for example, if an attacker is attempting to guess a user's password, or if a user repeatedly mistypes a password), Windows can block all authentication attempts for a specific amount of time.

Account lockout settings are defined by Group Policy settings in the Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policies\ node as follows:

- The number of incorrect attempts is defined by the Account Lockout Threshold setting.
- The time that the number of attempts must occur within is defined by the Reset Account Lockout Counter After policy.
- The time that the account is locked out is defined by the Account Lockout Duration policy.

If a user receives an error message indicating that her account is locked out or she cannot log in even if she thinks she has typed her password correctly, you should validate the user's identity and then unlock the user's account. To unlock a user's account, view the user's Properties dialog box, and clear the Account Is Locked Out check box (for local Windows 7 user accounts) Then, click Apply.

3.1.2. Logon Hour Restrictions

Administrators can also use the Account tab of an AD DS user's properties to restrict logon hours. This is useful when administrators do not want a user to log on outside his normal working hours.

If a user attempts to log on outside his allowed hours, Windows 7 displays the error message "*Your account has time restrictions that prevent you from logging on at this time. Please try again later*." The only way to resolve this problem is to adjust the user's logon hours by clicking the Logon Hours button on the Account tab of the user's Properties dialog box.

3.1.3. Password Expiration

Most security experts agree that users should be required to change their passwords regularly. Changing user passwords accomplishes two things:

- If attackers are attempting to guess a password, it forces them to restart their efforts. If users never change their passwords, attackers would be able to guess them eventually.
- If an attacker has guessed a user's password, changing the password prevents the attacker from using these credentials in the future.

Password expiration settings are defined by Group Policy settings in the Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy node as follows:

- The time before a password expires is defined by the Maximum Password Age policy.
- The number of different passwords that users must have before they can reuse a password is defined by the Enforce Password History policy.
- The time before users can change their password again is defined by the Minimum Password Age policy. When combined with the Enforce Password History policy, this can prevent users from changing their password back to a previous password.

If users attempt to log on interactively to a computer and their password has expired, Windows prompts them to change their password automatically. If users attempt to access a shared folder, printer, Web site, or other resource using an expired password, they will simply be denied access. Therefore, if a user calls and complains that she cannot connect to a resource, you should verify that the user's password has not expired. You can prevent specific accounts from expiring by selecting the Password Never Expires check box on the Account tab of the user's Properties dialog box.

3.1.4. Disabled Account

Administrators can disable user accounts to prevent a user from logging on. This is useful if a user is going on vacation and you know she won't be logging on for a period of time, or if a user's account is compromised and IT needs the user to contact them before logging on.

To enable a user's disabled account, clear the Account Is Disabled check box in the user's Properties dialog box.

3.1.5. Account Expiration

In AD DS domains, accounts can be configured to expire. This is useful for users who will be working with an organization for only a limited amount of time. For example, if a contract employee has a two-week contract, domain administrators might set an account expiration date of two weeks in the future.

To resolve an expired account, edit the account's properties, select the Account tab, and set the Account Expires value to a date in the future. If the account should never expire, you can set the value to Never.

3.2. Determining Logon Context

Users can authenticate to the local user database or an AD DS domain. Logon restrictions defined for the domain only apply to domain accounts, and vice versa. Therefore, when examining logon restrictions for users, you must determine their logon context.

The quickest way to do this is to open a command prompt and run the command set to display all environment variables. Then, look for the USERDOMAIN line. If the user logged on with a local user account, this will be the computer name (shown on the COMPUTERNAME line). If the user logged on with an AD DS user account, this will be the name of the domain. You can also check the LOGONSERVER line to determine whether a domain controller or the local computer authenticated the user.

Self-Check – 3	**Written Test**

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Authentication problems occur because administrators have configured logon restrictions to enforce the organization's ______________________. **(1 pts)**
2. If a user provides ______________________ several times in a row (for e.g., if a user repeatedly mistypes a password), Windows can block all authentication attempts for a specific amount of time. **(1 pts)**
3. If a user attempts to log on outside his allowed hours, Windows 7 displays the error message____ ____________________________________. **(2 pts)**
4. Write the two things that changing user passwords accomplishes: **(2 pts)**

   ____

   ____

   ____

   ____

5. If users attempt to log on interactively to a computer and their password has expired Windows prompts them to ______________________________. **(1 pts)**
6. Administrators can ______________________ to prevent a user from logging on. **(1 pts)**

Note: **Satisfactory rating - 5 points** **Unsatisfactory - below 5 points**

You can ask your teacher for the copy of the correct answers.

Answer Sheet

Score = ___________

Rating: ___________

Name: ________________________________ Date: ________________

Short Answer Questions

1. ________________________

2. ________________________

3. ____

____

4. ____

____

____

____

5. _______________________________________

6. ________________________

Information Sheet - 4	**Protect Your Computer with a Password**

4.1. Definitions of a Password

A *password* is a string of characters that people can use *to log on to a computer* and access files, programs, and other resources. Passwords help ensure that people *do not access the computer* unless they have been *authorized* to do so. In Windows, a password can include *letters*, *numbers*, *symbols*, and *spaces*. Windows passwords are also *case-sensitive*. To help keep your computer *secure*, you should always create a *strong password*.

To help keep the information on *your computer secure*, you should *not give out your password* or *write it in a place where others can see it*.

4.1.1. Strong Passwords and Passphrases

A *password* is a string of characters used to access information or a computer. *Passphrases* are typically longer than passwords, for added security, and contain *multiple words* that create a phrase. Passwords and passphrases help prevent unauthorized people from accessing files, programs, and other resources. When you create a password or passphrase, you should make it strong, which means it's difficult to guess or crack. It's a good idea to use strong passwords on all user accounts on your computer. If you're using a workplace network, your network administrator might require you to use a strong password.

Tables 4-1 make a password or passphrase strong

A strong password:	A strong passphrase:
• Is at least eight characters long. • Does not contain your user name, real name, or company name. • Does not contain a complete word. • Is significantly different from previous passwords.	• Is 20 to 30 characters long. • Is a series of words that create a phrase. • Does not contain common phrases found in literature or music. • Does not contain words found in the dictionary. • Does not contain your user name, real name, or company name. • Is different from previous passphrases.

Tables 4-1 four categories characters Strong passwords and passphrases contain:

Character category	Examples
Uppercase letters	A, B, C
Lowercase letters	a, b, c
Numbers	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols found on the keyboard (all keyboard characters not defined as letters or numerals) and spaces	` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /

A password or passphrase might meet all the criteria above and still be weak. For example, Hello2U! meets all the criteria for a strong password listed above, but is still weak because it contains a complete word. H3ll0 2 U! is a stronger alternative because it replaces some of the letters in the complete word with numbers and also includes spaces.

Help yourself remember your strong password or passphrase by following these tips:

- Create an acronym from an easy-to-remember piece of information. For example, pick a phrase that is meaningful to you, such as My son's birthday is 12 December, 2004. Using that phrase as your guide, you might use Msbi12/Dec,4 for your password.
- Substitute numbers, symbols, and misspellings for letters or words in an easy-to-remember phrase. For example, My son's birthday is 12 December, 2004 could become Mi$un's Brthd8iz 12124, which would make a good passphrase.
- Relate your password or passphrase to a favorite hobby or sport. For example, I love to play badminton could become ILuv2PlayB@dm1nt()n.

If you feel you must write down your password or passphrase to remember it, make sure you don't label it as such, and keep it in a safe place.

Windows passwords can be much longer than the eight characters recommended above. In fact, you can make a password up to 127 characters long. However, if you are on a network that also has computers running Windows 95 or Windows 98, consider using a password that is no longer than 14 characters. If your password is longer than 14 characters, you might not be able to log on to your network from computers running those operating systems.

4.2. Modify User Security Policy

4.2.1. Password policy

A **password policy** is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training. The password policy may either be advisory or mandated by technical means. Some governments have national authentication frameworks that define requirements for user authentication to government services, including requirements for passwords.

Some policies suggest or impose requirements on what type of password a user can choose, such as:

- the use of both upper- and lower-case letters (case sensitivity)
- inclusion of one or more numerical digits

- Inclusion of special characters, e.g. @, #, $ etc.
- prohibition of words found in a dictionary or the user's personal information
- prohibition of passwords that match the format of calendar dates, license plate numbers, telephone numbers, or other common numbers
- prohibition of use of company name or an abbreviation
- An Environ password, of the following form: consonant, vowel, consonant, consonant, vowel, consonant, number, number (for example *pinray45*). A disadvantage of this 8-character password is known to potential attackers, the number of possibilities that need to be tested is less than a 6-character password of no form (486,202,500 vs 2,176,782,336).

4.2.2. Common Password Practice

Password policies often include advice on proper password management such as:

- never share a computer account
- never use the same password for more than one account
- never tell a password to anyone, including people who claim to be from customer service or security
- never write down a password
- never communicate a password by telephone, e-mail or instant messaging
- being careful to log off before leaving a computer unattended
- changing passwords whenever there is suspicion they may have been compromised
- operating system password and application passwords are different
- password should be alpha-numeric

4.2.3. Types of Password

Before you will be able to change, clear or remove a computer password, you must first determine the password type that is being used.

- ***System Password*****: -** Does the password appear as the computer is booting? If yes, this is a BIOS or CMOS password. BIOS or CMOS passwords will not allow the computer to be boot at all unless the password is known.
- ***Operating System /Network/ Third-Party Password*****: -** Does the password appear after the computer is done booting and before the operating system runs? If yes, this is a network, Operating System, or third-party password.
- ***Window Password*****: -** Windows users, does the password appear in Windows before the desktop? If yes, this is a Windows or Windows network password. If you are able to press the Escape key and get to Windows, you have a standard Windows password; however, if this does

not bypass the password prompt, it is likely you have a Windows network password.

4.2.4. Enforce Password History in Group Policy Editor

Computer administrators can use the Group Policy Editor to deploy all types of general policy settings. When the "Enforce password history" policy setting is enabled, Windows keeps a record of a specified number of prior user account passwords. When users change their account password, they are prohibited from re-using any of the passwords still in the Windows memory. This policy helps to enhance computer security. By default, the "Enforce password history" policy is set to "0," which means no prior passwords are remembered. To enable the "Enforce password history" policy, the setting has to be a value greater than 0.

4.2.5. Assign Minimum and Maximum Password Age

4.2.5.1. Minimum Password Age

The minimum password age must be less than the Maximum password age, unless the maximum password age is set to 0, indicating that passwords will never expire. If the maximum password age is set to 0, the minimum password age can be set to any value between 0 and 998.

Configure the minimum password age to be more than 0 if you want Enforce password history to be effective. Without a minimum password age, users can cycle through passwords repeatedly until they get to an old favorite. The default setting does not follow this recommendation, so that an administrator can specify a password for a user and then require the user to change the administrator-defined password when the user logs on. If the password history is set to 0, the user does not have to choose a new password. For this reason, Enforce password history is set to 1 by default.

4.2.5.2. Maximum Password Age

This security setting determines the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. If the maximum password age is between 1 and 999 days, the Minimum password age must be less than the maximum password age. If the maximum password age is set to 0, the minimum password age can be any value between 0 and 998 days.

Note

- It is a security best practice to have passwords expires every 30 to 90 days, depending on your environment. This way, an attacker has a limited amount of time in which to crack a user's password and have access to your network resources

4.3. Password Complexity Requirements

This security setting determines whether passwords must meet complexity requirements. Complexity requirements are enforced when passwords are changed or created.

If this policy is enabled, passwords must meet the following minimum requirements when they are changed or created:

- Passwords must not contain the user's entire same account Name (Account Name) value or entire display Name (Full Name) value. Both checks are not case sensitive:
    - ✓ The same account Name is checked in its entirety only to determine whether it is part of the password. If the same account Name is less than three characters long, this check is skipped.
- The display Name is parsed for delimiters: commas, periods, dashes or hyphens, underscores, spaces, pound signs, and tabs. If any of these delimiters are found, the display Name is split and all parsed sections (tokens) are confirmed not to be included in the password.
- Passwords must contain characters from three of the following five categories:
    - ✓ Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
    - ✓ Lowercase characters of European languages (a through z, sharp-s, with diacritic marks, Greek and Cyrillic characters)
    - ✓ Base 10 digits (0 through 9)
    - ✓ None alphanumeric characters: ~! @#$%^&*_-+=`|\(){}[]:;"'<>,.?/
    - ✓ Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.

Self-Check - 4	**Written Test**

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. ______________________ is a string of characters that people can use *to log on to a computer* and access files, programs, and other resources. **(1 pts)**
2. In Windows, a password can include ______________, ______________, ______________, and ______________. **(4 pts)**
3. To help keep your computer *secure*, you should always create a ______________________. **(1 pts)**
4. ______________________ are typically longer than passwords, for added security, and contain *multiple words* that create a phrase. **(1 pts)**
5. When you create a password or passphrase, you should make it strong, which means **_____________________________________. (2 pts)**
6. Compare a strong password and a strong passphrase. **(3 pts)**

A strong password:	**A strong passphrase:**

7. Write the four categories of characters Strong passwords and passphrases contain: **(4 pts)**

____

____

____

____

8. ___________________ is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. **(1 pts)**

9. Write at least five advices on proper password management included in password policies. **(5 pts)**

____

____

____

____

____

10. Configure the _____________________ to be more than 0 if you want Enforce password history to be effective. **(1 pts)**
11. ______________________ security setting determines the period of time (in days) a password can be used before the system requires the user to change it. **(1 pts)**
12. ______________________ security setting determines whether passwords must meet complexity requirements. **(1 pts)**

Note: **Satisfactory rating - 13 points** **Unsatisfactory - below 13 points**

You can ask your teacher for the copy of the correct answers.

Answer Sheet

Score = ____________

Rating: ____________

Name: ________________________________ Date: ________________

Short Answer Questions

1. ______________________

2. _______________, _______________, _______________, and _______________

3. ______________________

4. ______________________

5. ____

6.

A strong password:	A strong passphrase:

7. ____

____

____

____

8. ______________________

9. ____

____

____

____

____

10.______________________

11.______________________

12.______________________

Information Sheet - 5	Accessing Information Services

5.1. Identify Security Gaps

5.1.1. Authenticating Users

Before a user can log on to a computer running Windows, connect to a shared folder, or browse a protected Web site, the resource must validate the user's identity using a process known as *authentication.*

Windows supports a variety of authentication techniques, including

- the traditional user name and password,
- smart cards, and
- third-party authentication components.

In addition, Windows can authenticate users with the local user database.

Authentication is the process of identifying a user. In home environments, authentication is often as simple as clicking a user name at the Windows 7 logon screen. However, in enterprise environments, almost all authentication requests require users to provide both a user name (to identify themselves) and a password (to prove that they really are the user they claim to be).

5.1.1.1. Smart Card

Windows 7 also supports authentication using a smart card. The smart card, which is about the size of a credit card, contains a chip with a certificate that uniquely identifies the user. So long as a user doesn't give the smart card to someone else, inserting the smart card into a computer sufficiently proves the user's identity. Typically, users also need to type a password or PIN to prove that they aren't using someone else's smart card. When you combine two forms of authentication (such as both typing a password and providing a smart card), it's called ***multifactor authentication***. Multifactor authentication is much more secure than single-factor authentication.

5.1.1.2. Biometrics

Biometrics is another popular form of authentication. Although a password proves your identity by testing "something you know" and a smart card tests "something you have," biometrics test "something you are" by examining a unique feature of your physiology. Today the most common biometric authentication mechanisms are fingerprint readers (now built into many mobile computers) and retinal scanners.

Biometrics is the most secure and reliable authentication method because you cannot lose or forget your authentication. However, it's also the least commonly used. Reliable biometric readers are too expensive for many organizations, and some users dislike biometric readers because they feel the devices violate their privacy.

5.1.2. Troubleshoot Authentication Issues

Sometimes, users might experience problems authenticating to resources that have more complex causes than mistyping a password or leaving the Caps Lock key on. The sections that follow describe troubleshooting techniques that can help you better isolate authentication problems.

UAC Compatibility Problems

Users often confuse authentication and authorization issues. This isn’t a surprise because both types of problems can show the exact same error message: “Access is denied.” Because UAC limits the user’s privileges and many applications were not designed to work with UAC, security errors are bound to be even more frequent in Windows Vista and Windows 7 than they were in Windows XP.

Most UAC-related problems are authorization-related, not authentication-related. If the user doesn’t receive a UAC prompt at all but still receives a security error, it’s definitely an authorization problem. If the user receives a UAC prompt and the user’s credentials are accepted (or if the user logs on as an administrator and only needs to click Continue), it’s definitely an authorization problem. UAC problems are authentication-related only if UAC prompts a user for credentials and rejects the user’s password.

5.2. Use Auditing to Troubleshoot Authentication Problems

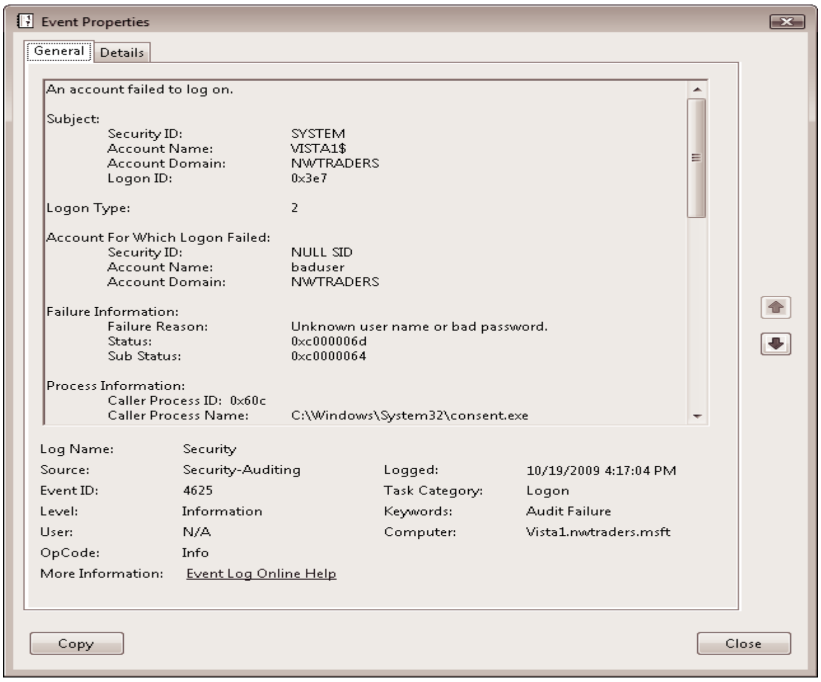
By default, Windows 7 does not add an event to the event log when a user provides incorrect credentials (such as when a user mistypes a password). Therefore, when troubleshooting authentication problems, your first step should be to enable auditing for logon events so that you can gather more information about the credentials the user provided and the resource being accessed.

Windows 7 (and earlier versions of Windows) provides two separate authentication auditing policies:

- **Audit Logon Events** This policy audits authentication attempts for local resources, such as a user logging on locally, elevating privileges using a UAC prompt, or connecting over the network (including connecting using Remote Desktop or connecting to a shared folder). All authentication attempts will be audited, regardless of whether the authentication attempt uses a domain account or a local user account.
- **Audit Account Logon Events** This policy audits domain authentications. No matter which computer the user authenticates to, these events appear only on the domain controller that handled the authentication request.

Typically, you do not need to enable auditing of account logon events when troubleshooting authentication issues on computers running Windows 7. However, successful auditing of these events is enabled for domain controllers by default.

Figure 5-1 shows an example of a logon audit failure that occurred when the user provided invalid credentials at a UAC prompt. Notice that the Caller Process Name (listed under Process Information) is Consent.exe, the UAC process.

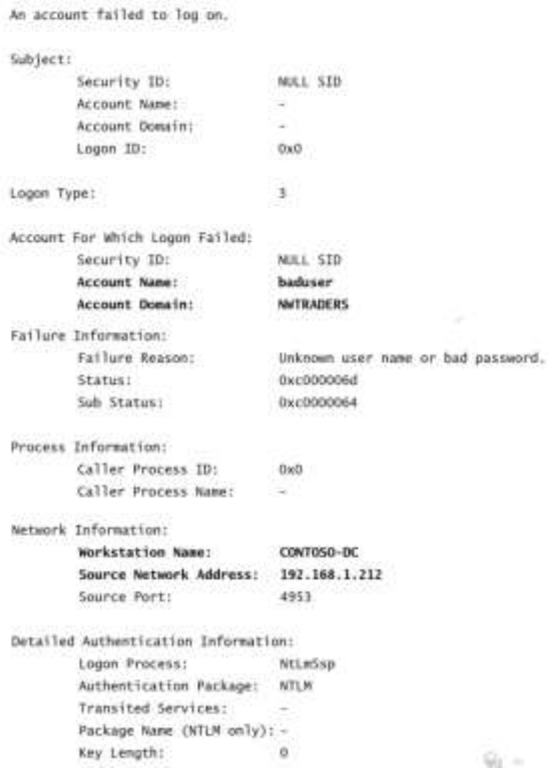


```
An account failed to log on.

Subject:
          Security ID:              SYSTEM
          Account Name:             VISTA1$
          Account Domain:           NWTRADERS
          Logon ID:                 0x3e7

Logon Type:                         2

Account For Which Logon Failed:
          Security ID:              NULL SID
          Account Name:             baduser
          Account Domain:           NWTRADERS

Failure Information:
          Failure Reason:           Unknown user name or bad password.
          Status:                   0xc000006d
          Sub Status:               0xc0000064

Process Information:
          Caller Process ID:  0x60c
          Caller Process Name:      C:\Windows\System32\consent.exe
```

```
Log Name:         Security
Source:           Security-Auditing       Logged:          10/19/2009 4:17:04 PM
Event ID:         4625                    Task Category:   Logon
Level:            Information             Keywords:        Audit Failure
User:             N/A                     Computer:        Vista1.nwtraders.msft
OpCode:           Info
More Information:  Event Log Online Help
```

FIGURE 5-1 A logon audit failure caused by invalid credentials

Audits from failed authentication attempts from across the network resemble the following code. In particular, the Account Name, Account Domain, Workstation Name, and Source Network Address are useful for identifying the origin computer.



```
An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           baduser
        Account Domain:         NWTRADERS
Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xc000006d
        Sub Status:             0xc0000064

Process Information:
        Caller Process ID:      0x0
        Caller Process Name:    -

Network Information:
        Workstation Name:       CONTOSO-DC
        Source Network Address: 192.168.1.212
        Source Port:            4953

Detailed Authentication Information:
        Logon Process:          NtLmSsp
        Authentication Package: NTLM
        Transited Services:     -
        Package Name (NTLM only): -
        Key Length:             0
```

When you are authenticating to network resources, authentication failures are always logged on the server, not on the client. For example, if you attempt to connect to a shared folder and you mistype the password, the event won't appear in your local event log—it appears instead in the event log of the computer sharing the folder.

Self-Check - 5	Written Test

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Before a user can log on to a computer running Windows 7, connect to a shared folder, or browse a protected Web site, the resource must validate the user's identity using a process known as _____________________. **(1 pts)**
2. Windows supports a variety of authentication techniques, including **(3 pts)**

   ____

   ____

   ____

3. ______________________ which is about the size of a credit card, contains a chip with a certificate that uniquely identifies the user. **(1 pts)**
4. When you combine two forms of authentication (such as both typing a password and providing a smart card), it's called ______________________.**(1 pts)**
5. ______________________ is the most secure and reliable authentication method because you cannot lose or forget your authentication. **(1 pts)**
6. When troubleshooting authentication problems, your first step should be to enable ______________________ so that you can gather more information about the credentials the user provided and the resource being accessed. **(1 pts)**
7. list and explain the two separate authentication auditing policies that Windows 7 (and earlier versions of Windows) provides. **(4 pts)**
   - ____

     ____

     ____

     ____
   - ____

     ____

     ____

     ____

***Note:* Satisfactory rating - 7 points   Unsatisfactory - below 7 points**

You can ask your teacher for the copy of the correctanswers.

Answer Sheet

Score = ___________

Rating: ___________

Name: ________________________________ Date: ________________

Short Answer Questions

1. ______________________

2. ____

____

____

3. ______________________

4. ______________________

5. ______________________

6. ______________________

7.

- ____

  ____

  ____

  ____

  ____

- ____

  ____

  ____

  ____

  ____

Operation Sheet - 1	Techniques of setting User Account Control

1.1. Create a User Account

1. Click on ***Start***, and then click on ***Control Panel***
2. Click on ***User Accounts***.
3. Click ***Manage Another Account***. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Click on ***Create a New Account***.
5. Type the ***name you want*** to give the user account, Click an ***account type***, and then click **Create Account**.

1.2. Change Picture for a User Account

1. Click on ***Start***, and then Click on ***Control Panel***
2. Click on ***User Accounts***.
3. Click ***Change your picture***.
4. Click the ***picture you want to use***, and then Click ***Change Picture***.
   - Or If you want to use a picture of your own, Click ***Browse*** for more pictures, navigate to the picture you want to use, Click ***the picture***, and then Click ***Open***. You can use a picture of any size, but it must have one of the following file name extensions: ***.jpg***, ***.png***, ***.bmp***, or ***.gif***.

1.3. Rename a User Account

1. Click on ***Start***, and then click on ***Control Panel***.
2. Click on ***User Accounts***.
3. Click ***Change your account name***. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Type the ***new name***, and then click ***Change Name***.

Notes

- You ***can't*** change the name of the ***guest account***.
- A username ***can't be longer than 20 characters***, consist entirely of periods or spaces, or contain any of these characters: \ / " [ ] : **|** < > + = ; , ? * @

1.4. Change a User's Account Type

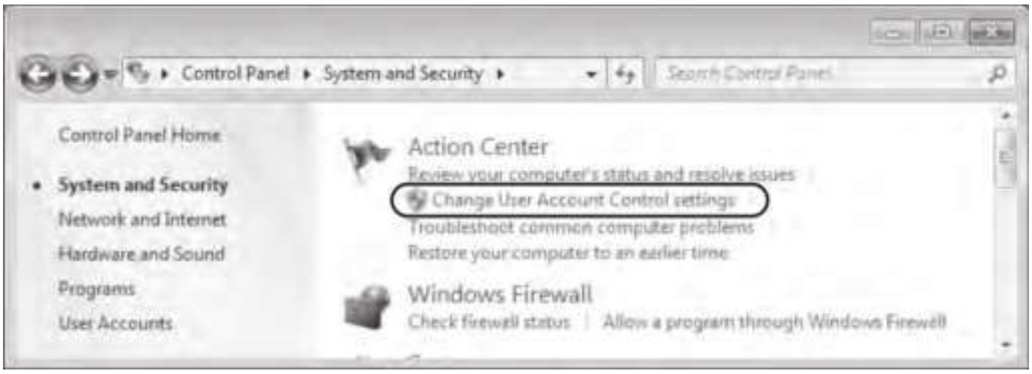
1. Click on ***Start***, and then click on ***Control Panel***
2. Click on ***User Accounts***.
3. Click ***Manage another account***. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Click the ***account you want to change***, and then click ***Change the account*** type.
5. Select the ***account type*** you want, and then click ***Change Account Type.***

Note: Windows requires at least one administrator account on a computer. If you have only one account on your computer, you can't change it to a standard account.

1.5. Configuring UAC in Control Panel

To configure UAC in Control Panel, perform the following steps:

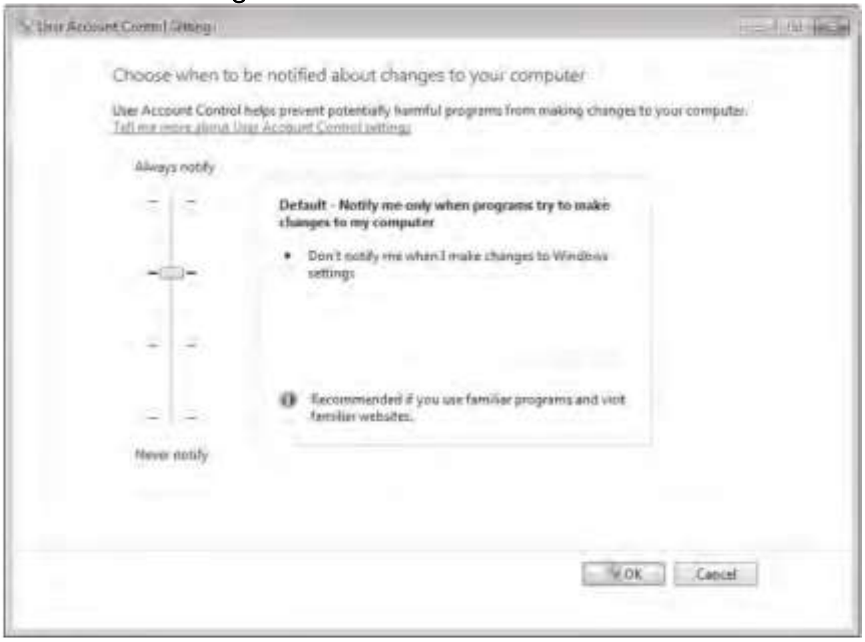
1. In ***Control Panel***, click ***System and Security***.
2. Under ***Action Center***, click ***Change User Account Control Settings***, as shown in Figure 1.5-1.



Control Panel ▸ System and Security ▸
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Action Center
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Restore your computer to an earlier time
Windows Firewall
Check firewall status
Allow a program through Windows Firewall

FIGURE 1.5-1 You can access UAC settings through the Action Center

This step opens the User Account Settings window, one version of which is shown in Figure 5. Note that the set of options that appears is different for administrators and standard users, and that each user type has a different default setting.



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.

Tell me more about User Account Control settings

Default - Notify me only when programs try to make changes to my computer

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar programs and visit familiar websites.

FIGURE 1.5-2 UAC allows you to choose among four notification levels.

3. Choose one of the following notification levels:
   - **Always Notify** This level is the default for standard users, and it configures UAC to act as it does in Windows Vista. At this level, users are notified whenever any changes that require administrator privileges are attempted on the system.

- **Notify Me Only When Programs Try To Make Changes To My Computer** This level is the default for administrators and is not available for standard users. At this level, administrators are not notified when they make changes that require administrator privileges. However, users are notified through consent prompt when a program requests elevation.
- **Always Notify Me (And Do Not Dim My Desktop)** This level is not available for administrators*.* It is similar to the default setting for standard users, except that at this particular level, the Secure Desktop is never displayed. Disabling the Secure Desktop tends to reduce protection against malware, but it improves the user experience. This setting might be suitable for standard users who very frequently need to request elevation.
- **Notify Me Only When Programs Try To Make Changes To My Computer (Do Not Dim The Desktop)** This level is available for both standard users and administrators. At this level, the behavior is the same as with the default administrator level ("Notify me only when programs try to make changes to my computer"), but with this option the Secure Desktop is not displayed.
- **Never Notify** This level disables notifications in UAC. Users are not notified of any changes made to Windows settings or when software is installed. This option is appropriate only when you need to use programs that are incompatible with UAC.

4. Click ***OK***.

Operation Sheet - 2	Configuring User Account

2.1. Add a User Account to a Group

By adding a ***user account*** to a ***group***, you can avoid having to grant the same access and ***permission*** to many different users one by one. Members of a group can make the same types of changes to settings and have the same access to folders, printers, and other network services.

1. Click on ***Start***, and then click on ***Control Panel***
2. Click on ***Administrative Tools*** and then Double-click on ***Computer Management***. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. In the ***left pane of Computer Management***, click ***Local Users and Groups***.
4. Click on ***Groups folder***.
5. Right-click the ***group you want to add the user account to***, and then click ***Add to Group***.
6. Click ***Add***, and then type ***the name of the user account***.
7. Click ***Check Names***, click ***OK***.
8. Click ***Apply***, and then click ***OK***.

Note

- To help make your computer more secure, add a user to the Administrators group only if it is absolutely necessary. Users in the Administrators group have complete control of the computer. They can see everyone's files, change anyone's password, and install any software they want.

2.2. Remove a User Account from a Group

1. Click on ***Start***, and then click on ***Control Panel***
2. Click on ***Administrative Tools*** and then Double-click on ***Computer Management***. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. In the ***left pane of Computer Management***, click ***Local Users and Groups***.
4. Click on ***Groups folder***.
5. Right-click the ***group you want to remove the user account from***, and then click ***Properties***.
6. Select ***the name of the user account*** and then Click ***Remove.***

7. Click ***Apply***, and then click ***OK***.

2.3. Disable a User Account

If you have a user account that you want to make unavailable, you can disable it. A disabled account can be enabled again later. Disabling an account is different from deleting an account. If you delete an account, it can't be restored.

1. Click on ***Start***, and then click on ***Control Panel***
2. Click on ***Administrative Tools*** and then Double-click on ***Computer Management***. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
3. In the ***left pane of Computer Management***, click ***Local Users and Groups***.
5. Click on ***Users folder***.
6. Right-click the ***user account you want to disable***, and then click ***Properties***.
7. On the General tab, ***select the Account is disabled check box***, and then Click ***OK***.

Note

- To enable a disabled account, follow the same steps as you would for disabling an account, but clear the Account is disabled check box.

2.4. Delete a User Account

If you have a user account on your computer that is not being used, you can permanently remove it by deleting it. When you delete a user account, you can choose whether you want to keep the files created under that account; however, e-mail messages and computer settings for the account will be deleted.

1. Click on ***Start***, and then click on ***Control Panel***
2. Click on ***User Accounts***.
3. Click ***Manage another account***. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
4. Click the ***account you want to delete***, and then click ***Delete the account***.
5. ***Decide*** if you want to ***keep*** or ***delete the files*** created under the account by clicking ***Keep Files*** or ***Delete Files***.
6. Click ***Delete Account***.

Operation Sheet - 3	Techniques to Access Information Services

3.1. Enable Audit Logon Events

To log failed authentication attempts, you must enable auditing by following these steps:

1. Click Start and then click Control Panel. Click System and Security. Click Administrative Tools, and then double-click Local Security Policy.
2. In the Local Security Policy console, expand Local Policies, and then select Audit Policy.
3. In the right pane, double-click Audit Logon Events.
4. In the Audit Logon Events Properties dialog box, select the Failure check box to add an event to the Security event log each time a user provides invalid credentials. If you also want to log successful authentication attempts (which include authentication attempts from services and other nonuser entities), select the Success check box.
5. Click OK.
6. Restart your computer to apply the changes.

3.2. View Audit Logon Events

With auditing enabled, you can view audit events in Event Viewer by following these steps:

1. Click Start, right-click Computer, and then click Manage.
2. Expand System Tools, Event Viewer, Windows Logs, and then select Security.
3. Event Viewer displays all security events. To view only successful logons, click the Filter Current Log link in the Actions pane and show only Event ID 4624. To view only unsuccessful logon attempts, click the Filter Current Log link and show only Event ID 4625.

LAP Test	Practical Demonstration

Name: ______________________________ Date: ________________

Time started: ________________________ Time finished: ________________

Instructions: Given necessary templates, tools and materials you are required to perform the following tasks within 4 hour.

Task 1. User Account Control

1.1. Create the following User Accounts

1.1.1. An Administrator Account

A. Make the Username “Admin1”

B. Make the password “Admin@123”

C. Make the Account picture any picture you want

1.1.2. An Administrator Account

A. Make the Username “Admin2”

B. Make the password “Admin@321”

C. Make the Account picture different picture you want

1.1.3. A Standard Account

D. Make the Username “Stand1”

E. Make the password “Stand@123”

F. Make the Account picture different picture you want

1.1.4. Another Standard Account

A. Make the Username “Stand2”

B. Make the password “Stand@210”

C. Make the Account picture different picture you want

1.1.5. Turn on the Guest Account

1.2. Rename a User Account with

- “Stand2” username to “Stand2Admin”
- “Admin1” username to “Admin2Stand”

1.3. Change a User's Account Type

- “Stand2Admin” to “Administrator Account”
- “Admin2Stand” to “Standard Account”

1.4. Change User Account Control

- Change Notification Level to “**Always Notify**”

Task 2. Configuring User Account

2.1. Disable the User Account with

- “Stand2Admin” username
- “Admin2Stand” username

2.2. Delete the User Account with

- “Stand1” username

2.3. Enable the User Account with

- “Stand2Admin” username
- “Admin2Stand” username

2.4. Add the User Account with

- “Admin2Stand” username to “Administrator” Group
- “Stand2Admin” username to “Users” Group

Task 3. Accessing Information Services

3.1. Enable Audit Logon Events

3.2. View Audit Logon Events

List of Reference Materials

MCITP Exam 70-685: Windows 7 Enterprise Desktop Support Technician, Tony Northrup and J.C. Mackin

https://www.sitepoint.com/5-steps-to-uncovering-your-it-security-gaps/

https://en.wikibooks.org/wiki/Fundamentals_of_Information_Systems_Security/Access_Control_Systems#Access_Control_Assurance

https://en.wikipedia.org/wiki/Computer_access_control

https://en.wikibooks.org/wiki/Category:Book:Fundamentals_of_Information_Systems_Security

https://www.computerweekly.com/opinion/Identify-security-gaps