Unit 8 : User Administration, Security System and Facilities

A user account defines the actions a user can perform in Windows. On a stand-alone computer or a computer that is a member of a workgroup, a user account establishes the privileges assigned to each user. On a computer that is part of a network domain, a user must be a member of at least one group. The permissions and rights granted to a group are assigned to its members.

Lesson 1 : User Administration in Windows

1.1. Learning Objectives

On completion of this lesson you will be able to describe:

- Types and access facilities of users.
- Creation, password setting and delete of users.

1.2. Introduction

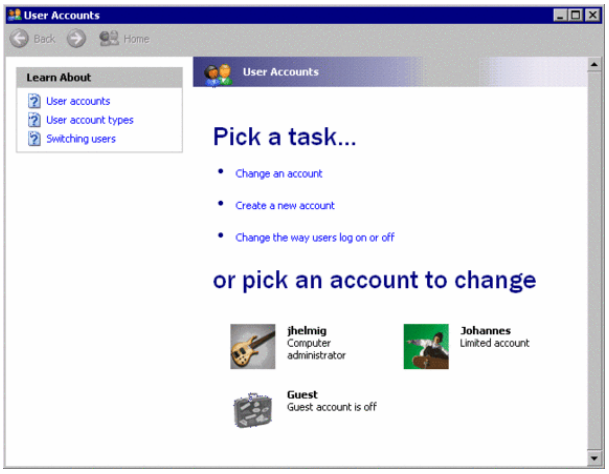
User Accounts allows you to add users to your computer and to add users to a group In Windows, permissions and user rights usually are granted to groups. By adding a user to a group, you give the user all the permissions and user rights assigned to that group.

1.3. User Management in Windows XP

User Management in Windows XP

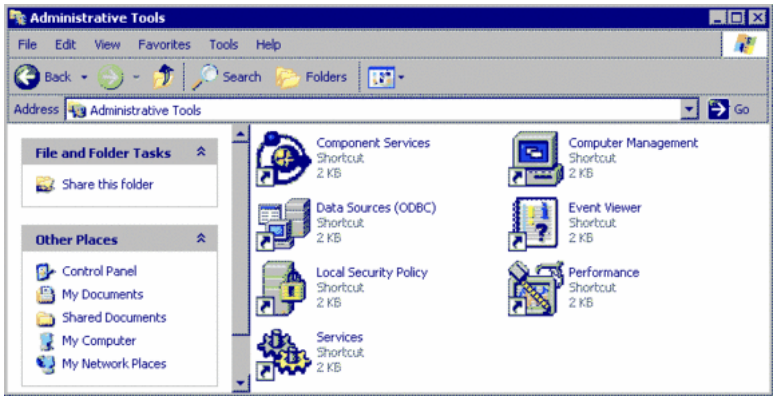
Windows XP Professional Edition is the replacement for Windows NT4 and Windows 2000, and offers therefore the same level of User Management and security as Windows NT4 and Windows2000.

Step 1: You have a choice: You can keep it simple with just 2 levels of Security and use in the Control-Panel: "User Accounts": 



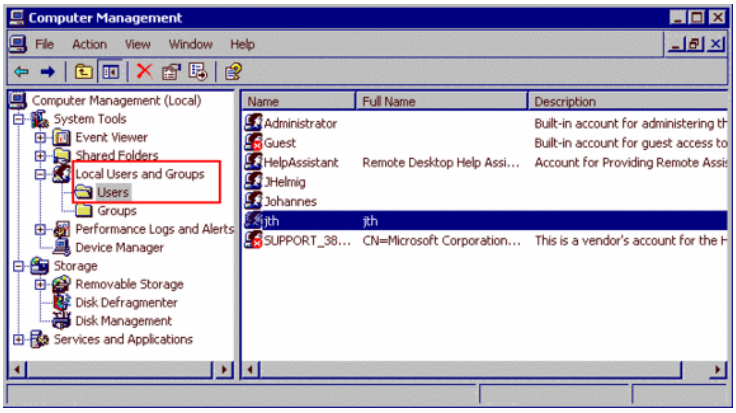
This is the simplified user management as in the Windows XP Home Edition, allowing
the definition of Users and Password.

Step 2: To be able to use all feature of the Windows XP Professional User management,
select in the Control-panel: "***Administrative Tools***":



User Management is part of "***Computer Management***":

Step 3: Select in the tree-view on the left: System Tools / Local Users and Groups / Users:



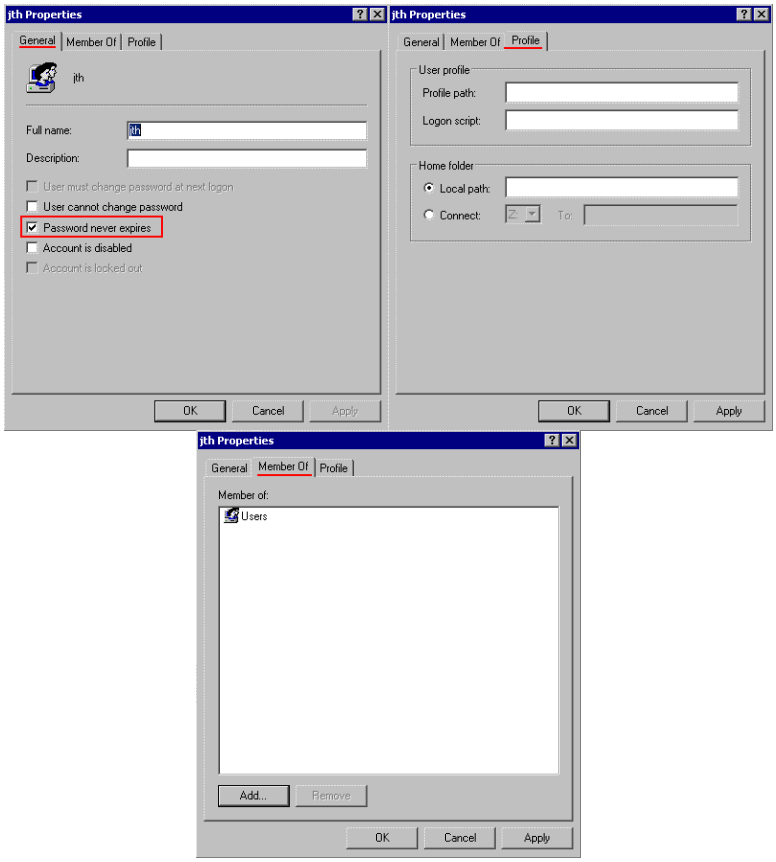
Step 4: Double click on a Username to display Details:

Tab: General

The security system of Windows XP Professional defines in the policies the enforcement of password. To avoid to be forced by your computer to have to change the password, you can select here that the "Password never expires".

Tab: Profile

You can create a Logon script (list of commands to be executed) to be run when you logon to your system.

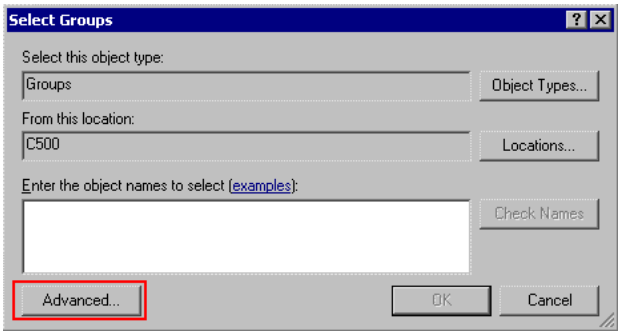


Tab: Member of

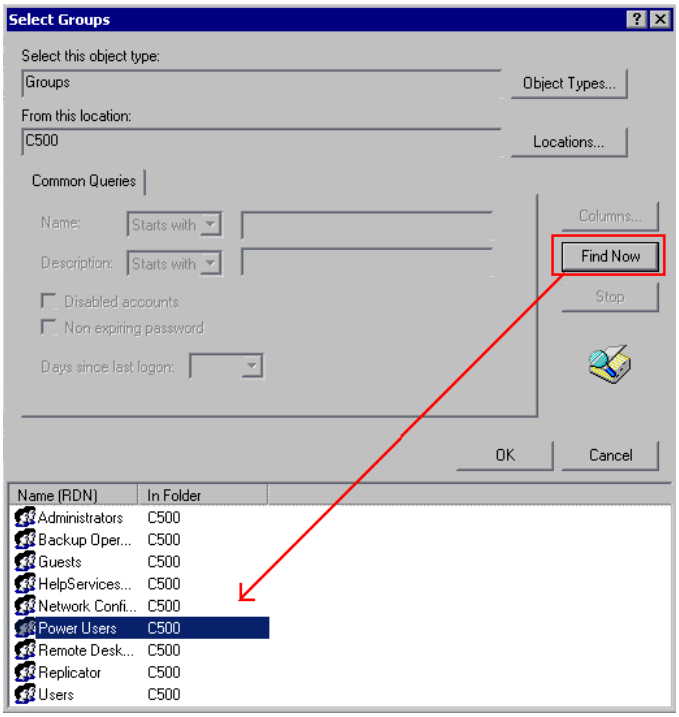
When Windows XP Professional is installed, a predefined set of user groups, each with different level of permissions, is installed on your system. By being a member of a user-group, a user has the permissions as defined for the group. A user can be member of MULTIPLE groups, getting the permission of each user group. All Users are automatically member of theusergroup "***Everyone***", which is NOT listed here. Therefore, if there is for a user NO Usergroup listed, then this user is still allowed all items, which are defined for the usergroup "Everyone"

To become member of an additional usergroup (to get additional permissions), click on the button "Add.."

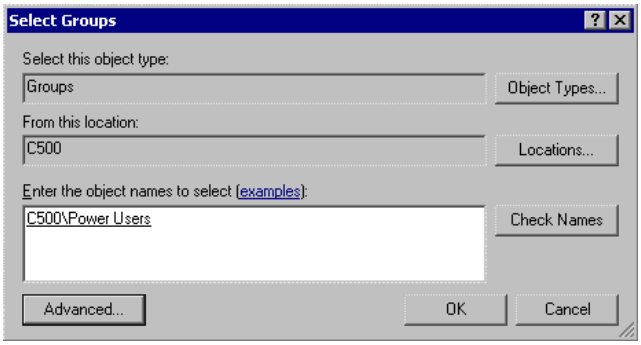
If you know the name of the usergroup, you can enter it, otherwise use the button "Advanced..." to get a Lookup.



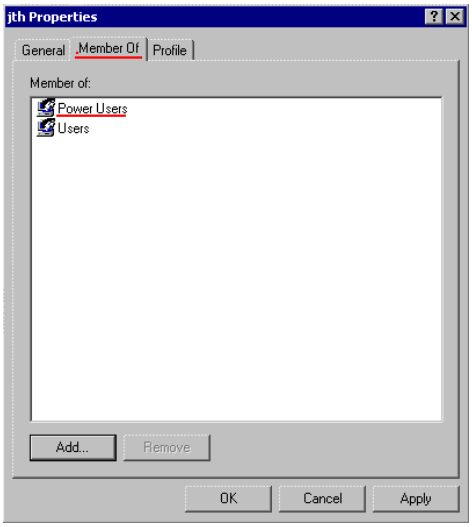
When working on a large network, you would have a very long list of items, so you can define here first a search criterion. For home use and small networks, just click on "Find Now" to get the display of Usergroups. Select the one to be added. To know, what permissionsare assigned to a Usergroup, see the Local Policies.



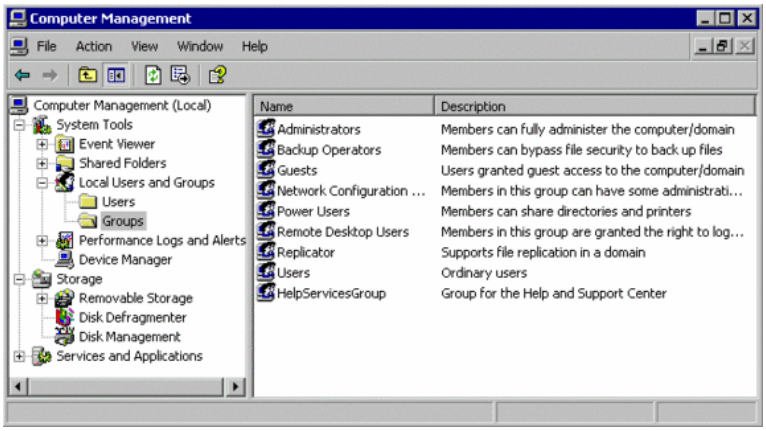
The full name of a usergroup includes the name of the computer, where the usergroup is defined.



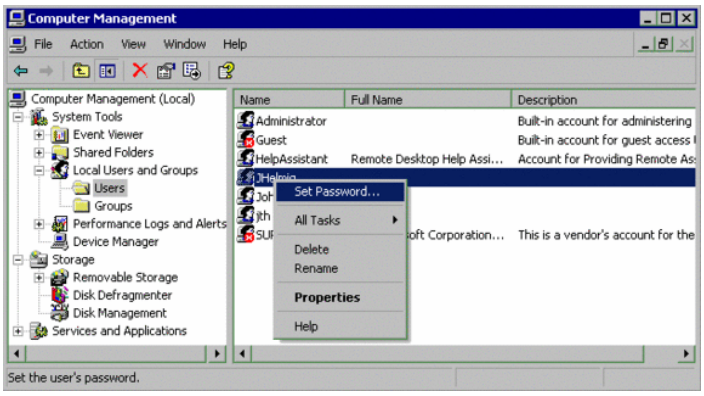
This user is now member of 2 Usergroups, having now the combined permissions of bothusergroups.



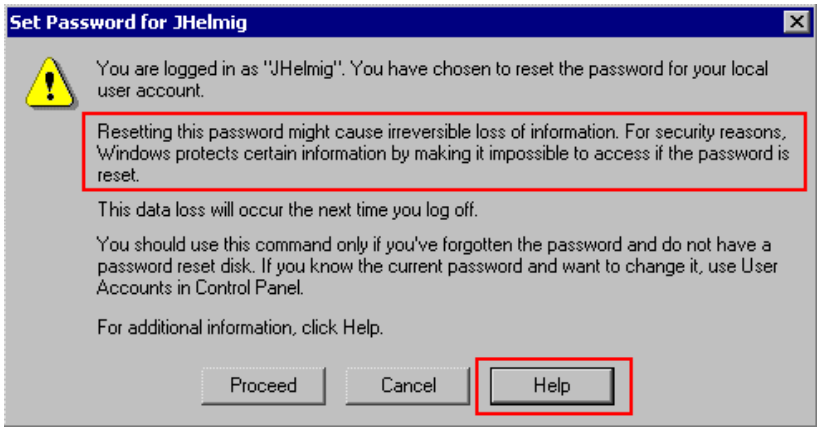
The installation of Windows XP Professional has created a predefined set of User groups,with different levels of permissions:



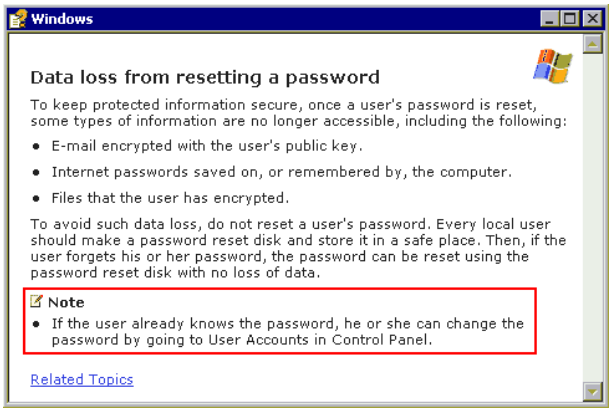
A special word of warning: it is possible to set the password for a user from Computer Management: select a Username and right-click to get the Context/Popup menu and
select: "***Set Password***":



But this feature seems to be reserved for cases, where a user has forgotten the password andthe administrator needs to define a new password.



This warning is displayed: "*Resetting this password might cause irreversible loss of information. For security reasons, Windows protects certain information by making it impossible to access if the password is reset*". Let's check for more information by selecting/clicking on the Button "Help":



If a user-account has NO password, or you like to change it, please use in the Control Panel the ***User Accounts"*** to change passwords.

1.4. Manage Users in Windows 7

Manage Users in Windows 7

A computer running Windows 7 might be used by a single person, by a group of people in an office, or by a family in a home. Fortunately, Windows 7 was designed from the ground up to be a multiuser operating system. The new OS is flexible and can support many different scenarios, with each user having appropriate permissions and a customized environment. Every person using Windows 7 must log in with an account, and each account has a personalized desktop, Start menu, documents folder, history, favorites, and other customizations.

1.4.1 Account Types

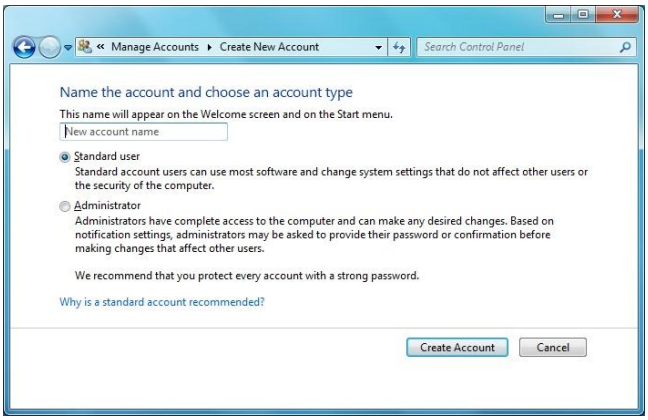
Before you start creating new users on your Windows 7 computer, you should understand the difference between the two main account types.
Administrators have full control over the system. They can install software programs and hardware drivers, and they can create and modify new users and groups. Additionally, they can reset passwords, set policies, and edit the Registry. The OS identifies tasks that require administrator permissions with a Windows security icon.
Standard users are permitted to log on to the computer, run programs, customize their accounts, and save files in their user folders. Users are restricted from making system wide changes.

1.4.2 The First User

When Windows first installs, it asks you for a user name and password, which it then uses to create your first account. This account joins the Administrators group, which has the highest set of privileges. From this account you can create and manage all other user accounts. When one person is the sole user of a computer, this first account is sometimes the only one ever created. However, even if you are the only user, a recommended practice is to create a second, standard account for daily use, so that you have it separate from your account with administrative privileges for managing the system. If you want to install software or make other system changes while logged in as a standard user, never fear: When you attempt to make the change, Windows will prompt you to authenticate your administrator account so that you won't need to log on with it.

1.4.3 Creating a New Account

To create a new account, open Control Panel and choose *User Accounts and Family Safety, Add or remove user accounts*. Click on *Create a new account*. Type in the new account name, select either the *Administrators* or *Standard Users* user type, and then click *Create Account*. By default, Windows assigns no password; you can make one by clicking on that user's icon and selecting *Create a password*. Alternatively, you can leave it blank to allow the user to set a password when they first log on.



1.4.4 Editing Accounts

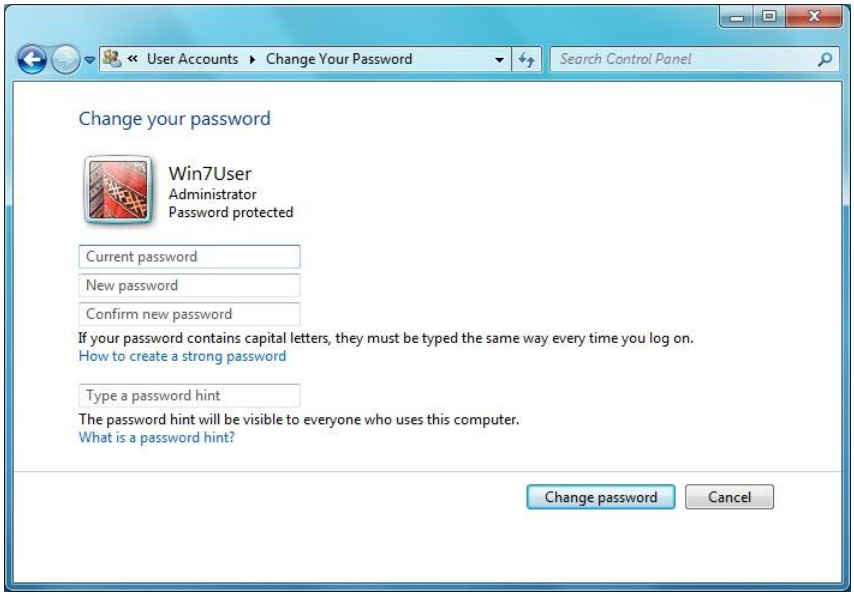
Once you've created an account, you can customize it further by editing. To edit an account, open Control Panel once again and select *User Accounts and Family Safety*, *Add or remove user accounts*. This takes you to the Manage Accounts window, where you can select an account to edit by clicking on its icon. In this window, you can change the account name, create or remove a password, change the picture, set up parental controls, change the account type, or delete the account.

1.4.5 If You Accidentally Delete Your Last Administrator Account

Windows 7 has a built-in Administrator account that has no password and is hidden by default. Like all other administrator accounts, it has full control of the system; for you to use it, however, it must be the only remaining administrator account, and you must start the computer in Safe Mode.

1.4.6 Changing Your Password

The simplest way to change your password when you are logged in is to press Ctrl-Alt-Del and click *Change a Password*. In this window, you simply type in your old password and your new one, and then confirm it. Administrators may also overwrite the user name and change the password for another user.



1.5. Exercise

1.5.1. Multiple choice questions

a. Windows XP Professional Edition is the replacement for

(i) Windows NT4
(ii) Windows 2000
(iii) Both (i) and (ii)
(iv) None of the above

b. To avoid to be forced by your computer to have to change the password, you can select

(i) Password never expires
(ii) User cannot change password
(iii) Account is disabled
(iv) All the above

c. How many account types are available in Windows 7?

(i) Three
(ii) Zero
(iii) One
(iv) Two

1.5.2. Questions for short answers

a. Explain the account types in Windows 7.
b. What is Guest Account?

1.5.3. Analytical question

a. Explain the process of "creating a new Account".

Lesson 2 : Security System and Facilities in Windows

2.1. Learning Objectives

On completion of this lesson you will be able to describe:

- Threads in PCs.
- Use and configuration of Microsoft Security Essentials.

2.2. Introduction

Hosts running Windows account for the majority of break-ins are due to the following, mostly preventable, causes:

- Viruses
- Weak passwords for users and applications
- Open shares
- Unpatched or poorly configured software

For each of these causes, there are a few simple steps that you can take to make your PC more secure:

- Use an anti-virus program & beware of attachments.
- Set good passwords for accounts and applications.
- Don't have open shares on your PC.
- Regularly patch operating system & application software.

2.3. Microsoft Security Essentials

Security

Microsoft Security Essentials (MSE) is an antivirus software (AV) product that provides protection against different types of malware such as computer viruses, spyware, rootkits and Trojan horses. It runs on Windows XP, Windows Vista and Windows 7, but not on Windows 8, which has a built-in AV component. The license agreement allows home users and small businesses to install and use the product free of charge. It replaces Windows Live OneCare, a discontinued commercial subscription-based AV service, and the free Windows Defender, which until Windows 8 only protected users from adware and spyware.
Microsoft Security Essentials includes the following new features and enhancements to better help protect your PC from threats:

- **Windows Firewall integration.** You can turn Windows Firewall on or off using Microsoft Security Essentials. Windows Firewall can help prevent attackers or malicious software from gaining access to your PC.
- **Network inspection system.** This feature enhances real-time protection by inspecting network traffic to help block exploitation of known network-based vulnerabilities.

- **New and improved protection engine.** The updated engine offers enhanced detection and cleanup capabilities with better performance.

2.4. Started with Microsoft Security Essentials

There's not much to do. Microsoft Security Essentials works in the background to protect your PC. It checks for updates automatically a few times a day and doesn't slow your PC down while it works.

2.4.1 Simple color-coding, simple actions

You can keep track of how your PC is doing by looking at the Microsoft Security Essentials icon in the notification area at the far right of the taskbar. Green means everything is okay, yellow means that your PC is potentially unprotected, and red means that your computer is at risk.
When you see yellow or red, click the icon and you'll be able to see the details and take actions. Usually the best thing to do is to choose **Clean computer** so that the threat can be removed. If you want to delete threats automatically whenever they are identified, open Microsoft Security Essentials, click the **Settings**tab and then choose **Default actions**.

2.4.2 Scanning right now

Open Microsoft Security Essentials and you'll be on the **Home** tab. You can select a **Quick** scan or a **Full** scan (and then click**Scan now**).
The quick scan will look for viruses in all the places they are most likely to hide. It's a good choice when you're just checking on the health of your PC.
But if something makes you think your PC is infected with a virus or spyware, we recommend a full scan. Your computer will be a little slower while it is running, but the full scan looks everywhere for possible problems.

2.4.3 Scheduling scans

By default, Microsoft Security Essentials runs a scan of your PC once a week when you're probably asleep (2:00 am on Sunday).
If you want to adjust this, open Microsoft Security Essentials and click the **Settings** tab. Under **Scheduled scan**, you'll be able to change the day and time as well as the type of scan.

2.4.4 Scanning more than just your hard drive

It may be useful to scan external drives and USB drives since they can get infected too.
Open Microsoft Security Essentials and click the **Settings** tab. Go to **Advanced** and click the option to **Scan removable drives**. Whenever scans run, your removable

drives will also be scanned (if they're attached to your PC). If you want to run a scan right away, go back to the **Home** tab and click **Scan now**.

2.5. What should I do if Microsoft Security Essentials detects malicious software on my PC?

If Microsoft Security Essentials detects malicious software or potentially unwanted software on your PC (either when monitoring your PC using real-time protection or after running a scan), it notifies you about the detected item by displaying a message in the notification area to the right of the taskbar.
In some cases, Microsoft Security Essentials takes automatic action to remove malicious software from your PC, and will notify you that it is doing so. In other cases, Microsoft Security Essentials will show you a notification that malicious or potentially unwanted software has been detected. Click **Clean computer** to remove the software, or click **Show details** to open the **Potential threat details window** and get additional information about the detected item. Depending on the alert level, you can choose one of the following actions to apply to the detected item:
Remove – This action permanently deletes the software from your PC.
Quarantine – This action quarantines the software so that it can't run. When Microsoft Security Essentials quarantines software, it moves it to another location on your PC, and then prevents the software from running until you choose to restore it or remove it.
Allow – This action adds the software to the Microsoft Security Essentials allowed list and allows it to run on your PC. Microsoft Security Essentials will stop alerting you to risks that the software might pose to your privacy or to your PC.
Caution:
If you choose **Allow** for an item, such as software, Microsoft Security Essentials will stop alerting you to risks that the software might pose to your privacy or to your PC. Therefore, add software to the allowed list only if you trust the software and the software publisher.

2.6. Exercise

2.6.1. Multiple choice questions

a. Microsoft's announcement of its own Anti-Virus software on
(i) 18 November 2007
(ii) 18 November 2008
(iii) 18 October 2007
(iv) 18 November 2008

b. Microsoft Security Essentials does not run automatically on
(i) Windows XP
(ii) Windows 7
(iii) Windows Vista
(iv) Windows 8

c. By default, Microsoft Security Essentials runs a scan of your PC once a week at
(i) 3:00 am on Sunday
(ii) 2:00 am on Saturday
(iii) 2:00 am on Sunday
(iv) 2:00 am on Friday

d. "Which of the following can help prevent attackers or malicious software from gaining access to your PC?

(i) Windows Firewall
(ii) Network inspection system
(iii) Protection Engine
(iv) All the above

2.6.2. Questions for short answers

a. What is Microsoft Security Essentials?

2.6.3. Analytical question

a) What should it be done if Microsoft Security Essentials detects malicious software on a PC? – Explain.

Lesson 3 : System Access Control

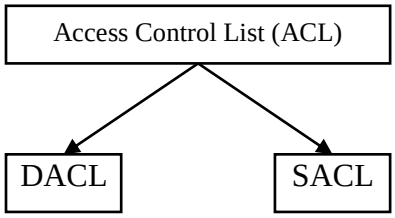
3.1. Learning Objectives

On completion of this lesson you will be able to describe:

- ❖ Definition and types of Access Control List.

3.2. Introduction

Earlier version of Windows (Windows 95, Windows 98, Windows ME) are all running as a single user desktop operating system and thus access control is unnecessary. However, start from Windows NT, following with Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, and Windows Server 2008, are all use a system of access control lists (ACLs). Windows resources, including files, registry, synchronization primitives (e.g. mutexes, events), IPC mechanisms (e.g. name pipes, mailslots), are all accessed through objects which may be secured using ACLs.



Access Control List Model

There are 2 types of ACLs in Windows: DACL and SACL. Discretionary Access Control list (DACL).

3.3. Discretionary Access Control List

A discretionary access control list (DACL) identifies the trustees that are allowed or denied access to a securable object. When a process tries to access a securable object, the system checks the ACEs in the object's DACL to determine whether to grant access to it. If the object does not have a DACL, the system grants full access to everyone. If the object's DACL has no ACEs, the system denies all attempts to access the object because the DACL does not allow any access rights. The system checks the ACEs in sequence until it finds one or more ACEs that allow all the requested access rights, or until any of the requested access rights are denied.

3.4. System Access Control List

Access Control List

A system access control list (SACL) enables administrators to log attempts to access a secured object. Each ACE specifies the types of access attempts by a specified

trustee that cause the system to generate a record in the security event log. An ACE in a SACL can generate audit records when an access attempt fails, when it succeeds, or both.
An ACL that controls the generation of audit messages for attempts to access a securable object. The ability to get or set an object's SACL is controlled by a privilege typically held only by system administrators.

3.5. SACL Access Right

The ACCESS_SYSTEM_SECURITY access right controls the ability to get or set the SACL in an object's security descriptor. The system grants this access right only if the SE_SECURITY_NAME privilege is enabled in the access token of the requesting thread.

3.5.1 To access an object's SACL

1. Call the AdjustTokenPrivileges function to enable the SE_SECURITY_NAME privilege.
2. Request the ACCESS_SYSTEM_SECURITY access right when you open a handle to the object.
3. Get or set the object's SACL by using a function such as GetSecurityInfoorSetSecurityInfo.
4. Call AdjustTokenPrivileges to disable the SE_SECURITY_NAME privilege.

To access a SACL using the GetNamedSecurityInfo or SetNamedSecurityInfo functions, enable the SE_SECURITY_NAME privilege. The function internally requests the access right.

The ACCESS_SYSTEM_SECURITY access right is not valid in a DACL because DACLs do not control access to a SACL. However, you can use the ACCESS_SYSTEM_SECURITY access right in a SACL to audit attempts to use the access right.

3.6. Exercise

3.6.1. Multiple choice questions

a. How many types of ACLs are in Windows?

(i) Three
(ii) Four
(iii) Two
(iv) One

b. SACL stands for

(i) SecureAccess Control List
(ii) System Access Control List
(iii) System Access ConfigurationList
(iv) SecureAccess ConfigurationList

3.6.2. Questions for short answers

a) What is Access Control List?

3.6.3. Analytical questions

a) Describe the SACL access right.

Lesson 4 : Managing User Accounts

4.1 Learning Objectives

On completion of this lesson you will be able to describe:

- Different ways of managing user accounts.
- User Accounts management in different version of Windows.

4.2. Introduction

Windows gives you two different ways to manage users on a machine. For either of these methods to work, you must be logged on as an administrator.

4.3. Managing User Accounts Using Windows XP

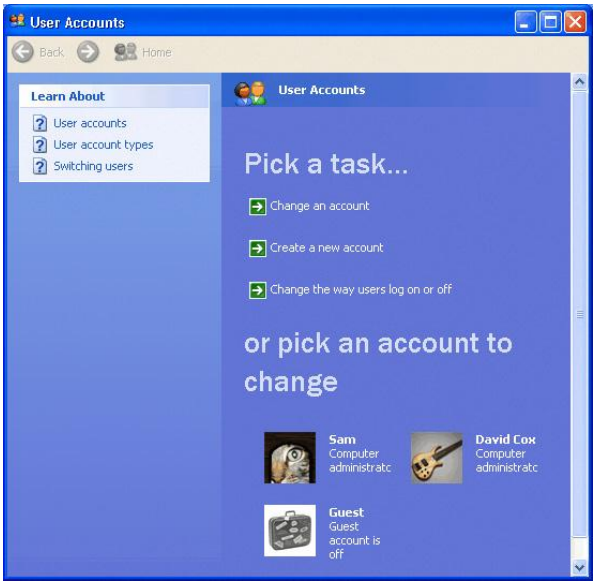
A user is someone who uses a computer. A user account defines what a user can do using Windows XP. In Windows XP, there are three types of user accounts.

Types of user accounts

- **Administrator account.** The administrator can do everything with the computer and can go anything he or she desires - essentially giving them control over the entire computer, including other accounts. The administrator account can never be disabled or deleted.
- **Standard account.** Users with standard accounts can install programs and hardware, change pictures and related personal data, and create, change, or remove his or her password.
- **Guest account.** The guest account doesn't require a password, can't add or remove programs from the computer, and is disabled by default. This account type is great for kids or students.

  Steps for managing user accounts in windows XP are as follows:
  To easily manage user accounts, click the **User Accounts** icon in the Control Panel.

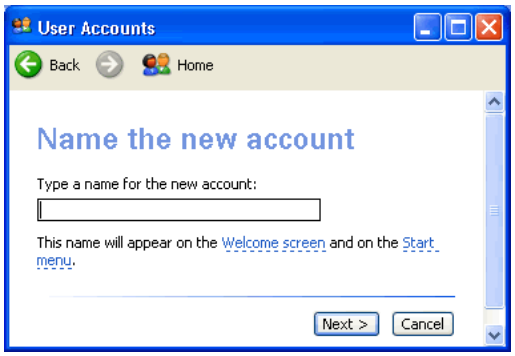
The **User Accounts** window presents you with an easy-to-use interface.



4.3.1 Creating a New Account

You can **create new user accounts** as needed, giving others access to your computer (without sharing your password).
To create a new account:

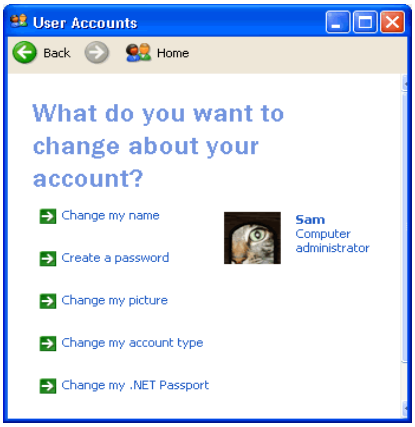
1. Click **Create a New Account** in the **User Accounts** window.
2. A **User Accounts** window appears. Enter the **name** of the new account and click **Next**.
3. The next window asks you to pick an account type. Choose **Computer Administrator** or **Limited** by clicking the appropriate radio button.
4. If you're not sure, click each one and read the list of actions that can be performed by the account type.
5. When finished, click the **Create Account** button.
6. The **new account** now appears in the **User Account** window.



4.3.2 Changing An Account

Any account can be easily **edited** or **changed** from the **User Accounts** window.
To change an existing user account:

1. Click **Change an Account** in the **User Accounts** window.
2. A window appears asking you which account you want to change.
3. The next window (figure below) allows you to change the name on the account, change the picture, change the account type, create a password, or delete the account. Make necessary changes.
4. Use the **Back** button to return to the original list to make any additional changes.



Note: Passwords provide security and prevent unauthorized users from logging in using someone else's user account. For more information on passwords, see our Internet Basics course.

4.3.3 Changing User Log on/Log off Procedures

You can also select the way users **log on and log off**.
To change log on and log off options:

- Click **Change the way users log on and off** in the User Accounts window.
- You'll see two checkboxes that allow you to enable the **Welcome screen** and **Fast User Switching**. **Fast User Switching** allows you to switch to another user account without closing any programs.

4.4. Managing User Accounts Using Windows 7

With Windows 7, each person that uses your computer can have their own user account. This allows each person to have their own settings, and it allows you to set up Parental Controls to limit the types of games and programs your child is able to use.

In this article, you will learn how to create new user accounts, change account settings, and set up Parental Controls for your child's account.

4.4.1 Setting Up Multiple User Accounts

If you wanted to, you could have a **single account** on your computer that everybody could use. But having **multiple accounts** has some advantages. If each user has their own account, then they'll have their own desktop where they can organize their own files and folders. They'll also be able to choose their own **desktop background**, along with other personalization features. In addition, parents will be able to set **Parental Controls** for each child's account.

Before you start making new user accounts, it's important to understand the two types of accounts:

- **Standard:** Standard accounts are the basic accounts you use for normal, everyday tasks. As a Standard user, you can do just about anything you would need to do, such as running software or personalizing your desktop. Also, Parental Controls can be placed on Standard accounts.

- **Administrator:** Administrator accounts are special accounts used for making certain changes to system settings or managing other people's accounts. They have full access to every setting on the computer. Every computer will have at least one Administrator account.

So as you can see, Administrator accounts are more powerful. But for the same reason, Standard accounts are safer, so they are generally better for everyday use. In fact, you can make **Administrator-level changes** while logged into a **Standard account**; you will just need to provide an **Administrator password** when making the changes.

To Go to Your User Accounts:

1. Go to your **Control Panel** from the **Start Menu**.
2. Click **Add or remove user accounts**.

3. The **Manage Accounts** pane will appear. You will see all of the user accounts here, and you can add more accounts or manage existing ones.

To create a new account:

1. From the **Manage Accounts** pane, click **Create a new account**.
2. Type an **account name**.
3. Select **Standard user** or **Administrator**.
4. Click **Create Account**.

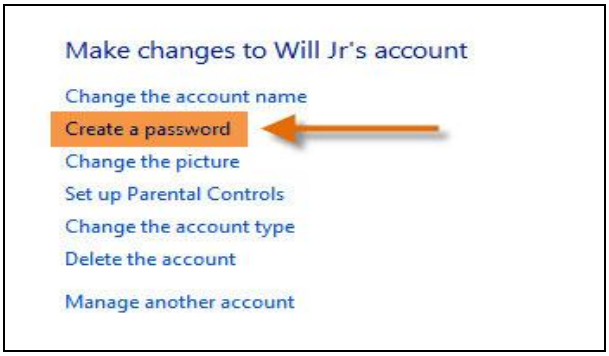
4.4.2 Changing an Account's Settings

Once you've created a new account, you may want to add a **password** or make other changes to the account's settings.

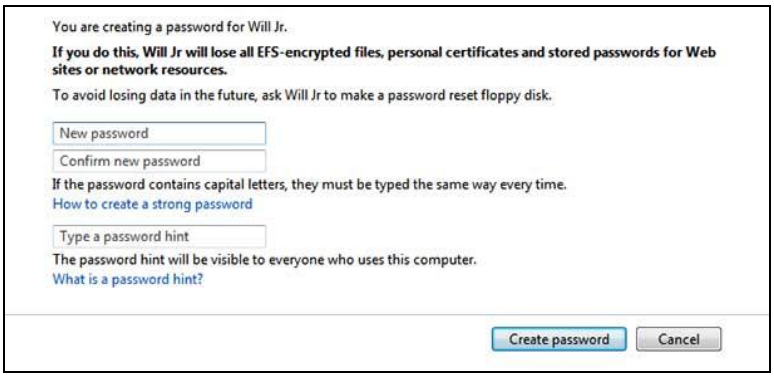
To Create a Password:

1. From the **Manage Accounts** pane, click the account name or picture.

2. Click **Create a password**.



3. Type a password in the **New password** field and retype it in the **Confirm new password** field.
4. If you want, you can type a password hint to help you remember your password.
5. Click **Create password**.
6. To go back to the Manage Accounts pane, click **Manage another account**.



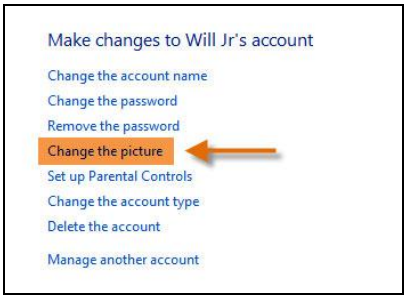
Note: Account passwords are **case sensitive**, which means that capital and lowercase letters are treated as different characters. For example, **aBc1** is not the same as**abc1**.

To Change Your Account Picture:

You can also **change the picture** for any account. This picture appears next to the account name and helps you easily identify the account.

1. From the **Manage Accounts** pane, click the account name or picture.

2. Click **Change the picture**.



3. Select a picture, or click **Browse for more pictures** to select one of your own.

4. Click **Change Picture**.

4.5. Exercise

4.5.1. Multiple choice questions

a. How many ways does Windows give you to manage users on a machine?

(i) Three
(ii) Four
(iii) Two
(iv) One

4.5.2. Questions for short answers

a. Explain “Multiple User Account”.

4.5.3. Analytical questions

a. Describe the changing process of account setting.