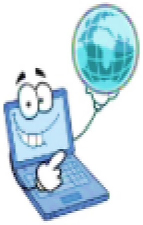
SETTING UP COMPUTER SERVERS



INFORMATION SHEET 1.1

Network Operating Systems Features

Learning Objectives:

After reading this Information Sheet, the learner is expected to:

a. Identify Network Operating system
b. Enumerate Network Operating system features
c. Explain each features of Network Operating System

A network operating system is an operating system designed for the sole purpose of supporting workstations, database sharing, application sharing and file and printer accessing and sharing among multiple computers in a network. It provides services to clients over a network.

A server is a running instance of an application (software) capable of accepting requests from the client and giving responses accordingly. Servers can run on any computer including dedicated computers, which individually are also often referred to as "the Servers operate within a Servers are computer programs running to serve the -requests of other programs, the clients. Thus, the server performs some tasks on behalf of clients. It facilitates the clients to share data, information or any hardware and software resources.

The clients typically connect to the server through the network but may run on the same computer. In the context of Internet Protocol (IP) networking, a server is a program that operates as a socket listener. Servers often provide essential services across a network, either to private users inside a large organization or to public users via the Internet. Typical computing servers are database server, file server, mail server, print server, web server, and numerous systems use this client server networking model including Web sites and email services. An alternative model, enables all computers to act as either a server or client as needed. Usage The term server is used quite broadly in information technology. Despite the many server-branded products available (such as server versions of hardware, software or operating systems), in theory, any computerized process that shares a resource to one or more client processes is a server.

Network operating systems (NOS) typically are used to run computers that act as servers. They provide the capabilities required for network operation.

DIRECTORY SERVICES

A directory service is a database of user accounts and other information that network administrators use to control access to shared network resources. When users connect to a network, they have to be authenticated before they can access network resources.

AUTHENTICATION

Authentication is the process of checking the user's credentials (usually a user name and a password) against the directory. Users that supply the proper credentials are permitted access according to the permissions specified by the network administrator. Successful user authentication in a Windows 2000 2003,2008 computing environment consists of separate processes: interactive logon, which confirms the user's identification to either a domain account or a local computer, and network authentication, which confirms the-user's identification to any network service that the user attempts to access.

WINDOWS SERVER 2008 is designed around certain roles and features. A role is a primary duty that a server performs. A feature is something that helps a server perform its primary duty (Windows Backup, network load balancing). Certain roles are comprised of sub-elements called Role Services, which are distinct units of functionality.

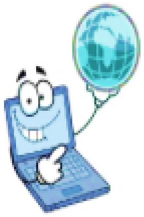
- *The server manager console* introduced in the full installation of Windows 2008 server r2 made the installation of roles and features straightforward.
- Group Policy Management Console (GPMC) is a scriptable Microsoft Management Console (MMC) snap-in, providing a single administrative tool for managing Group Policy across the enterprise. GPMC is the standard tool for managing Group Policy. Group Policy Object (GPO) is a collection of settings that define what a system will look like and how it will behave for a defined group of users. Microsoft provides a program snap-in that allows you to use the Group Policy Microsoft Management Console (MMC). The selections result in a Group Policy Object. The GPO is associated with selected Active Directory containers, such as sites, domains, or organizational units (OUs). The MMC allows you to create a GPO that defines registry-based polices, security options, software installation and maintenance options, scripts options, and folder redirection options.

Some Features:

- *Active Directory Domain Services (AD DS)* stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users. AD DS is also required to be installed on the network in order to install directory-enabled applications such as Microsoft Exchange Server and for applying other Windows Server technologies such as Group Policy.
- *DNS Server* - Domain Name System (DNS) provides a standard method for associating names with numeric Internet addresses. This lets users refer to network computers by using easy-to-remember names instead of a long series of numbers. Windows DNS services can be integrated with DHCP services, eliminating the need to add DNS records as computers are added to the network.
- *Dynamic Host Configuration Protocol* (DHCP) is responsible for assigning IP addresses to the computers automatically. IP addresses assigned to the computers by DHCP server are known as dynamic IP addresses, and the computers that are

configured to obtain the IP addresses automatically from the DHCP server are called DHCP client computers.

- *File Services* provides technologies for storage management, file replication, distributed namespace management, fast file searching, and streamlined client access to files, such as UNIX-based client computers.
- *Print and Document Services* enables you to centralize print server and network printer management tasks. With this role, you can also receive scanned documents from network scanners, and route the documents to a shared network resource, a Windows SharePoint Services site, or to e-mail addresses.
- *Remote Desktop Services* provides technologies that enable users to access Windows-based programs that are installed on a remote desktop server, or to access the Windows desktop itself, from almost any computing device. Users can connect to a remote desktop server to run programs and to use network resources on that server.



INFORMATION SHEET 1.2

User Access Level Configurations

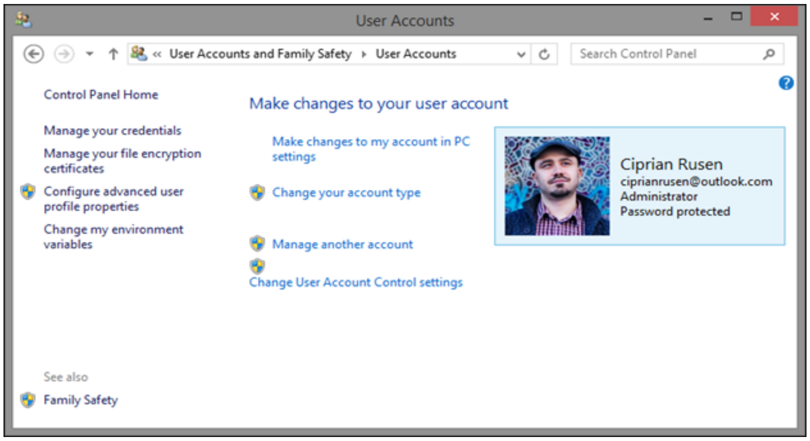
Learning Objectives:

After reading this Information Sheet, the learner is expected to:

a. Define user access level configuration
b. Configure user access level
c. Create user account in accordance with network operating systems features

User Access Level Configuration is part of an access control procedure for computer systems, which allows a system administrator to set up a hierarchy of users. Thus, the low level users can access only a limited set of information, whereas the highest level users can access the most sensitive data on the system. Also called access rights.
A user account is a collection of settings and information that tells Windows which files and folders you can access, what you can do on your computer, what are your preferences, and what network resources you can access when connected to a network. The user account allows you to authenticate to Windows or any other operating system so that you are granted authorization to use them. Multi-user operating systems such as Windows don’t allow a user to use them without having a user account.

In Windows, you can manage your computer's user accounts by going to the "Control Panel" and then to "User Accounts and Family Safety > User Accounts."

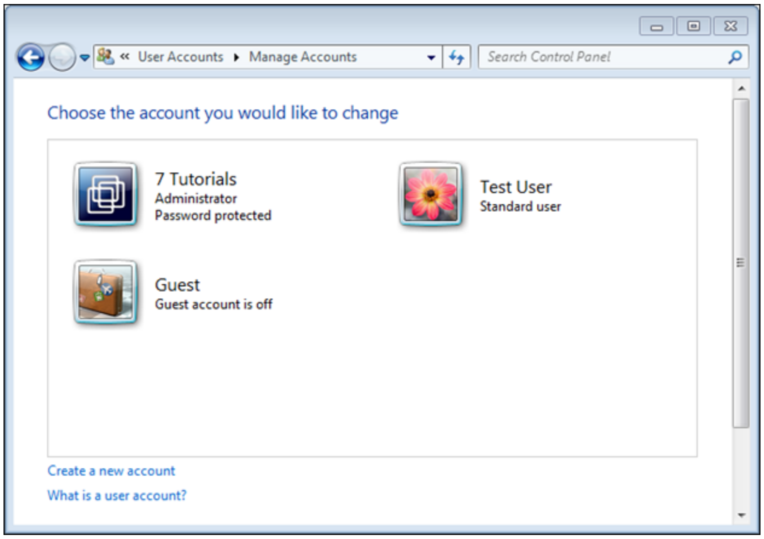

User Accounts
« User Accounts and Family Safety ▸ User Accounts
Search Control Panel
Control Panel Home
Manage your credentials
Manage your file encryption certificates
Configure advanced user profile properties
Change my environment variables
See also
Family Safety
Make changes to your user account
Make changes to my account in PC settings
Change your account type
Manage another account
Change User Account Control settings
Ciprian Rusen
ciprianrusen@outlook.com
Administrator
Password protected

A user account in Windows is characterized by the following attributes:

- User name – the name you are giving to that account.
- Password – the password associated with the user account (in Windows 7 or older versions you can also use blank passwords).
- User group – a collection of user accounts that share the same security rights and permissions. A user account must be a member of at least one user group.
- Type – all user accounts have a type which defines their permissions and what they can do in Windows.

Windows 7 User Accounts

Windows 7 and earlier versions has three important types of accounts:



Administrator

The "Administrator" user account has complete control over the PC. He or she can install anything and make changes that affect all users of that PC.

Standard

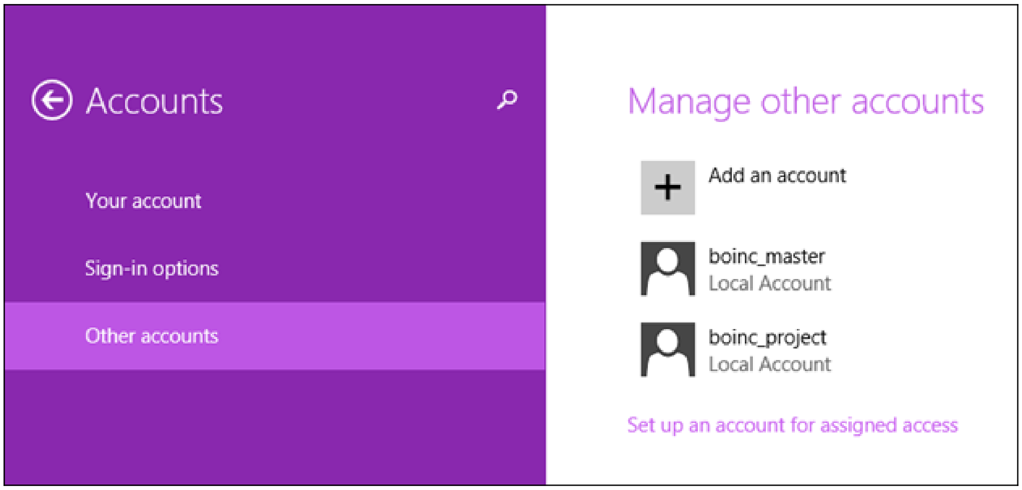
The “Standard” user account can only use the software that’s already installed by the administrator and change system settings that don’t affect other users.

Guest

The “Guest” account is a special type of user account that has the name Guest and no password. This is only for users that need temporary access to the PC. This user can only use the software that’s already installed by the administrator and cannot make any changes to system settings.

Windows 8 User Accounts

Windows 8 introduces two new types of user accounts, alongside those already in Windows 7:



Microsoft account

Microsoft accounts are user accounts with an associated e-mail address that give you access to all Microsoft products and services. They always have password that’s not blank. If you are using an outlook.com e-mail address (let’s say howtogeek@outlook.com), you have a Microsoft account with that address.

To further complicate things, Microsoft allows people to create Microsoft accounts using third-party e-mail services like Gmail. To simplify things for you, remember that you have a Microsoft account when you use an email address to log into Windows or to any Microsoft product or service.

Microsoft accounts work on multiple systems and devices. Therefore you can use the same account to log into all your Windows 8.x devices, your Xbox One console and your Windows Phone. You don’t have to create a separate account for each device.

Microsoft accounts can be administrators or standard user accounts.

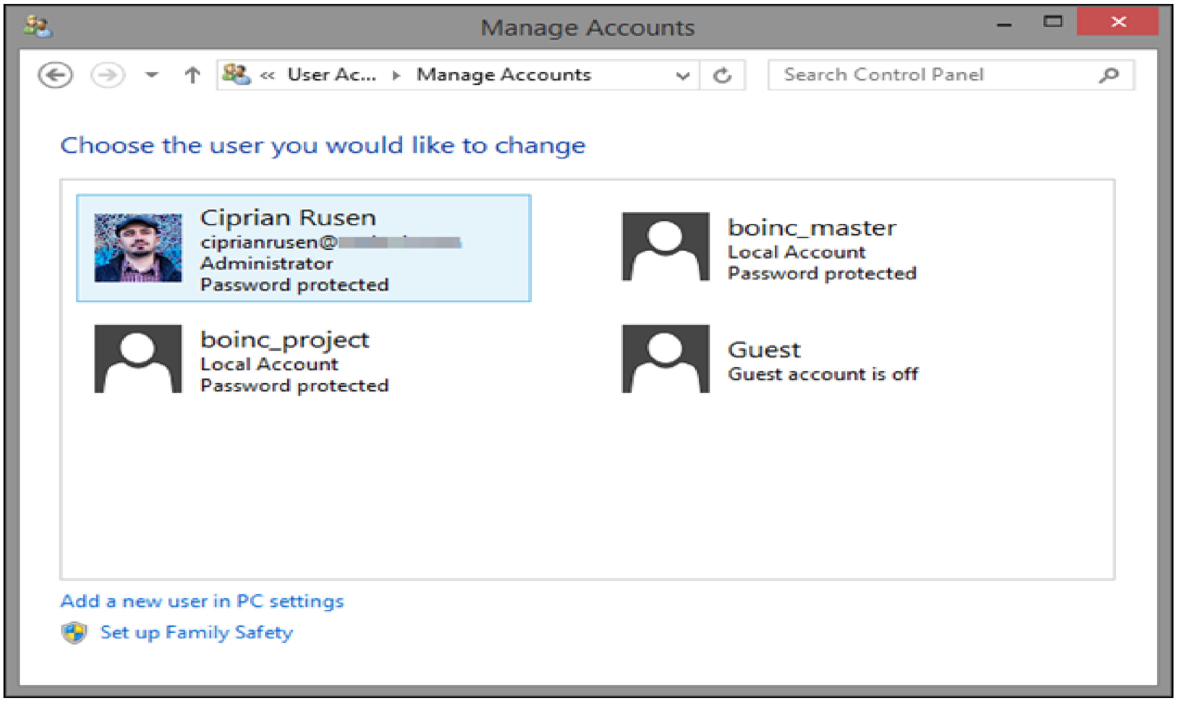
Local account

Local accounts are classic user accounts that exist locally and can use blank passwords. For example, in Windows 7 all user accounts are local accounts. Local accounts can be administrators or standard user accounts. They work on a single system only, so if you do have multiple devices, you'll have to create a separate account for each.

User accounts provide the added benefit of letting you share the same computer with several people, while having your own files and settings. Each person accesses his or her user account without interfering with others.

How to tell them apart?

In Windows 8.x you can quickly differentiate local user accounts from Microsoft accounts by looking at whether they use an email address or not. Look at the screenshot below, sharing the Manage Accounts window, which is accessed by going to "Control Panel > User Accounts and Family Safety > User Accounts > Manage Accounts."



Choose the user you would like to change

Ciprian Rusen
ciprianrusen@[redacted]
Administrator
Password protected

boinc_master
Local Account
Password protected

boinc_project
Local Account
Password protected

Guest
Guest account is off

The first account, named Ciprian Rusen, is a Microsoft account. All the other user accounts are local accounts. The Microsoft account is an administrator, which is marked by the "Administrator" statement beneath its email address. All other user accounts are standard user accounts because they do not have the "Administrator" statement.

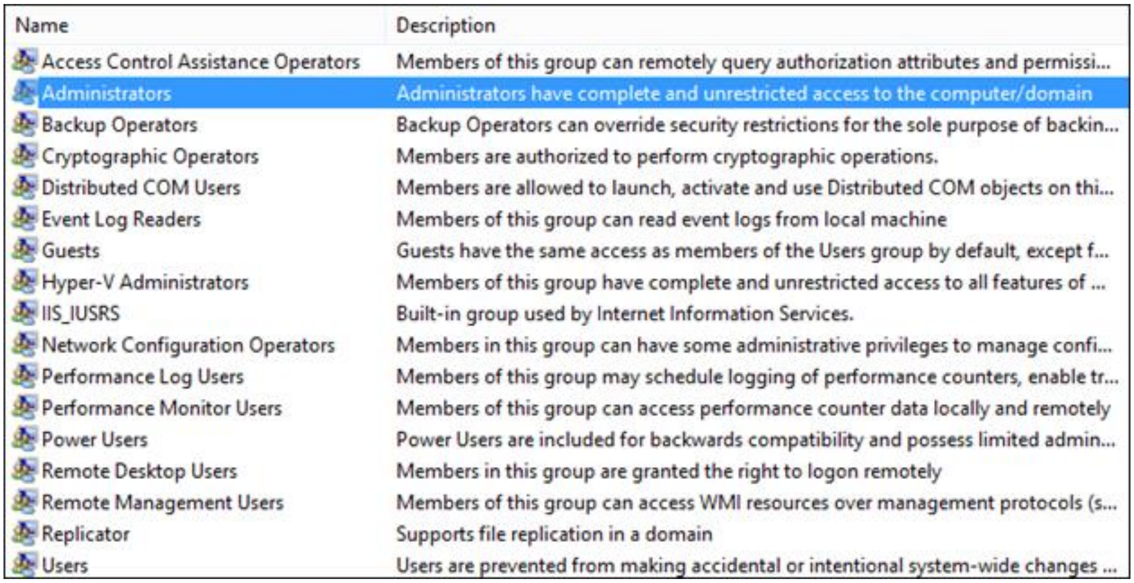
What is a User Group?

As mentioned earlier, the user group is a collection of user accounts that share the same security rights and permissions.

Keep Reading…

Windows has a long list of predefined user groups which includes “Administrators” and “Users.” However, most predefined user groups do not have user accounts until the administrator or third-party apps start customizing them. User groups can also be created by third-party software and services like virtual machines which create hidden user accounts and groups in order to provide different features or services.

A user account is a member of at least one user group while some user accounts are members of two groups or more, depending on how they are set.



Name	Description
Access Control Assistance Operators	Members of this group can remotely query authorization attributes and permissi...
Administrators	Administrators have complete and unrestricted access to the computer/domain
Backup Operators	Backup Operators can override security restrictions for the sole purpose of backin...
Cryptographic Operators	Members are authorized to perform cryptographic operations.
Distributed COM Users	Members are allowed to launch, activate and use Distributed COM objects on thi...
Event Log Readers	Members of this group can read event logs from local machine
Guests	Guests have the same access as members of the Users group by default, except f...
Hyper-V Administrators	Members of this group have complete and unrestricted access to all features of ...
IIS_IUSRS	Built-in group used by Internet Information Services.
Network Configuration Operators	Members in this group can have some administrative privileges to manage confi...
Performance Log Users	Members of this group may schedule logging of performance counters, enable tr...
Performance Monitor Users	Members of this group can access performance counter data locally and remotely
Power Users	Power Users are included for backwards compatibility and possess limited admin...
Remote Desktop Users	Members in this group are granted the right to logon remotely
Remote Management Users	Members of this group can access WMI resources over management protocols (s...
Replicator	Supports file replication in a domain
Users	Users are prevented from making accidental or intentional system-wide changes ...

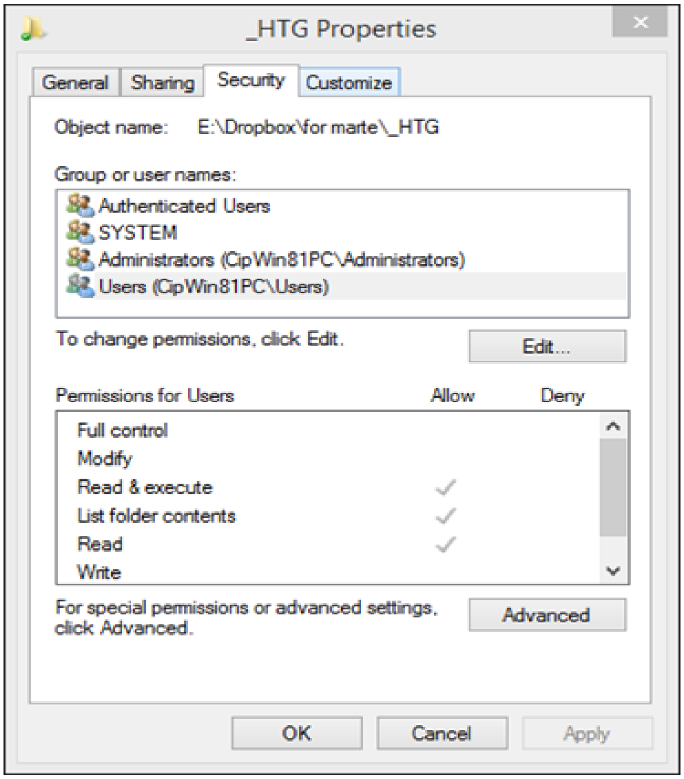
For example, all user accounts that are set as administrators will be part of the “Administrators” group. Standard user accounts are part of the “Users” group. However, both types of user accounts will become members of the “HomeUsers” group, when you start using the Homegroup networking feature in Windows.

User groups are managed automatically by Windows and you won’t need to fiddle with them, even though you can if you are an administrator. This concept is important so that you better understand how file sharing works, how permissions are assigned, etc.

What are File & Folder Permissions?

Permissions are a method for assigning access rights to specific user accounts and user groups. Through the use of permissions, Windows defines which user accounts and user groups can access which files and folders, and what they can do with them. To put it simply, permissions are the operating system’s way of telling you what you can or cannot do with a file or folder.

To learn the permissions of any folder, right click on it and select “Properties.” In the Properties window, go to the Security tab. In the “Group or user names” section you will see all the user accounts and use groups that have permissions to that folder. If you select a group or a user account, then see its assigned permissions, in the “Permissions for Users” section.



Object name: E:\Dropbox\for marte_HTG

Group or user names:

- Authenticated Users
- SYSTEM
- Administrators (CipWin81PC\Administrators)
- Users (CipWin81PC\Users)

To change permissions, click Edit.

Permissions for Users	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		

For special permissions or advanced settings, click Advanced.

In Windows, a user account or a user group can receive one of the following permissions to any file or folder:

- Read – allows the viewing and listing of a file or folder. When viewing a folder, you can view all its files and subfolders.
- Write – allows writing to a file or adding files and subfolders to a folder.
- List folder contents – this permission can be assigned only to folders. It permits the viewing and listing of files and subfolders, as well as executing files that are found in that folder.
- Read & execute – permits the reading and accessing of a file’s contents as well as its execution. When dealing with folders, it allows the viewing and listing of files and subfolders, as well as the execution of files.
- Modify – when dealing with files, it allows their reading, writing and deletion. When dealing with folders, it allows the reading and writing of files and subfolders, plus the deletion of the folder.
- Full control – it allows reading, writing, changing and deleting of any file and subfolder.

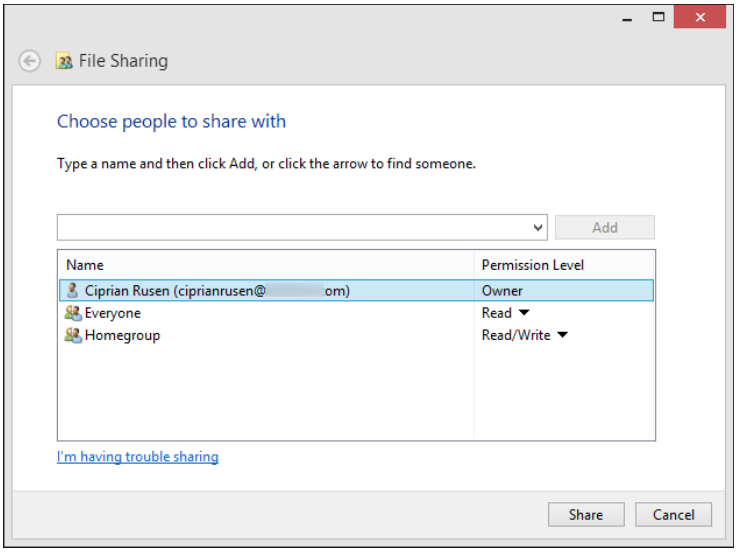
Generally, files inherit the permissions of the folder where they are placed, but users can also define specific permissions that are assigned only to a specific file. To make your computing life simpler, it is best to edit permissions only at a folder level.

Why are Permissions Important to Sharing in Windows?

Permissions are important because when you share something in Windows, you actually assign a set of permissions to a specific user account or user group. A shared folder can only be accessed by someone with a user account that has the permission to access that folder.

For example, when using the Sharing Wizard, you choose the user name or the user group and then one of these two permission levels:

- Read/Write – it is the equivalent of the “Modify” permission level.
- Read – it is the equivalent of the “Read & execute” permission level.



Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

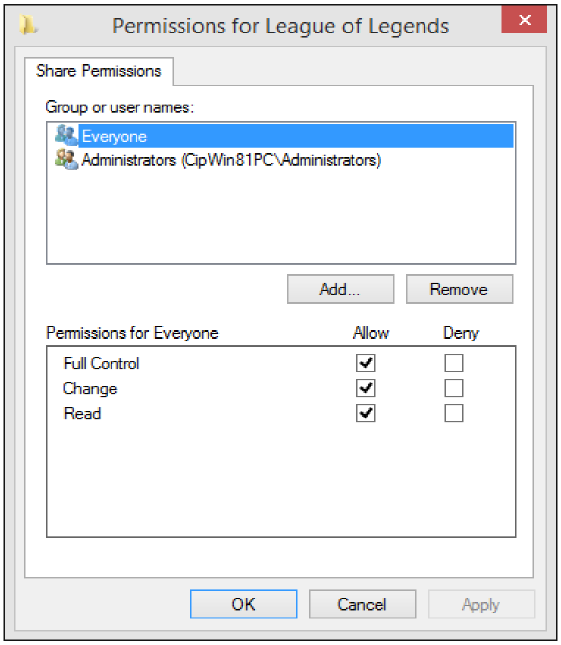
Name	Permission Level
Ciprian Rusen (ciprianrusen@[redacted]om)	Owner
Everyone	Read ▼
Homegroup	Read/Write ▼

I'm having trouble sharing

When using the Sharing Wizard you will also see a permission level named “Owner.” This is not a permission level per-se. It just signals that the folder you are about to share is owned by the user account for which you see this entry. An owner has full control over that folder. You will learn more about the Sharing Wizard and how to use it in lesson 6.

When using advanced sharing, you can assign one of these three permission levels:

- Full Control – it allows reading, writing, changing, and deleting of any file and subfolder.
- Change – it is the equivalent of the *Modify* permission level.
- Read – it is the equivalent of the *Read & execute* permission level.



Permissions for League of Legends

Share Permissions

Group or user names:

- Everyone
- Administrators (CipWin81PC\Administrators)

Permissions for Everyone	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

When sharing resources with the network, you will encounter a special group that's named "Everyone." This user group stands for anyone with or without a user account on the computer who is sharing the resource with the network. As you will learn in future lessons, this user group is very useful when you have a network with very diverse devices and operating systems. Advanced sharing will be explained in detail, in lesson 7.

Why is it Useful to Use a Microsoft Account in Your Network?

Using a Microsoft account has both benefits (e.g. the ability to sync all your apps and settings across multiple devices) and downsides (e.g. you will give more data to Microsoft). From a network sharing perspective, using a Microsoft account can be useful if you have a network with many PCs and devices with Windows 8.x:

- You log in with the same Microsoft account on all your devices, using the same credentials.
- You don't have to create separate local accounts on each computer or device with Windows 8.x.
- Setting up permissions when sharing is easier because you don't have to deal with multiple local user accounts.
- Accessing network shares is also easier because you log in with the same user account everywhere and you can quickly access everything that's shared with it.

Source: http://www.businessdictionary.com/definition/system-access-level.html

https://www.howtogeek.com/school/windows-network-sharing/lesson1/

Note:

If "Access permissions" are granted to users who are registered to computers, they are authorized to operate folders and files.
There are two types of access permissions:

- Network-level access permission

This is to control users who access to the shared folder over the network.

- Local-level access permission

This is to control users who access folders by logging on to their computers.
The local-level access permission can be set only when the drive in which folders are located is formatted in NTFS.

Shared Folder without Access Control

In Windows Server 2008, you can use the special folder named "Public folder," which allows files to be shared with other users on the same network. Using the Public folder, you can set up a shared folder without access control.

NOTE:

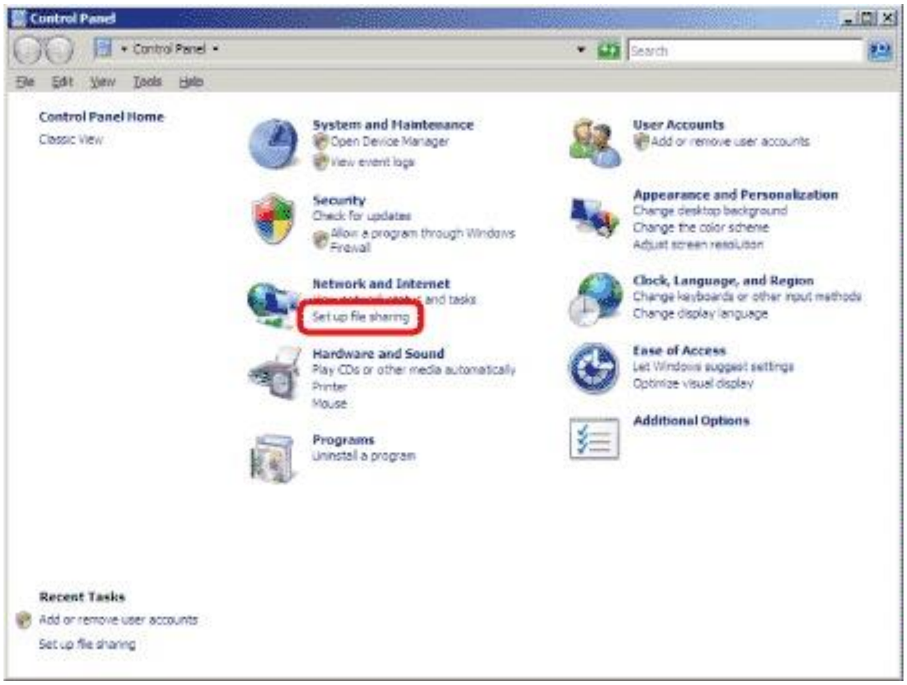
By default, the Public folder is created in the [Users] folder, on the drive (e.g. C drive) Windows Vista is installed on.
Example: \Public\share

● For Windows Server 2008 users

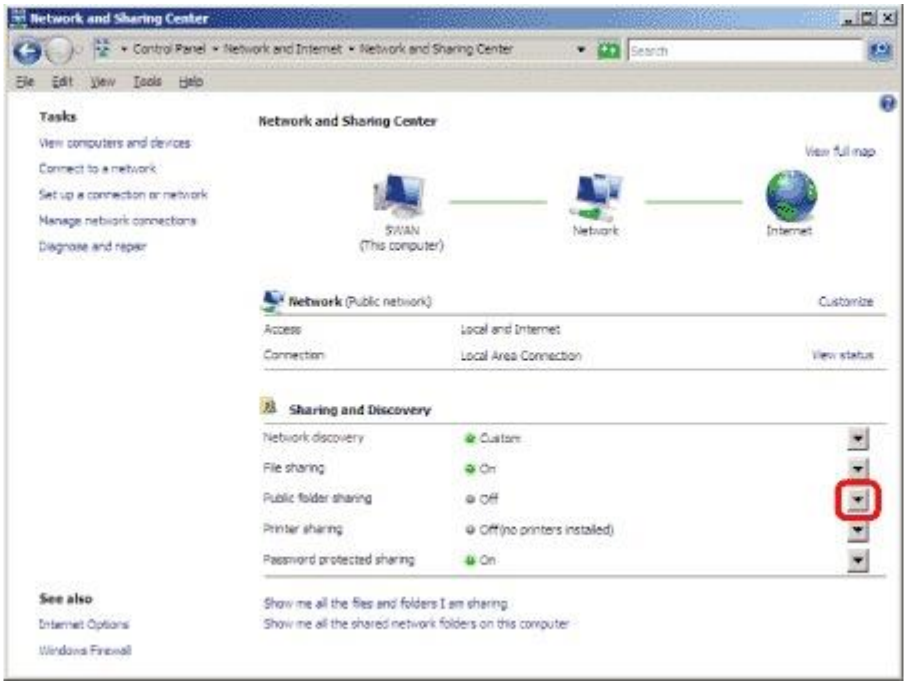
Sharing the Public folder

1. On the [Start] menu, select [Control Panel] to open [Control Panel] window.

2. Click [Set up file sharing] to open the [Network and Sharing Center] window.



3. In the [Network and Sharing Center] window, click the downwards arrow next to [Public folder sharing].


Network and Sharing Center
Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search
File Edit View Tools Help
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
View full map
SWAN
(This computer)
Network
Internet
Customize
View status
See also
Internet Options
Windows Firewall
Show me all the files and folders I am sharing
Show me all the shared network folders on this computer

Network and Sharing Center

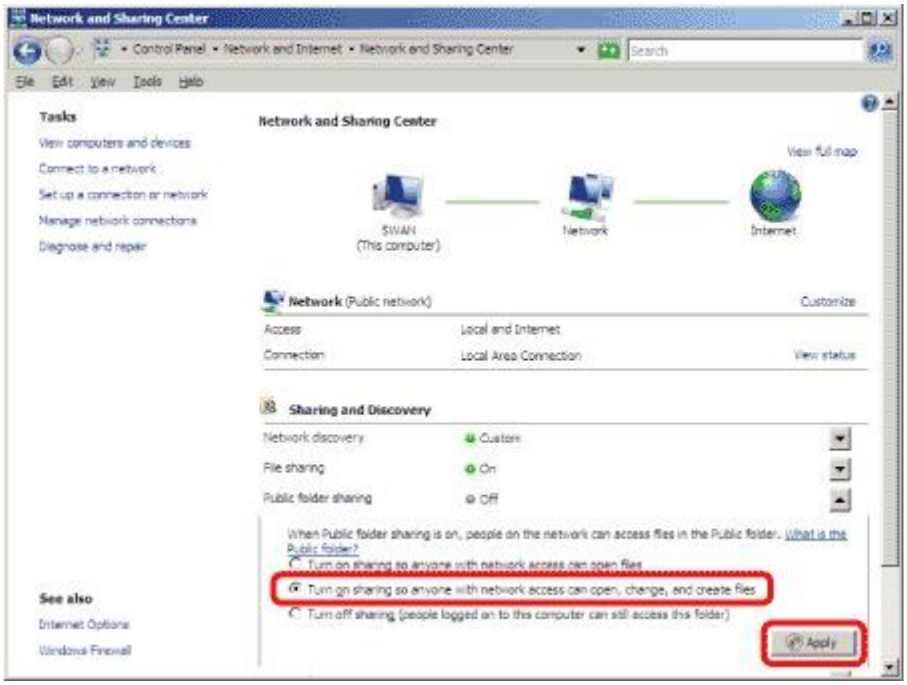
Network (Public network)

Access	Local and Internet
Connection	Local Area Connection

Sharing and Discovery

Network discovery	Custom
File sharing	On
Public folder sharing	Off
Printer sharing	Off (no printers installed)
Password protected sharing	On

4. Select [Turn on sharing so anyone with network access can open, change, and create files], and then click [Apply].


Network and Sharing Center
Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search
File Edit View Tools Help
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
View full map
SWAN
(This computer)
Network
Internet
Customize
View status
See also
Internet Options
Windows Firewall
Apply

Network and Sharing Center

Network (Public network)

Access	Local and Internet
Connection	Local Area Connection

Sharing and Discovery

Network discovery	Custom
File sharing	On
Public folder sharing	Off

When Public folder sharing is on, people on the network can access files in the Public folder. What is the Public folder?

○ Turn on sharing so anyone with network access can open files

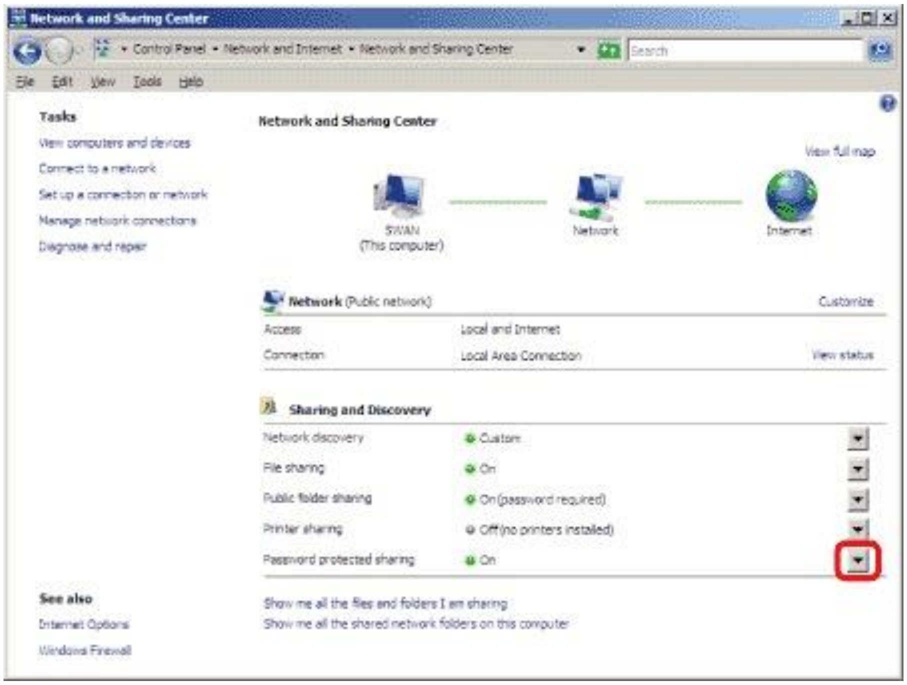
● Turn on sharing so anyone with network access can open, change, and create files

○ Turn off sharing (people logged on to this computer can still access this folder)

NOTE:

- Do not select [Turn on sharing so anyone with network access can open files]. Otherwise, you will not be able to store a document scanned with this machine in a shared folder.
- If the [User Account Control] dialog box appears in Windows Server 2008, click [Continue].

5. Click the downwards next to [Password protected sharing].


Network and Sharing Center
Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search
File Edit View Tools Help
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
View full map
SWAN
(This computer)
Network
Internet
Customize
View status
See also
Internet Options
Windows Firewall
Show me all the files and folders I am sharing
Show me all the shared network folders on this computer

Network and Sharing Center

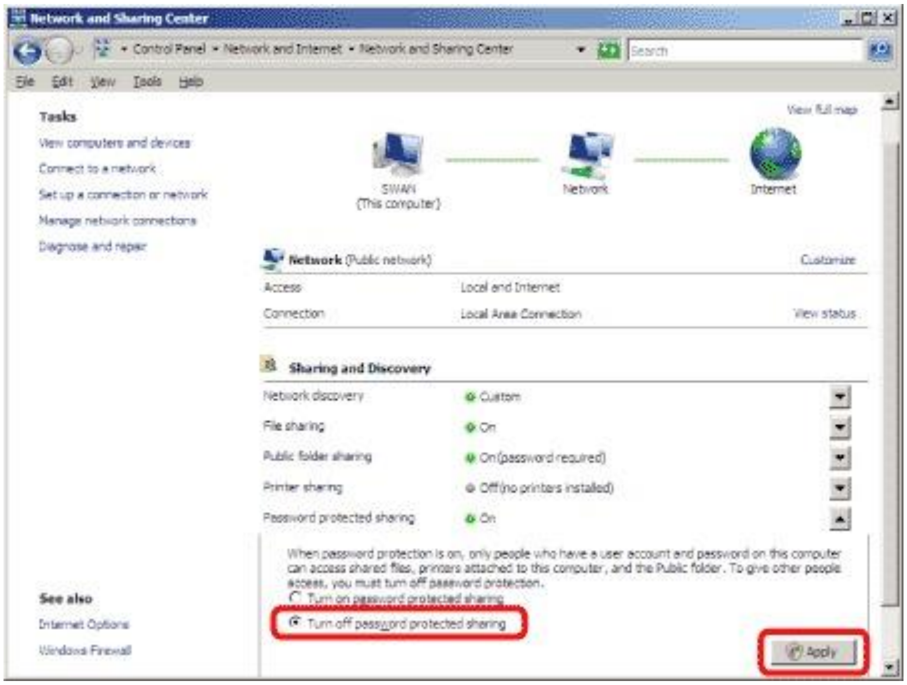
Network (Public network)

Access	Local and Internet
Connection	Local Area Connection

Sharing and Discovery

Network discovery	Custom
File sharing	On
Public folder sharing	On (password required)
Printer sharing	Off (no printers installed)
Password protected sharing	On

6. Check [Turn off password protected sharing], and then click [Apply].


Network and Sharing Center
Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Search
File Edit View Tools Help
Tasks
View computers and devices
Connect to a network
Set up a connection or network
Manage network connections
Diagnose and repair
View full map
SWAN
(This computer)
Network
Internet
Customize
View status
See also
Internet Options
Windows Firewall
Apply

Network (Public network)

Access	Local and Internet
Connection	Local Area Connection

Sharing and Discovery

Network discovery	Custom
File sharing	On
Public folder sharing	On (password required)
Printer sharing	Off (no printers installed)
Password protected sharing	On

When password protection is on, only people who have a user account and password on this computer can access shared files, printers attached to this computer, and the Public folder. To give other people access, you must turn off password protection.

○ Turn on password protected sharing

● Turn off password protected sharing

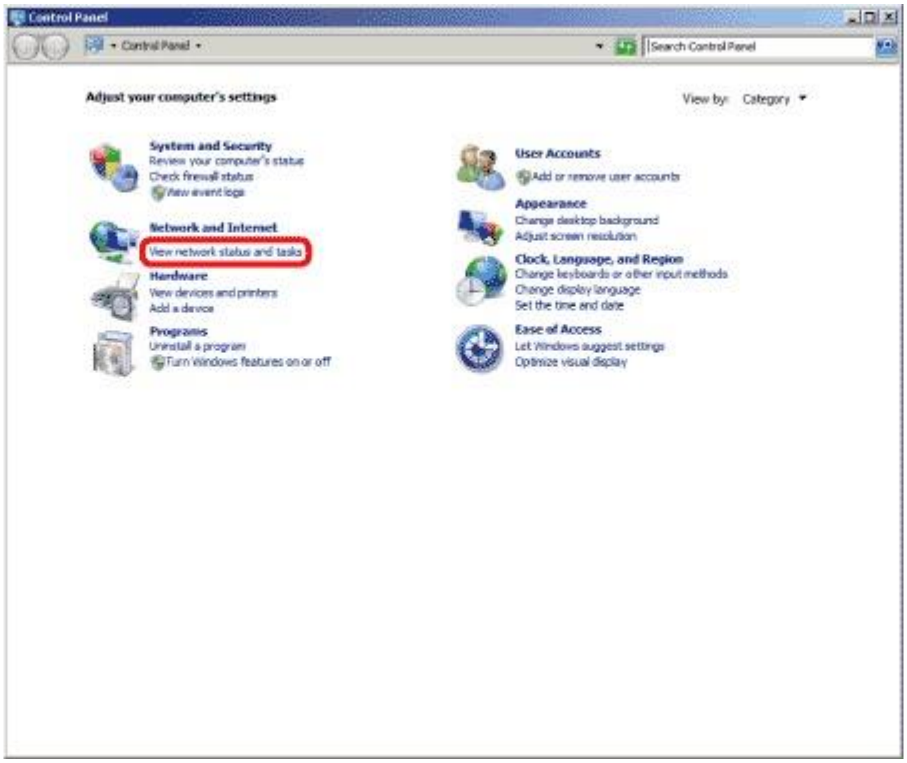
NOTE:

If the [User Account Control] dialog box appears in Windows Server 2008, click [Continue].

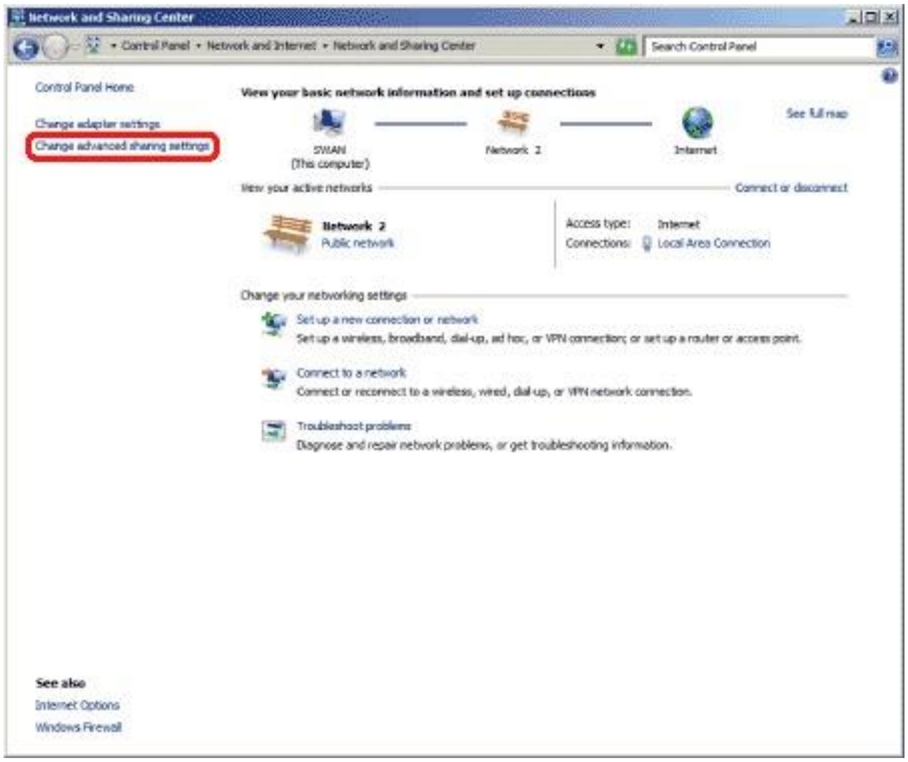
● For Windows Server 2008 R2 users

Sharing the Public folder

1. On the [Start] menu, select [Control Panel] to open [Control Panel] window.
2. Click [View network status and tasks] to open the [Network and Sharing Center] window.



3. Click [Change advanced sharing settings] in the [Network and Sharing Center] window.



View your basic network information and set up connections

View your active networks

Network 2
Public network

Access type: Internet
Connections: Local Area Connection

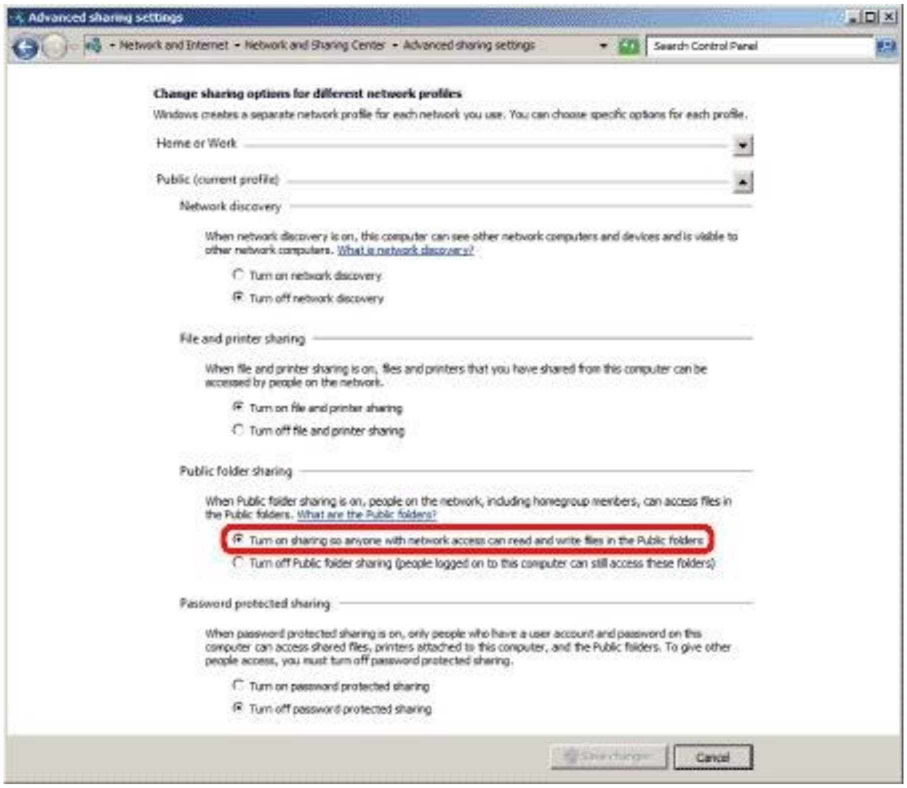
Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

4. In the [Advanced sharing settings] window, under [Public folder sharing], select [Turn on sharing so anyone with network access can read and write files in the Public folders].


Advanced sharing settings
Network and Internet ▸ Network and Sharing Center ▸ Advanced sharing settings
Search Control Panel
Save changes
Cancel

Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Home or Work

Public (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

○ Turn on network discovery
● Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing
○ Turn off file and printer sharing

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. What are the Public folders?

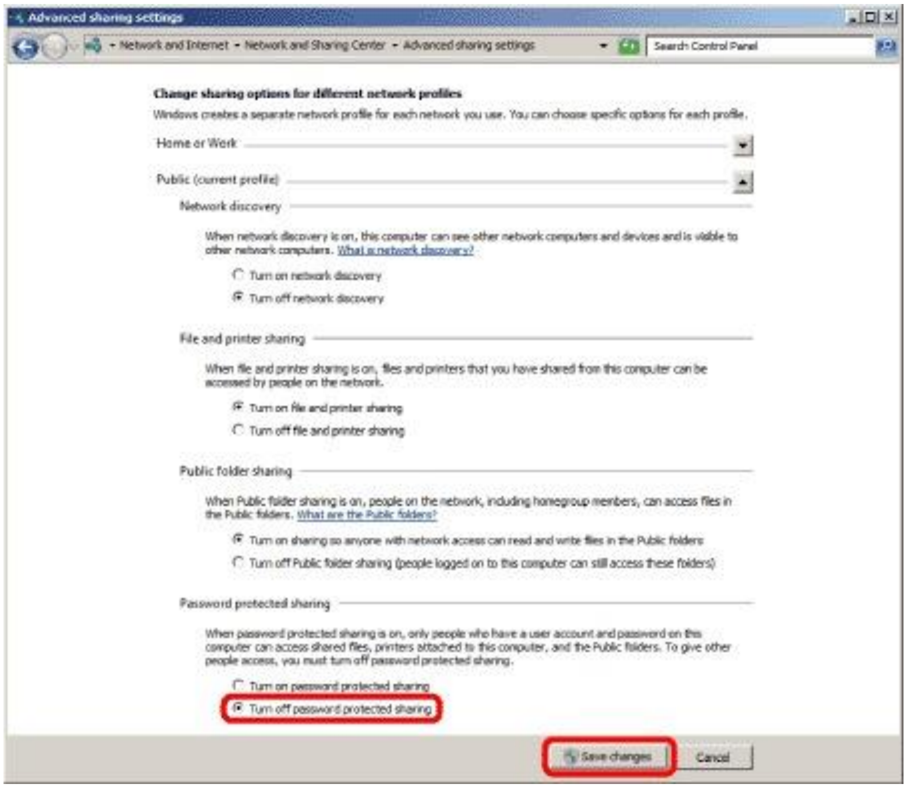
● Turn on sharing so anyone with network access can read and write files in the Public folders
○ Turn off Public folder sharing (people logged on to this computer can still access these folders)

Password protected sharing

When password protected sharing is on, only people who have a user account and password on this computer can access shared files, printers attached to this computer, and the Public folders. To give other people access, you must turn off password protected sharing.

○ Turn on password protected sharing
● Turn off password protected sharing

5. Under [Password protected sharing], select [Turn off password protected sharing], and then click [Save changes].


Advanced sharing settings
Network and Internet ▸ Network and Sharing Center ▸ Advanced sharing settings
Search Control Panel
Save changes
Cancel

Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Home or Work

Public (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

○ Turn on network discovery

● Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing

○ Turn off file and printer sharing

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. What are the Public folders?

● Turn on sharing so anyone with network access can read and write files in the Public folders

○ Turn off Public folder sharing (people logged on to this computer can still access these folders)

Password protected sharing

When password protected sharing is on, only people who have a user account and password on this computer can access shared files, printers attached to this computer, and the Public folders. To give other people access, you must turn off password protected sharing.

○ Turn on password protected sharing

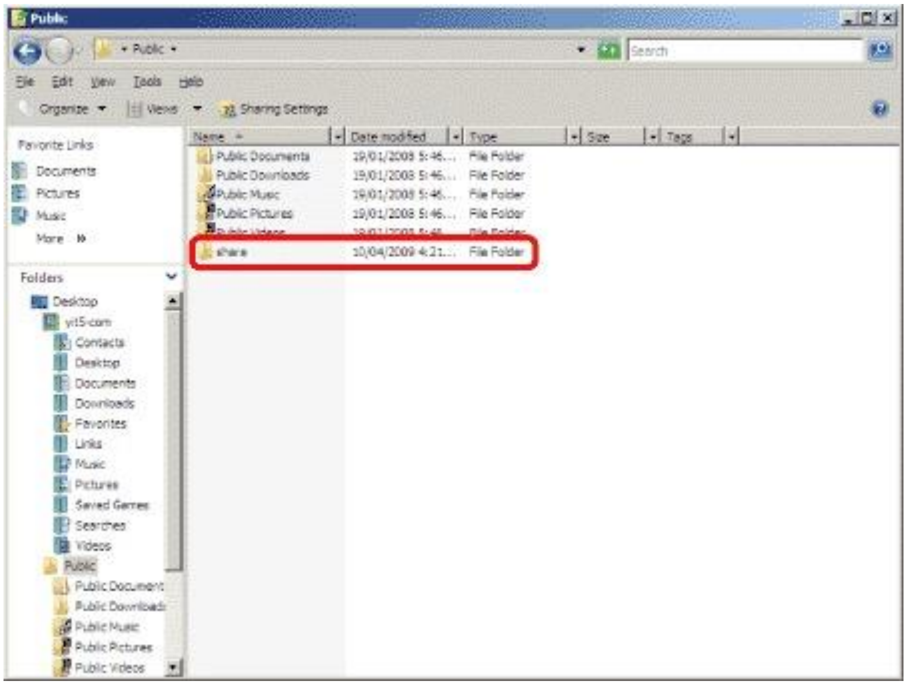
● Turn off password protected sharing

Creating a folder to store a file

You can store a file in the first level of the Public folder. This section describes the procedure for creating a new folder in which to store a file in the Public folder.

1. Display the Public folder in Windows Explorer, etc.

2. Create a new folder in the Public folder.



Name	Date modified	Type	Size	Tags
Public Documents	19/01/2008 5:46...	File Folder		
Public Downloads	19/01/2008 5:46...	File Folder		
Public Music	19/01/2008 5:46...	File Folder		
Public Pictures	19/01/2008 5:46...	File Folder		
Public Videos	19/01/2008 5:46...	File Folder		
share	10/04/2009 4:21...	File Folder		

NOTE:

It is recommended that you write down the folder name you created here.

Shared Folder with Access Control

Creating a User Account for Accessing a Shared Folder

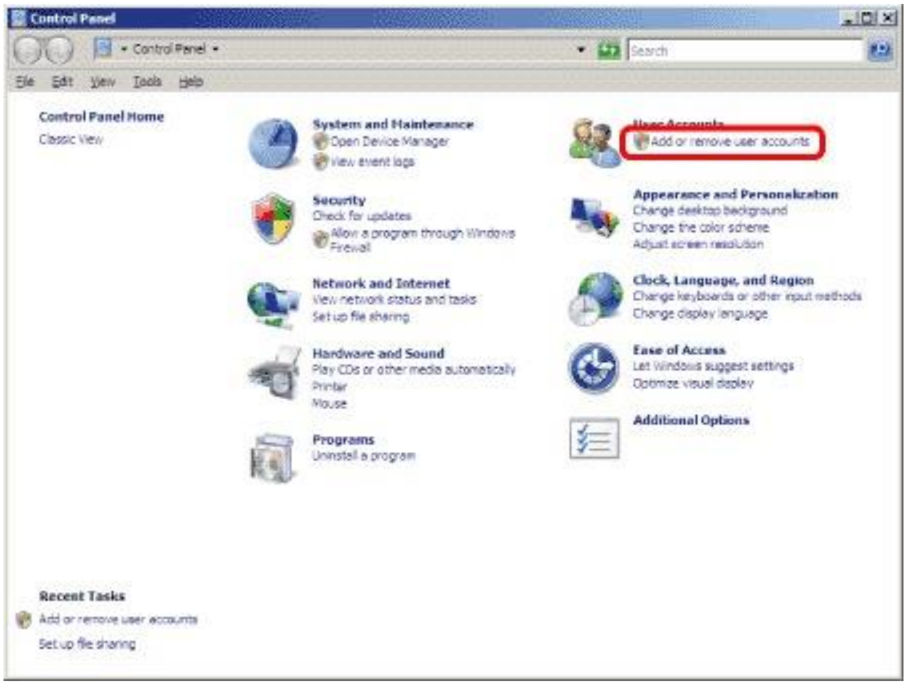
You need to create user accounts for users who access the shared folder in advance. This section describes the procedure for creating a new account on your computer.

NOTE:

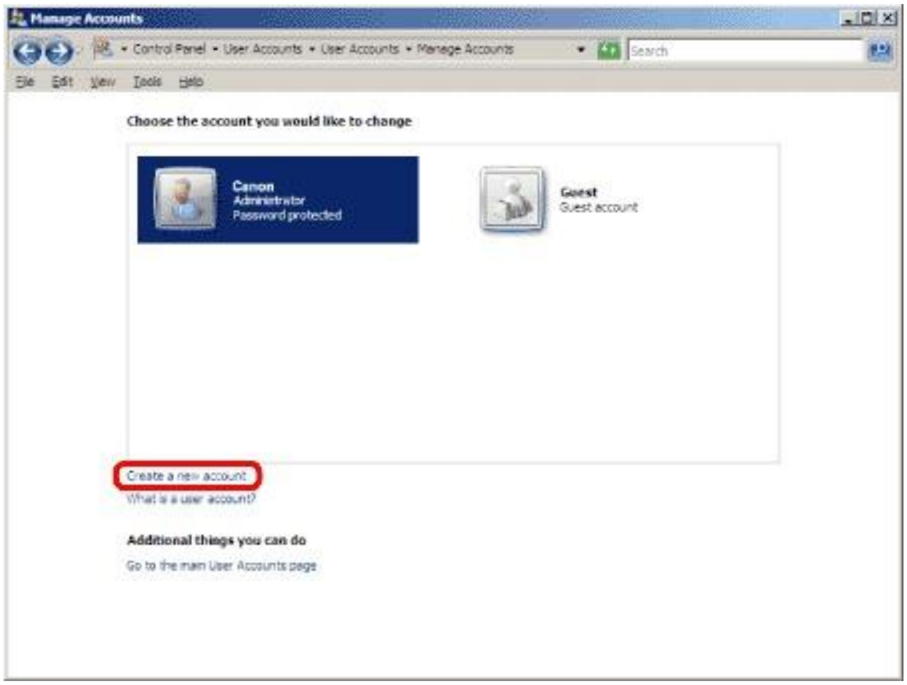
Even if you do not create a new account by following the procedures below, you can add a pre-registered account for users who are permitted to access the shared folder. In such case, you need to create a password if one has not been set for the pre-registered account. Once the password is created, the user is prompted to type it when he/she logs on to a computer.

1. On the [Start] menu, select [Control Panel] to open [Control Panel] window.

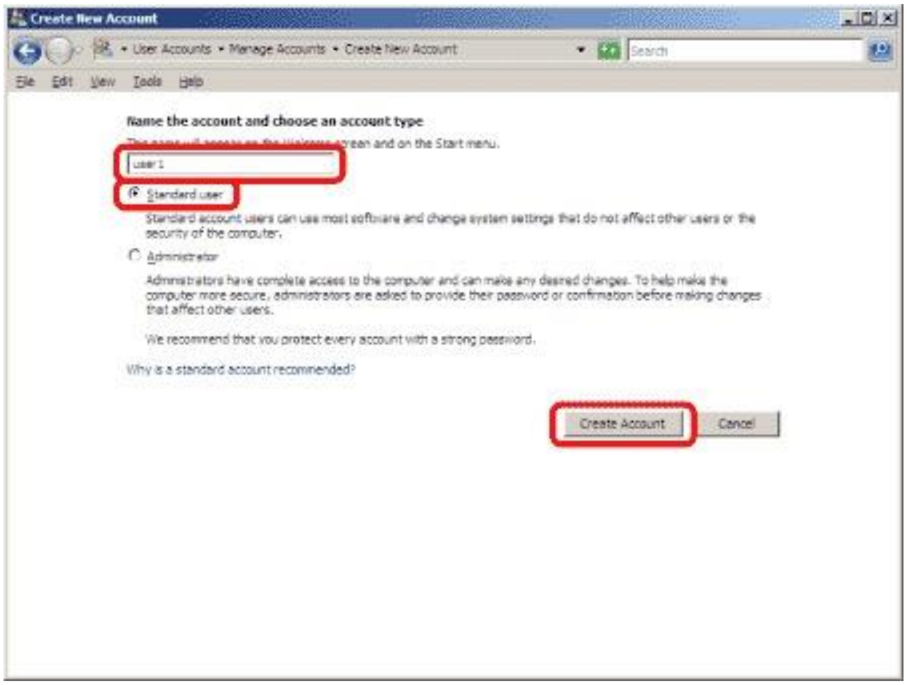
2. Click [Add or remove user accounts].



3. In the [Manage Accounts] dialog box, click [Create a new account].


Manage Accounts
Control Panel ▸ User Accounts ▸ User Accounts ▸ Manage Accounts
Search
File Edit View Tools Help
Choose the account you would like to change
Canon
Administrator
Password protected
Guest
Guest account
Create a new account
What is a user account?
Additional things you can do
Go to the main User Accounts page

4. In the [Create New Account] dialog box, enter the user name, check [Standard user], and then click [Create Account].


Create New Account
User Accounts ▸ Manage Accounts ▸ Create New Account
Search
File Edit View Tools Help
Create Account
Cancel

Name the account and choose an account type

This name will appear on the Welcome screen and on the Start menu.

user 1

● Standard user

Standard account users can use most software and change system settings that do not affect other users or the security of the computer.

○ Administrator

Administrators have complete access to the computer and can make any desired changes. To help make the computer more secure, administrators are asked to provide their password or confirmation before making changes that affect other users.

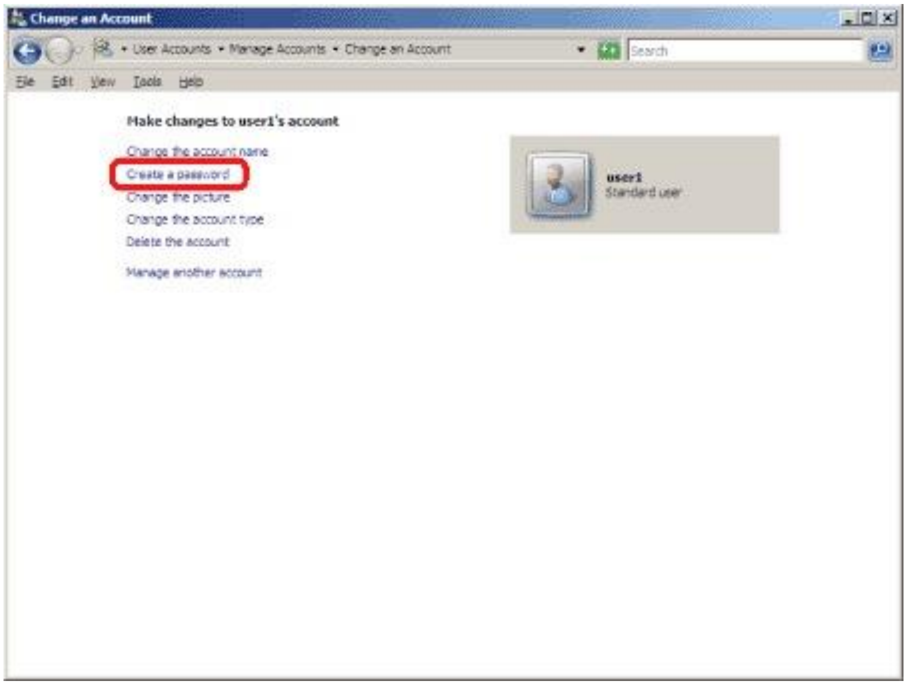
We recommend that you protect every account with a strong password.

Why is a standard account recommended?

NOTE:

- The user name must be up to 20 alphanumeric characters long.
- It is recommended that you write down the user name you created here.

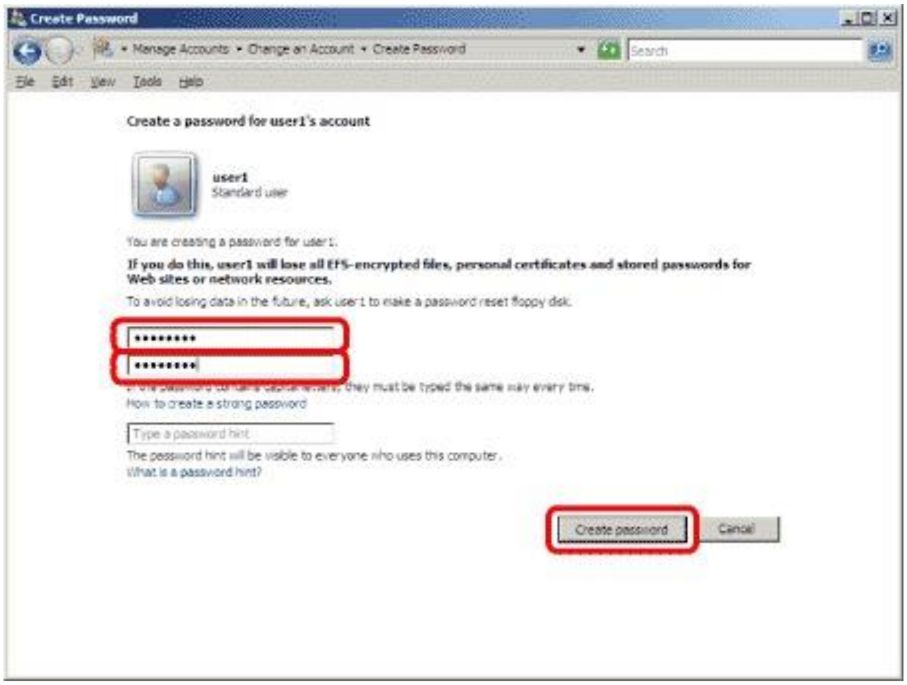
5. Click the user name created in step 4, and then click [Create a password].



Make changes to user1's account

user1
Standard user

6. In the [Create Password] dialog box, type the password in two boxes, and then click [Create password].



Create a password for user1's account

You are creating a password for user1.

If you do this, user1 will lose all EFS-encrypted files, personal certificates and stored passwords for Web sites or network resources.

To avoid losing data in the future, ask user1 to make a password reset floppy disk.

If the password contains capital letters, they must be typed the same way every time.

How to create a strong password

The password hint will be visible to everyone who uses this computer.

What is a password hint?

NOTE:

- The password must be up to 14 alphanumeric characters long.
- It is recommended that you write down the password you created here.

7. Close the [Change an Account] dialog box.

Setting a Shared Folder and Access Permissions

Once you create the account on your computer, create a shared folder. Add the created account to the shared folder as a user who is permitted to access that folder. Set the permission which allows the user to access the folders as well.

NOTE:

If "Access permissions" are granted to users who are registered for computers, they are authorized to operate folders and files.
This section describes the procedure for granting FULL Control permission to the "Everyone" account so that any user can access the shared folder.

There are two types of access permissions:

- Network-level access permission
  This is to control users who access to the shared folder over the network.
- Local-level access permission

  This is to control access to folders by users who are logged on to the computer.

The local-level access permission can be set only when the drive in which folders are located is formatted in NTFS.

The [File Sharing] dialog box is used to set up the access permissions. The network-level and local-level access permissions for a user will be set simultaneously when you select a permission level in the [File Sharing] dialog box.

For Windows Server 2008 users

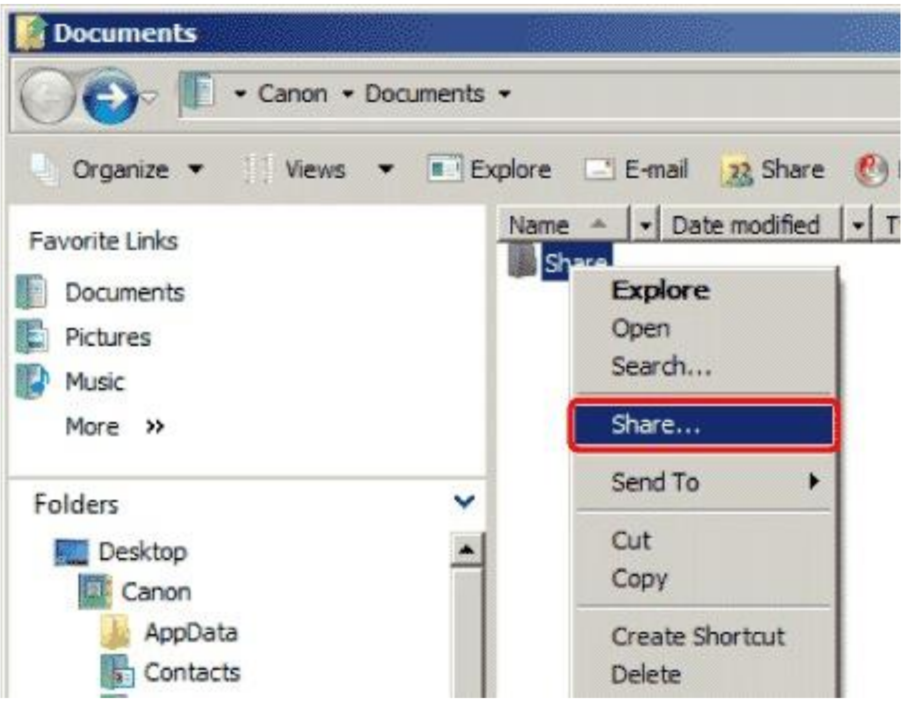
1. Create a folder in any drive.

It is recommended to create the folder in a place where users can find it easily, such as the first level in C drive.

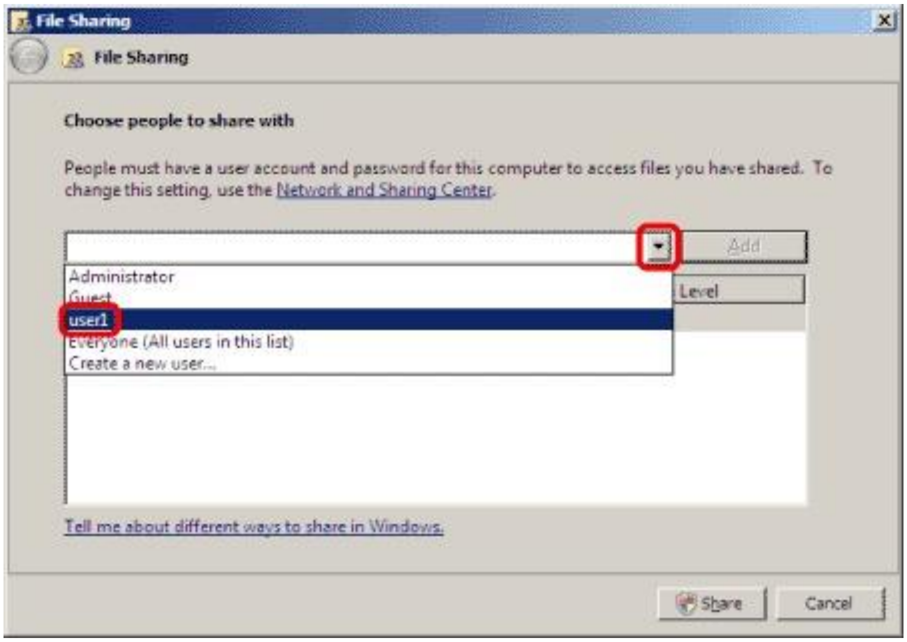
Ex) C:\share

2. Right-click the created folder.

3. Select [Share...] to open the [File Sharing] dialog box.



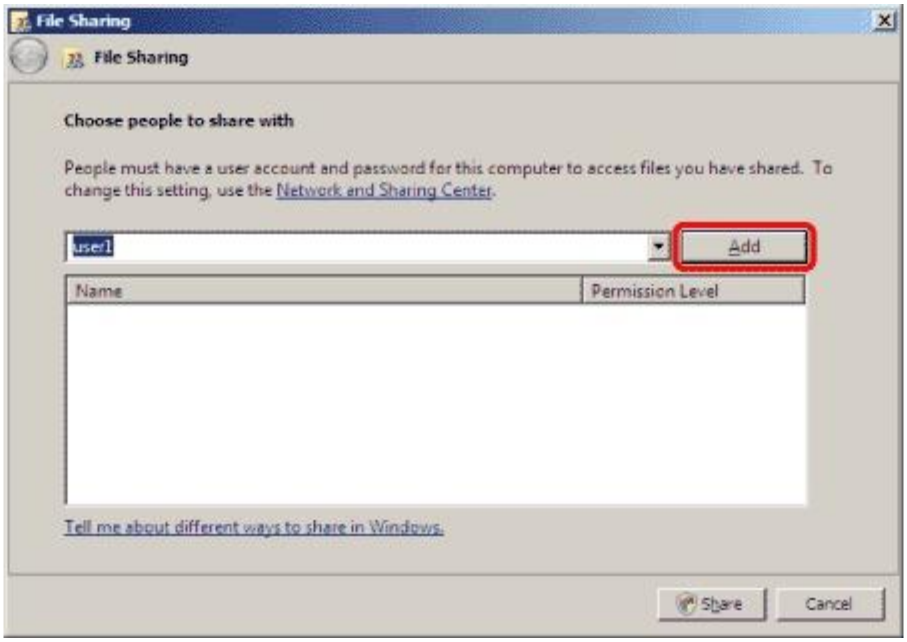
4. Click [▼] on the left side of [Add], and select the user



Choose people to share with

People must have a user account and password for this computer to access files you have shared. To change this setting, use the Network and Sharing Center.

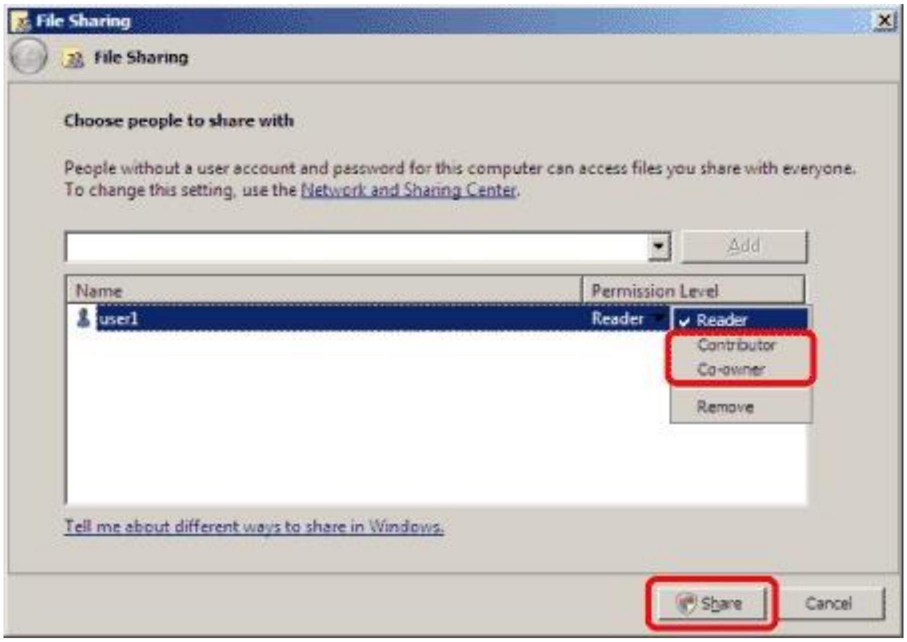
5. Click [Add].



Choose people to share with

People must have a user account and password for this computer to access files you have shared. To change this setting, use the Network and Sharing Center.

6. Select the added user. Select the [Contributor] or [Co-owner] check box. Click [Share].



File Sharing

Choose people to share with

People without a user account and password for this computer can access files you share with everyone. To change this setting, use the Network and Sharing Center.

Name	Permission Level
user1	Reader

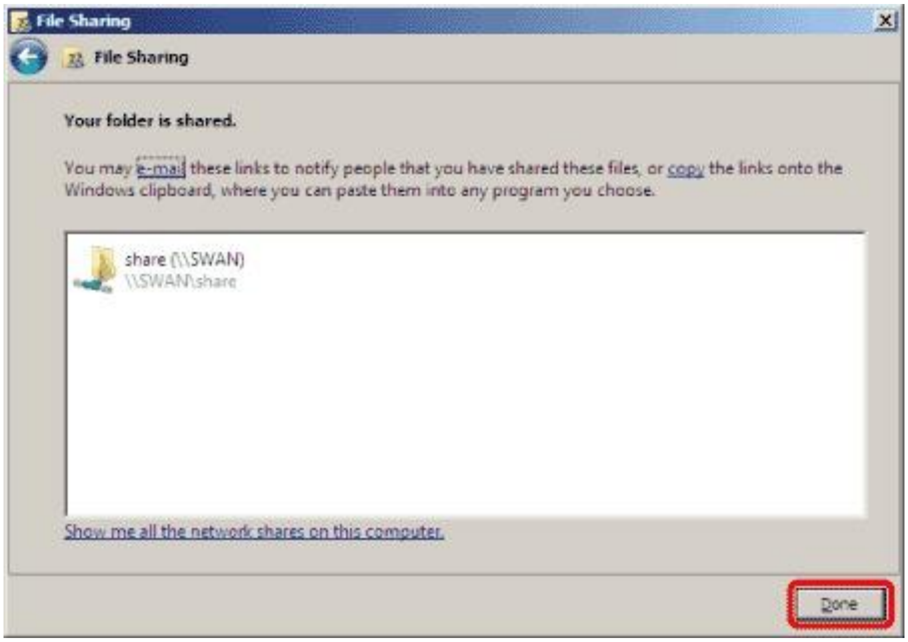
- If the [User Account Control] dialog box appears in Windows Server 2008, click [Continue].
- Access permissions in Windows Server 2008

- Reader: A reader can only view shared files.

- Contributor: A contributor can create, alter and delete shared files, but not alter access permissions.

- Co-owner: A co-owner can perform all file operations including creating, altering, deleting shared files and altering access permissions.

7. Click [Done] to close the [File Sharing] dialog box.



File Sharing

Your folder is shared.

You may e-mail these links to notify people that you have shared these files, or copy the links onto the Windows clipboard, where you can paste them into any program you choose.

share (\\SWAN)
\\SWAN\share

For Windows Server 2008 R2 users

1. Create a folder in any drive.

It is recommended to create the folder in a place where users can find it easily, such as the first level in C drive.

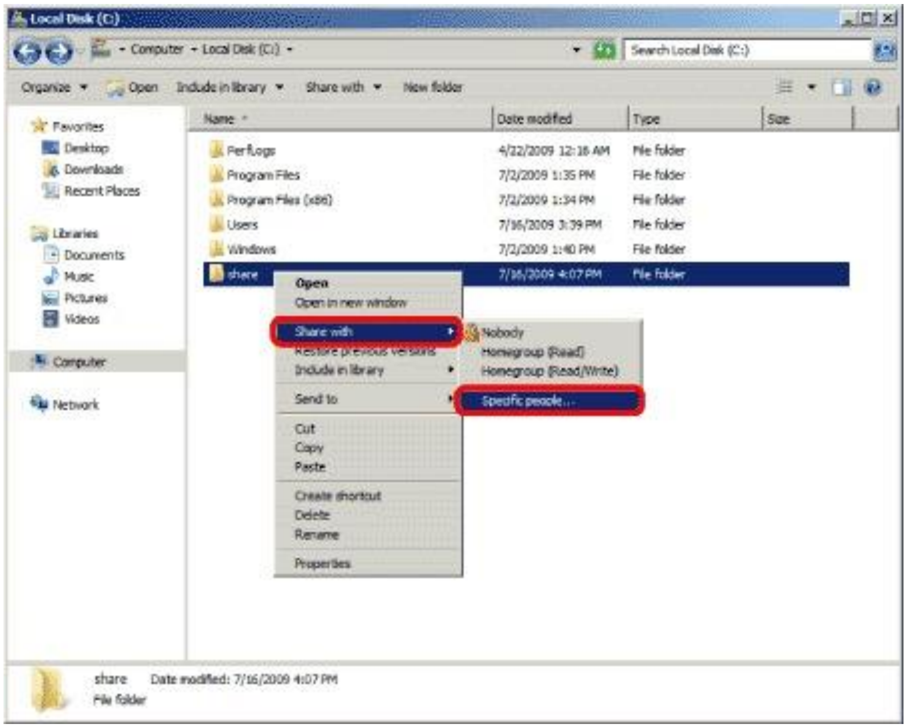
Ex) C:\share

NOTE:

It is recommended that you write down the folder name you created here.

2. Right-click the created folder.

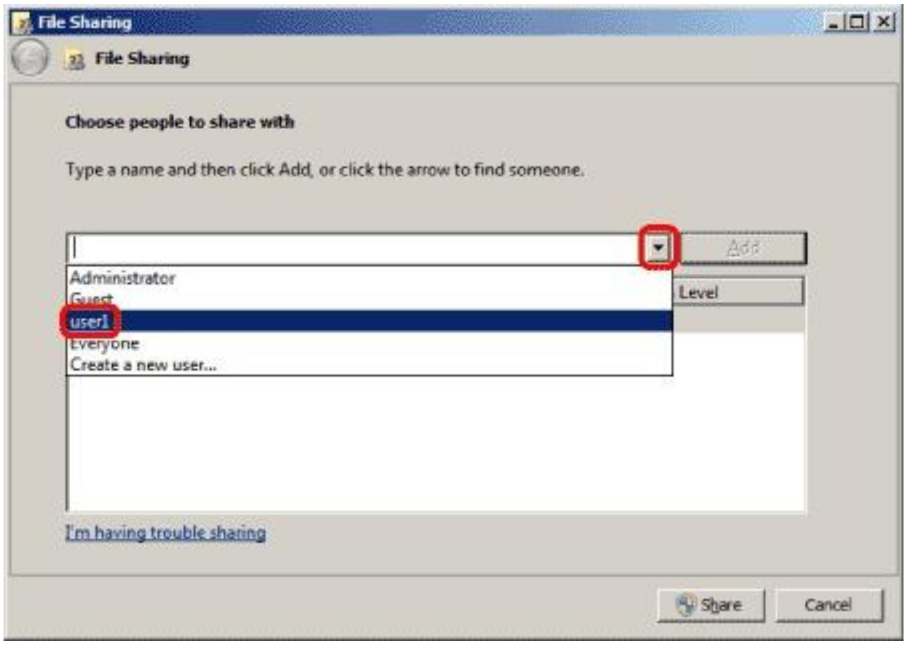
3. Select [Share with], and then select [Specific people...] to open the [File Sharing] dialog box.



Name	Date modified	Type	Size
PerfLogs	4/22/2009 12:16 AM	File folder	
Program Files	7/2/2009 1:35 PM	File folder	
Program Files (x86)	7/2/2009 1:34 PM	File folder	
Users	7/16/2009 3:39 PM	File folder	
Windows	7/2/2009 1:40 PM	File folder	
share	7/16/2009 4:07 PM	File folder	

share Date modified: 7/16/2009 4:07 PM
File folder

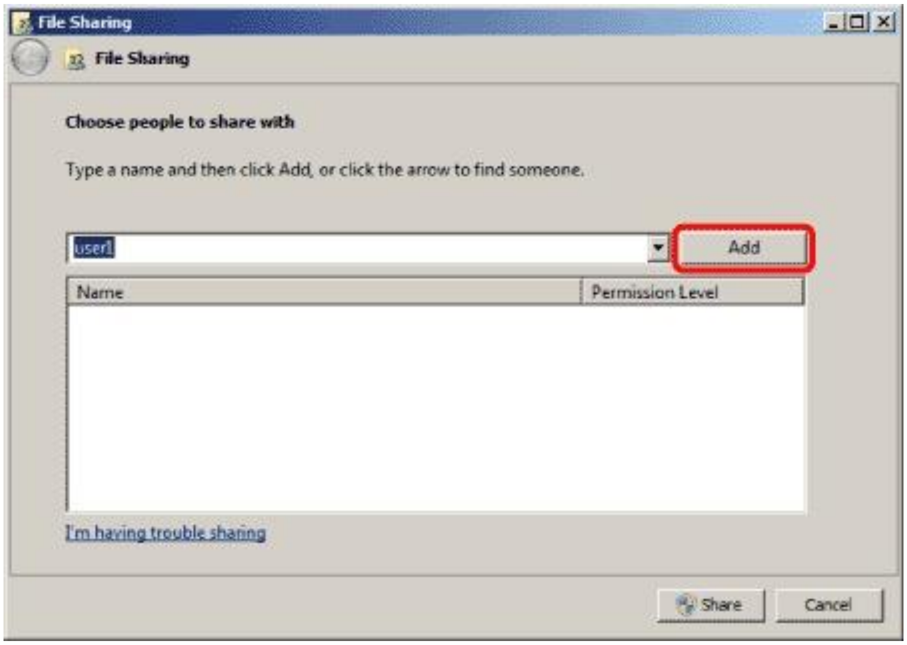
4. Click [▼] on the left side of [Add], and then select the user.



Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

5. Click [Add].

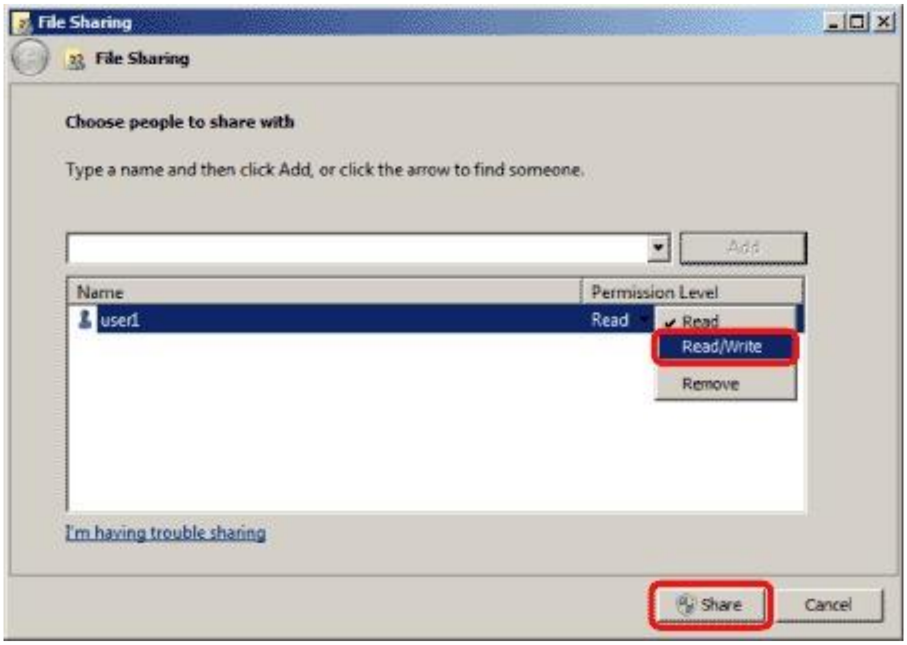


Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level

6. Select the added user. Select the [Read/Write] check box. Click [Share].



Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

Name	Permission Level
user1	Read

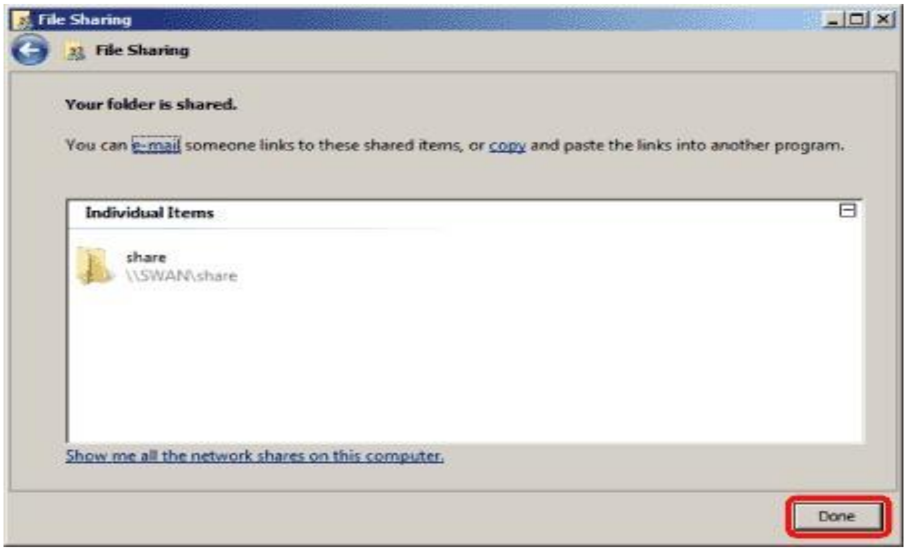
NOTE:

Access permissions in Windows Server 2008 R2

- Read: "Read" can only view shared files.

- Read/Write: "Read/Write" can create, alter and delete shared files, but not alter access permissions.

7. Click [Done] to close the [File Sharing] dialog box.



Your folder is shared.

You can e-mail someone links to these shared items, or copy and paste the links into another program.

share
\\SWAN\share

Sources: https://support.usa.canon.com/kb/index?page=content&id=ART108077

INFORMATION SHEET 1.3

Network Policies and Services

Learning Objectives:

After reading this Information Sheet, the learner is expected to:

a. Understand network policies and services

b. Install network policies and services

c. Value the importance of network security policy

Network Policy and Access Services (NPAS) is a component of Windows Server 2008. It replaces the Internet Authentication Service (IAS) from Windows Server 2003. NPAS helps you safeguard the health and security of a network.

The Network Policy Server is the core component of a NAP deployment. It is used to manage network access through the VPN server, RADIUS servers, and other points of access to the network. Depending on your network environment, you may deploy multiple NPS servers.

Network Policy and Access Services provides the following network connectivity solutions:

- Network Access Protection (NAP). NAP is a client health policy creation, enforcement, and remediation technology that is included in the Windows Vista® client operating system and in the Windows Server® 2008 operating system. With NAP, system administrators can establish and automatically enforce health policies, which can include software requirements, security update requirements, required computer configurations, and other settings. Client computers that are not in compliance with health policy can be provided restricted network access until their configuration is updated and brought into compliance with policy. Depending on how you choose to deploy NAP, noncompliant clients can be automatically updated so that users can quickly regain full network access without manually updating or reconfiguring their computers.

- Secure wireless and wired access. When you deploy 802.1X wireless access points, secure wireless access provides wireless users with a secure password-based authentication method that is easy to deploy. When you deploy 802.1X authenticating switches, wired access allows you to secure your network by ensuring that intranet users are authenticated before they can connect to the network or obtain an IP address using DHCP.
- Remote access solutions. With remote access solutions, you can provide users with virtual private network (VPN) and traditional dial-up access to your organization's network. You can also connect branch offices to your network with VPN solutions, deploy full-featured software routers on your network, and share Internet connections across the intranet.
- Central network policy management with RADIUS server and proxy. Rather than configuring network access policy at each network access server, such as wireless access points, 802.1X authenticating switches, VPN servers, and dial-up servers, you can create policies in a single location that specify all aspects of network connection requests, including who is allowed to connect, when they can connect, and the level of security they must use to connect to your network.

Role services for Network Policy and Access Services

When you install Network Policy and Access Services, the following role services are available:

- **Network Policy Server (NPS)**. NPS is the Microsoft implementation of a RADIUS server and proxy. You can use NPS to centrally manage network access through a variety of network access servers, including wireless access points, VPN servers, dial-up servers, and 802.1X authenticating switches. In addition, you can use NPS to deploy secure password authentication with Protected Extensible Authentication Protocol (PEAP)-MS-CHAP v2 for wireless connections. NPS also contains key components for deploying NAP on your network.

  The following technologies can be deployed after the installation of the NPS role service:

  - **NAP health policy server**. When you configure NPS as a NAP health policy server, NPS evaluates statements of health (SoH) sent by NAP-capable client computers that want to communicate on the network. You can configure NAP policies on NPS that allow client computers to update their configuration to become compliant with your organization's network policy.

  - **IEEE 802.11 Wireless**. Using the NPS MMC snap-in, you can configure 802.1X-based connection request policies for IEEE 802.11 wireless client network access. You can also configure wireless access points as Remote Authentication Dial-In User Service (RADIUS) clients in NPS, and use NPS as a RADIUS server to process connection requests, as well as perform authentication, authorization, and accounting for 802.11 wireless connections. You can fully integrate IEEE 802.11 wireless access with NAP when you deploy a wireless 802.1X authentication infrastructure so that the health status of wireless clients is verified against health policy before clients are allowed to connect to the network.
  - **IEEE 802.3 Wired**. Using the NPS MMC snap-in, you can configure 802.1X-based connection request policies for IEEE 802.3 wired client Ethernet network access. You can also configure 802.1X-compliant switches as RADIUS clients in NPS, and use NPS as a RADIUS server to process connection requests, as well as perform authentication, authorization, and accounting for 802.3 Ethernet connections. You can fully integrate IEEE 802.3 wired client access with NAP when you deploy a wired 802.1X authentication infrastructure.
  - **RADIUS server**. NPS performs centralized connection authentication, authorization, and accounting for wireless, authenticating switch, and remote access dial-up and VPN connections. When you use NPS as a RADIUS server, you configure network access servers, such as wireless access points and VPN servers, as RADIUS clients in NPS. You also configure network policies that NPS uses to authorize connection requests, and you can configure RADIUS accounting so that NPS logs accounting information to log files on the local hard disk or in a Microsoft® SQL Server™ database.
  - **RADIUS proxy**. When you use NPS as a RADIUS proxy, you configure connection request policies that tell the NPS server which connection requests to forward to other RADIUS servers and to which RADIUS servers you want to forward connection requests. You can also configure NPS to forward accounting data to be logged by one or more computers in a remote RADIUS server group.

- **Routing and Remote Access**. With Routing and Remote Access, you can deploy VPN and dial-up remote access services and multiprotocol LAN-to-LAN, LAN-to-WAN, VPN, and network address translation (NAT) routing services.

The following technologies can be deployed during the installation of the Routing and Remote Access role service:

- **Remote Access Service**. Using Routing and Remote Access, you can deploy Point-to-Point Tunneling Protocol (PPTP), Secure Socket Tunneling Protocol (SSTP), or Layer Two Tunneling Protocol (L2TP) with Internet Protocol security (IPsec) VPN connections to provide end users with remote access to your organization's network. You can also create a site-to-site VPN connection between two servers at different locations. Each server is configured with Routing and Remote Access to send private data securely. The connection between the two servers can be persistent (always on) or on-demand (demand-dial).

  Remote Access also provides traditional dial-up remote access to support mobile users or home users who are dialing in to an organization's intranets. Dial-up equipment that is installed on the server running Routing and Remote Access answers incoming connection requests from dial-up networking clients. The remote access server answers the call, authenticates and authorizes the caller, and transfers data between the dial-up networking client and the organization intranet.

- **Routing**. Routing provides a full-featured software router and an open platform for routing and internetworking. It offers routing services to businesses in local area network (LAN) and wide area network (WAN) environments.

  Health Registration Authority (HRA). HRA is a NAP component that issues health certificates to clients that pass the health policy verification that is performed by NPS using the client SoH. HRA is used only with the NAP IPsec enforcement method.

- **Host Credential Authorization Protocol (HCAP)**. HCAP allows you to integrate your Microsoft NAP solution with Cisco Network Access Control Server. When you deploy HCAP with NPS and NAP, NPS can perform client health evaluation and the authorization of Cisco 802.1X access clients.

Managing the Network Policy and Access Services server role

The following tools are provided to manage the Network Policy and Access Services server role:

- **NPS MMC snap-in**. Use the NPS MMC to configure a RADIUS server, RADIUS proxy, or NAP technology.

- **Netsh commands for NPS**. The Netsh commands for NPS provide a command set that is fully equivalent to all configuration settings that are available through the NPS MMC snap-in. Netsh commands can be run manually at the Netsh prompt or in administrator scripts.
- **HRA MMC snap-in**. Use the HRA MMC to designate the certification authority (CA) that HRA uses to obtain health certificates for client computers and to define the NPS server to which HRA sends client SoHs for verification against health policy.
- **Netsh commands for HRA**. The Netsh commands for HRA provide a command set that is fully equivalent to all configuration settings that are available through the HRA MMC snap-in. Netsh commands can be run manually at the Netsh prompt or in administrator-authored scripts.
- **NAP Client Management MMC snap-in**. You can use the NAP Client Management snap-in to configure security settings and user interface settings on client computers that support the NAP architecture.
- **Netsh commands for configuring NAP client settings**. The Netsh commands for NAP client settings provide a command set that is fully equivalent to all configuration settings that are available through the NAP Client Management snap-in. Netsh commands can be run manually at the Netsh prompt or in administrator-authored scripts.
- **Routing and Remote Access MMC snap-in**. Use this MMC snap-in to configure a VPN server, a dial-up networking server, a router, NAT, VPN and NAT, or a VPN site-to-site connection.
- **Netsh commands for remote access**. The Netsh commands for remote access provide a command set that is fully equivalent to all remote access configuration settings that are available through the Routing and Remote Access MMC snap-in. Netsh commands can be run manually at the Netsh prompt or in administrator scripts.
- **Netsh commands for routing**. The Netsh commands for routing provide a command set that is fully equivalent to all routing configuration settings that are available through the Routing and Remote Access MMC snap-in. Netsh commands can be run manually at the Netsh prompt or in administrator scripts.
- **Wireless Network (IEEE 802.11) Policies - Group Policy Management Console (GPMC)**. The Wireless Network (IEEE 802.11) Policies extension automates the configuration of wireless network settings on computers with wireless network adapter drivers that support the Wireless LAN Autoconfiguration

Service (WLAN Autoconfig Service). You can use the Wireless Network (IEEE 802.11) Policies extension in the Group Policy Management Console to specify configuration settings for either or both Windows XP and Windows Vista wireless clients. Wireless Network (IEEE 802.11) Policies Group Policy extensions include global wireless settings, the list of preferred networks, Wi-Fi Protected Access (WPA) settings, and IEEE 802.1X settings.

When configured, the settings are downloaded to Windows wireless clients that are members of the domain. The wireless settings configured by this policy are part of the Computer Configuration Group Policy. By default, Wireless Network (IEEE 802.11) Policies are not configured or enabled.

- **Netsh commands for wireless local area network (WLAN)**. Netsh WLAN is an alternative to using Group Policy to configure Windows Vista wireless connectivity and security settings. You can use the Netsh wlan commands to configure the local computer, or to configure multiple computers using a logon script. You can also use the Netsh wlan commands to view wireless Group Policy settings and administer Wireless Internet Service Provider (WISP) and user wireless settings.

- **Wired Network (IEEE 802.3) Policies - Group Policy Management Console (GPMC)**. You can use the Wired Network (IEEE 802.3) Policies to specify and modify configuration settings for Windows Vista clients that are equipped with network adapters and drivers that support Wired AutoConfig Service. Wireless Network (IEEE 802.11) Policies Group Policy extensions include global wired and IEEE 802.1X settings. These settings include the entire set of wired configuration items associated with the **General** tab and the **Security** tab.

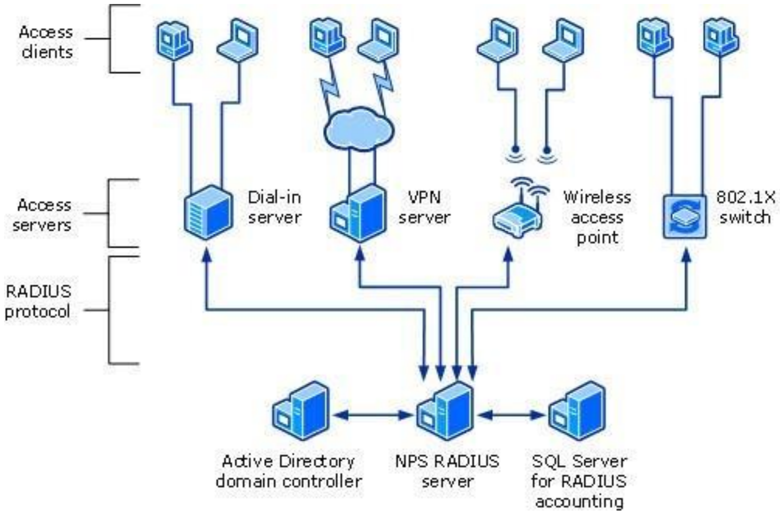
Using NPS as a RADIUS server

You can use NPS as a RADIUS server when:

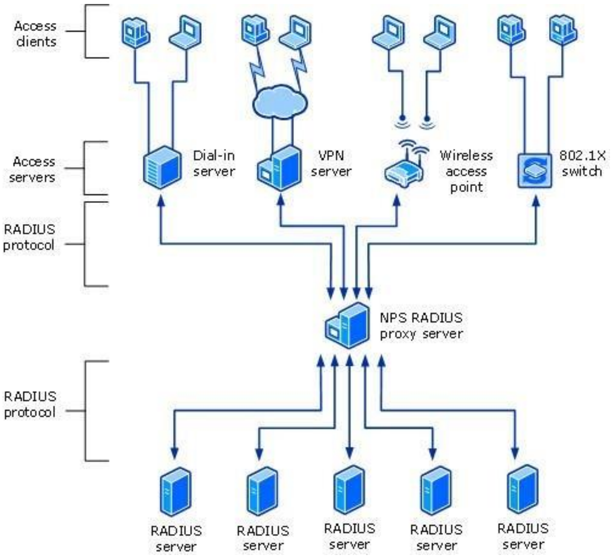
- You are using an AD DS domain or the local SAM user accounts database as your user account database for access clients.
- You are using Remote Access on multiple dial-up servers, VPN servers, or demand-dial routers and you want to centralize both the configuration of network policies and connection logging and accounting.
- You are outsourcing your dial-up, VPN, or wireless access to a service provider. The access servers use RADIUS to authenticate and authorize connections that are made by members of your organization.

- You want to centralize authentication, authorization, and accounting for a heterogeneous set of access servers.

The following illustration shows NPS as a RADIUS server for a variety of access clients.



The following illustration shows NPS as a RADIUS proxy between RADIUS clients and RADIUS servers.



With NPS, organizations can also outsource remote access infrastructure to a service provider while retaining control over user authentication, authorization, and accounting.

NPS configurations can be created for the following scenarios:

- Wireless access
- Organization dial-up or virtual private network (VPN) remote access
- Outsourced dial-up or wireless access
- Internet access
- Authenticated access to extranet resources for business partners

Source:

http://techgenix.com/understanding-configuring-network-policy-access-services-server-2012-part1/

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server 2012-r2-and-2012/hh831683(v=ws.11)

http://winintro.ru/nas.en/

INFORMATION SHEET 1.4

Setup Peer-to-Peer Network Access

Learning Objectives: After reading this Information Sheet, the learner is expected to:

a. Understand peer to peer networking

b. Create peer to peer server

c. Value the importance of peer to peer network access

In a peer-to-peer (P2P) network, the "peers" are computer systems which are connected to each other via the Internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client.

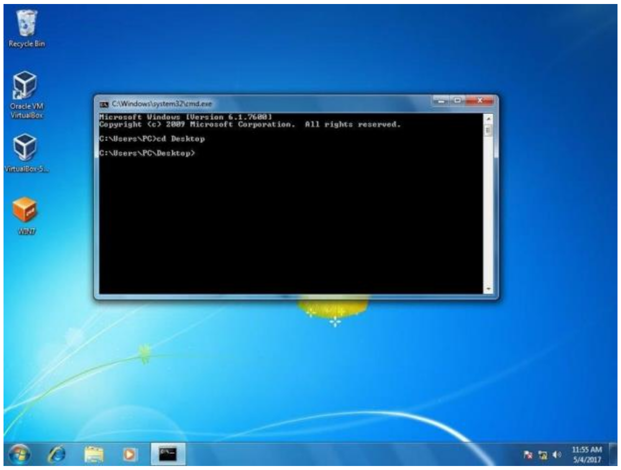
Once connected to the network, P2P software allows you to search for files on other people's computers. Meanwhile, other users on the network can search for files on your computer, but typically only within a single folder that you have designated to share. While P2P networking makes file sharing easy and convenient, is also has led to a lot of software piracy and illegal music downloads. Therefore, it is best to be on the safe side and only download software and music from legitimate websites.

Create peer to peer Server

- Computer Name→ IP Address→ Subnet Mask→ Primary DNS Server→ Test Network Connection using PING

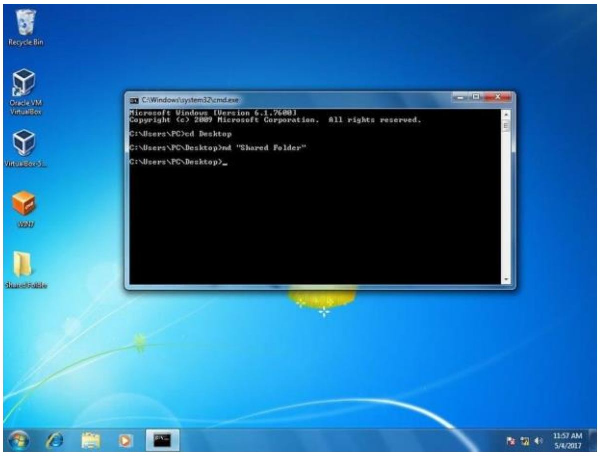
PEER TO PEER METWORK SHARING

Step 1: Navigate to the Desktop. Open command prompt and then use the command <cd Desktop> to change into the desktop directory. This step is simply for convenience so that it is easier to find the folder you're going to be working with . You can open command prompt by clicking on the windows button at the bottom left and tying <cmd>.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\PC>cd Desktop

C:\Users\PC\Desktop>
```

Step 2: Create Your Folder

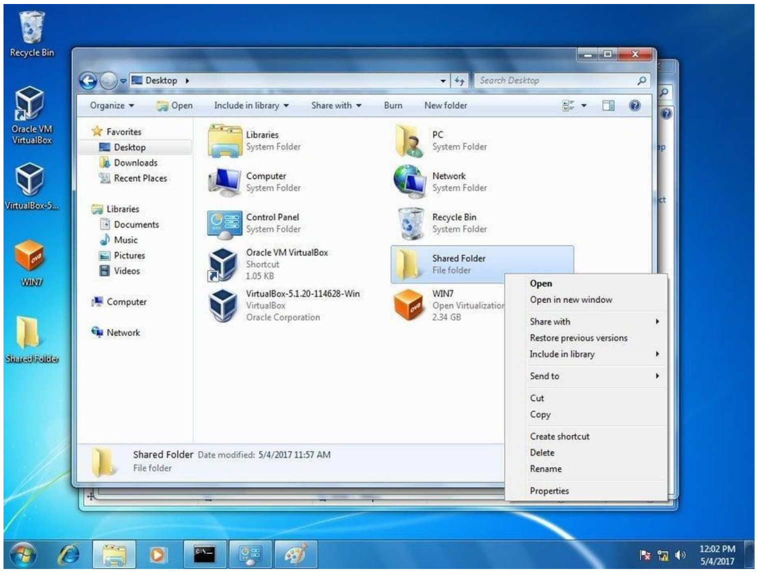


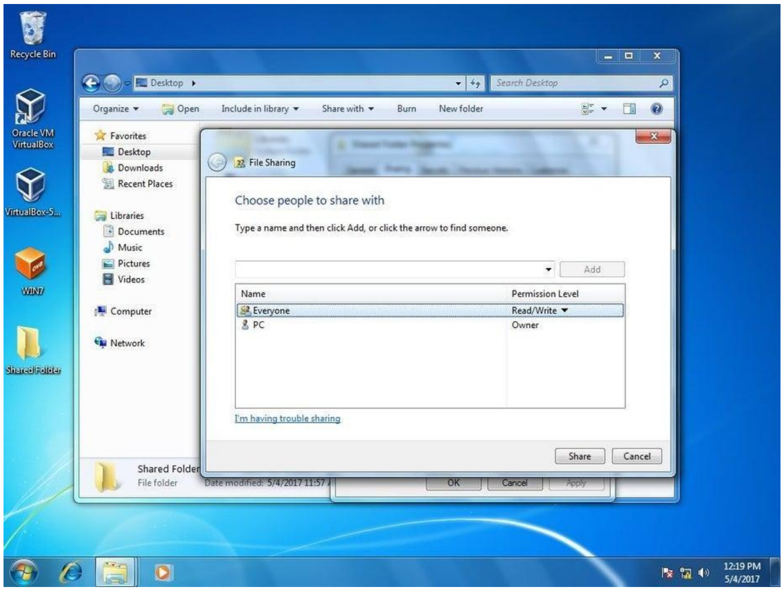
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\PC>cd Desktop

C:\Users\PC\Desktop>md "Shared Folder"

C:\Users\PC\Desktop>_
```

Use the command <md *folder name*> . Make sure that it is visible on your desktop. The command md allows you to create a new folder. After tying md press space and type the name of the folder you want to create. If the folder has more than one word in the name make sure to put the name in quotation marks.

Step 3: Navigate to the Folder and Open the Properties

Open the file explorer and go under the Desktop section. Left-click then right-click on the folder. The left-click highlights the folder, and the right-click opens a menu of options. Once the menu of options pops up click on the properties. When you open the properties window go to the sharing section.





Choose people to share with

Type a name and then click Add, or click the arrow to find someone.

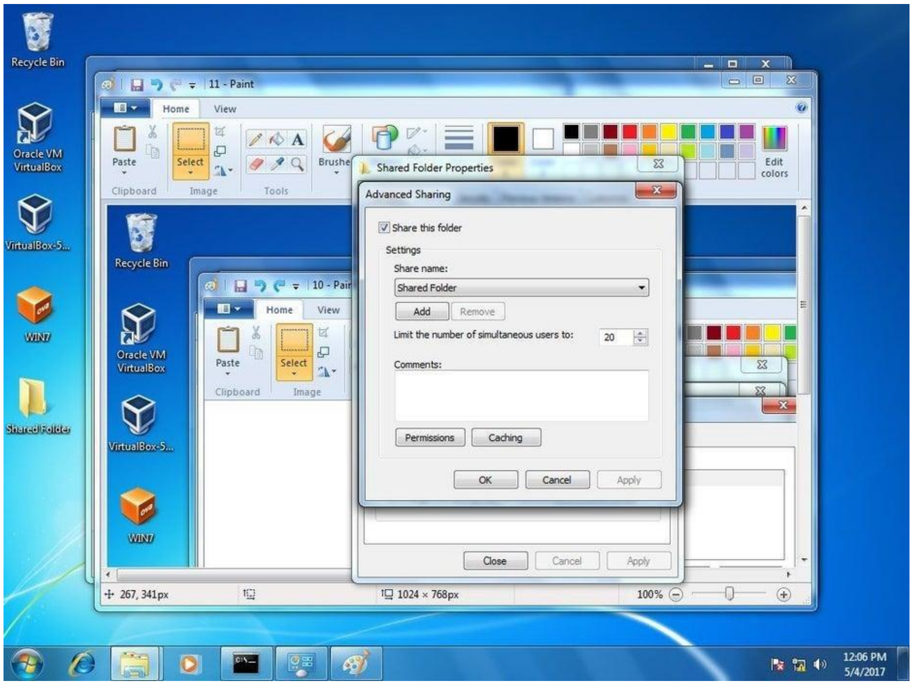
Name	Permission Level
Everyone	Read/Write
PC	Owner

I'm having trouble sharing

Step 4: Choose Who You Want to Share With.

Type <Everyone> and click add. Once you're done with that click share and then go to the advanced sharing.The default setting for the folder is set to only read. This means that if a person accesses the folder they will only be able to view the files and not actually be able to write to the folder.

Step 5: Sharing the Folder


Advanced Sharing

☑ Share this folder

Settings

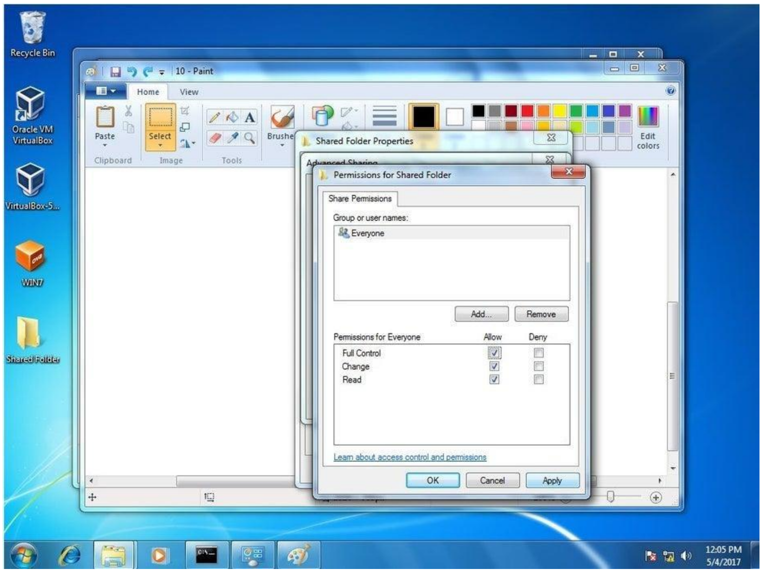
Share name: Shared Folder

Limit the number of simultaneous users to: 20

Comments:

Press the box that lets you share the folder and then go into the permissions section.

Step 6: Permissions


Permissions for Shared Folder

Share Permissions

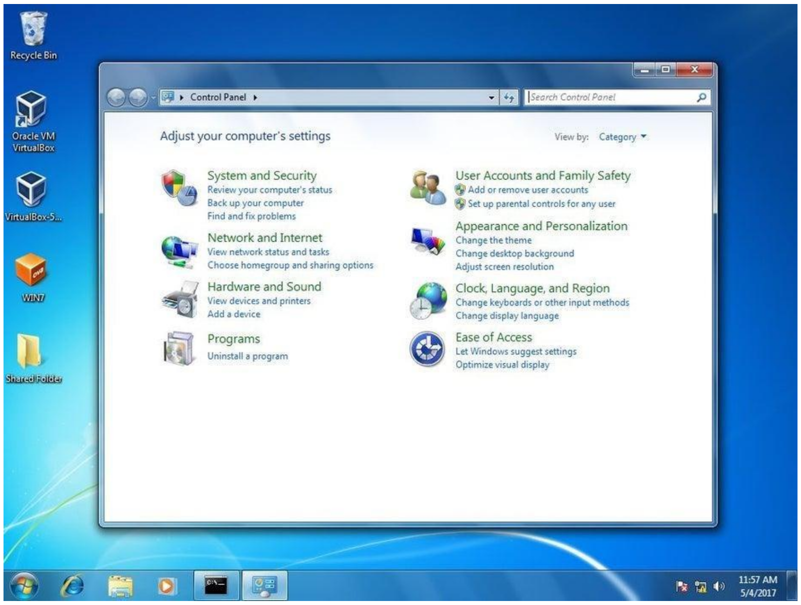
Group or user names:

Everyone

Permissions for Everyone	Allow	Deny
Full Control	☑	☐
Change	☑	☐
Read	☑	☐

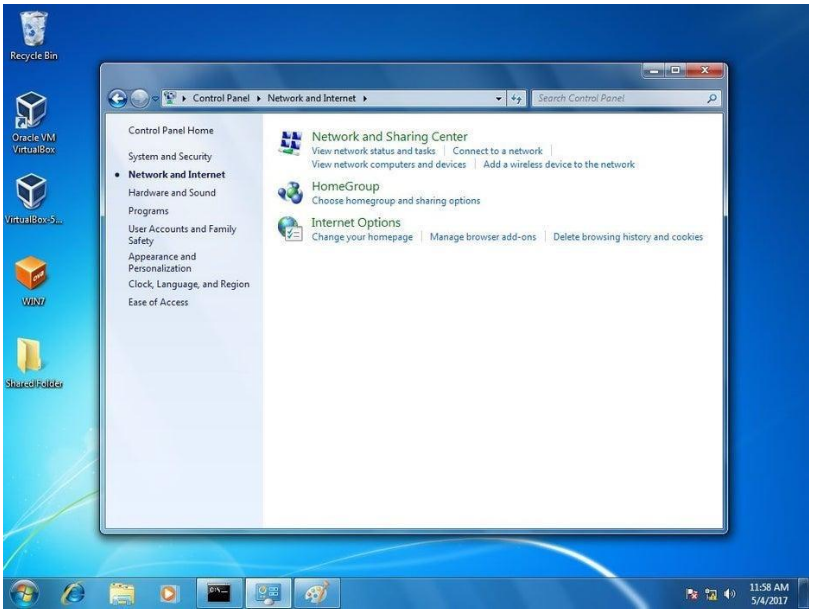
Make sure to give full control to the people that have access to the shared folder. Click Apply then click OK. Once you press OK you'll be back at the advanced sharing page. Press Apply and OK on that page too.

Step 7: Open Control Panel


Recycle Bin
Oracle VM VirtualBox
VirtualBox-5...
WIN7
Shared Folder
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display
11:57 AM
5/4/2017

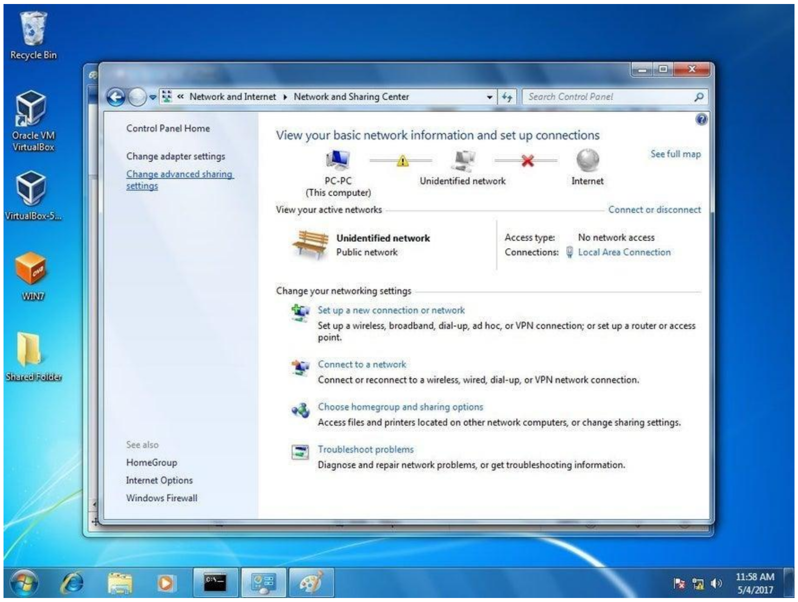
Navigate into the control panel and click on the Network and Internet section.

Step 8: Network and Sharing



Navigate into the Network and Sharing section.

Step 9: Advanced Sharing



Control Panel Home

Change adapter settings

Change advanced sharing settings

See also

HomeGroup

Internet Options

Windows Firewall

View your basic network information and set up connections

See full map

PC-PC (This computer) — Unidentified network — Internet

View your active networks

Connect or disconnect

Unidentified network
Public network

Access type: No network access
Connections: Local Area Connection

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

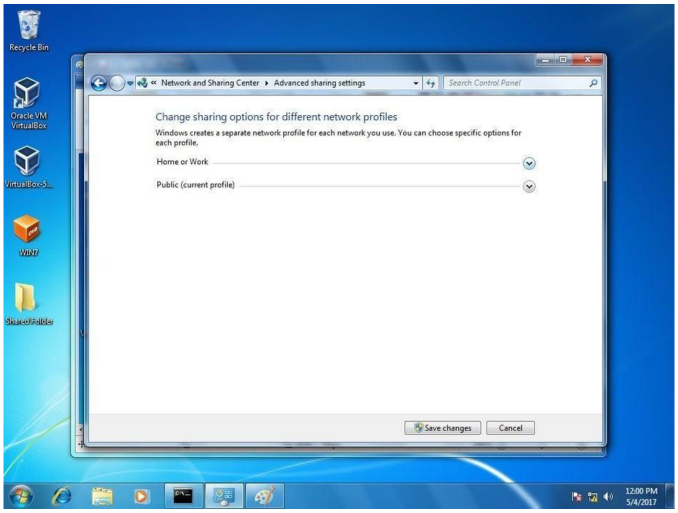
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Navigate to the advanced sharing settings.

Step 10: Choose Home and Work / Public



Change sharing options for different network profiles

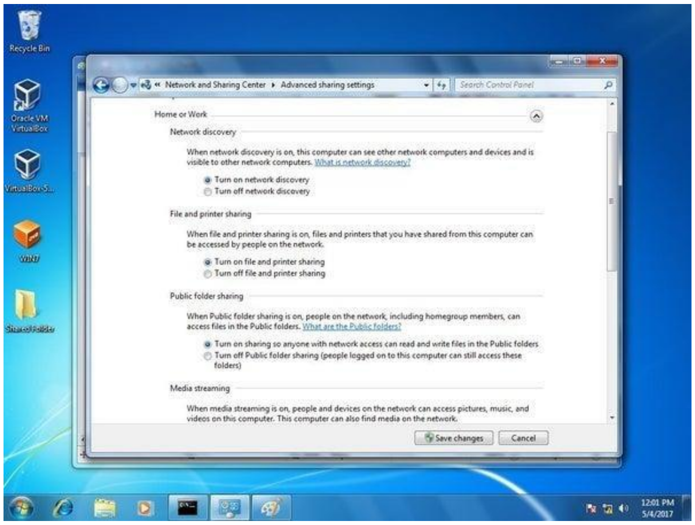
Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Home or Work

Public (current profile)

There are many settings that need to be changed in both of the options.

Step 11: Select All Options



Network and Sharing Center ▸ Advanced sharing settings

Home or Work

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

● Turn on network discovery
○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing
○ Turn off file and printer sharing

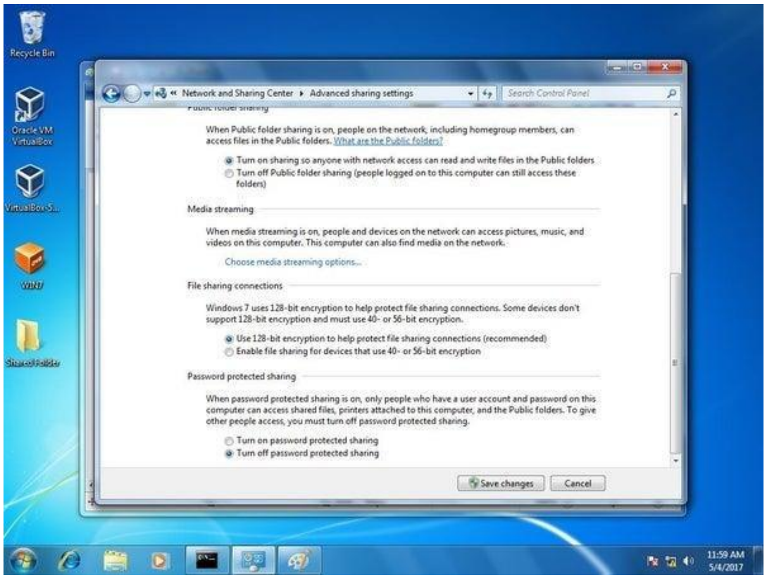
Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. What are the Public folders?

● Turn on sharing so anyone with network access can read and write files in the Public folders
○ Turn off Public folder sharing (people logged on to this computer can still access these folders)

Media streaming

When media streaming is on, people and devices on the network can access pictures, music, and videos on this computer. This computer can also find media on the network.



Network and Sharing Center ▸ Advanced sharing settings

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. What are the Public folders?

● Turn on sharing so anyone with network access can read and write files in the Public folders
○ Turn off Public folder sharing (people logged on to this computer can still access these folders)

Media streaming

When media streaming is on, people and devices on the network can access pictures, music, and videos on this computer. This computer can also find media on the network.

Choose media streaming options...

File sharing connections

Windows 7 uses 128-bit encryption to help protect file sharing connections. Some devices don't support 128-bit encryption and must use 40- or 56-bit encryption.

● Use 128-bit encryption to help protect file sharing connections (recommended)
○ Enable file sharing for devices that use 40- or 56-bit encryption

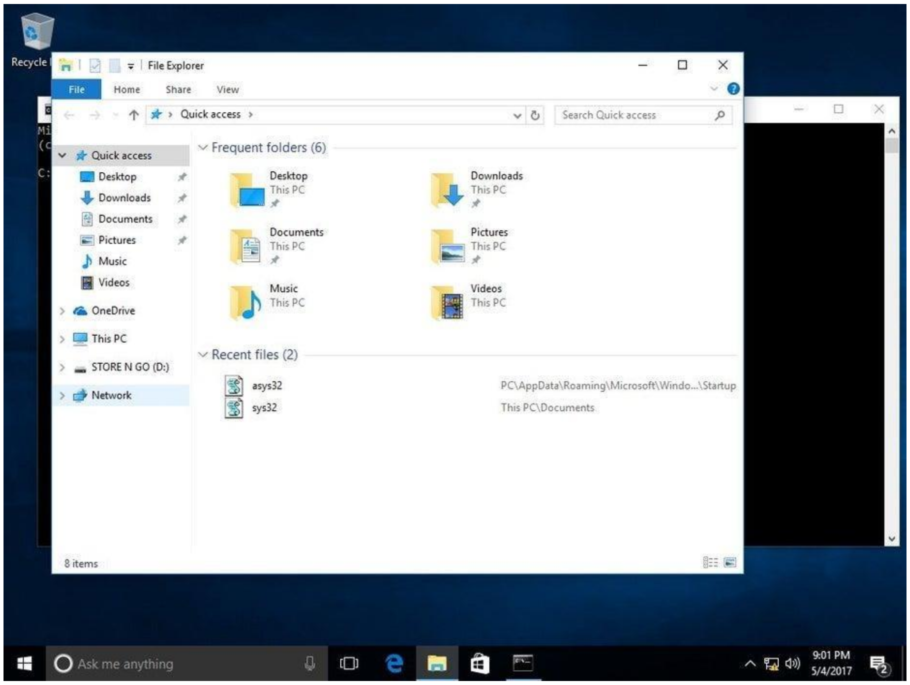
Password protected sharing

When password protected sharing is on, only people who have a user account and password on this computer can access shared files, printers attached to this computer, and the Public folders. To give other people access, you must turn off password protected sharing.

○ Turn on password protected sharing
● Turn off password protected sharing

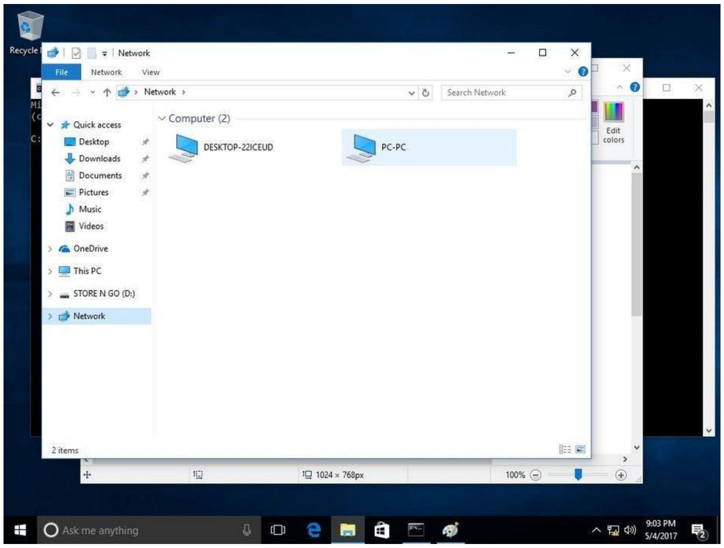
There are going to be many options, the ones you need for the sharing to work are pretty common sense like making sure that your device is allowed to be discovered. And turn off password protected sharing.

Step 12: Go Into Network



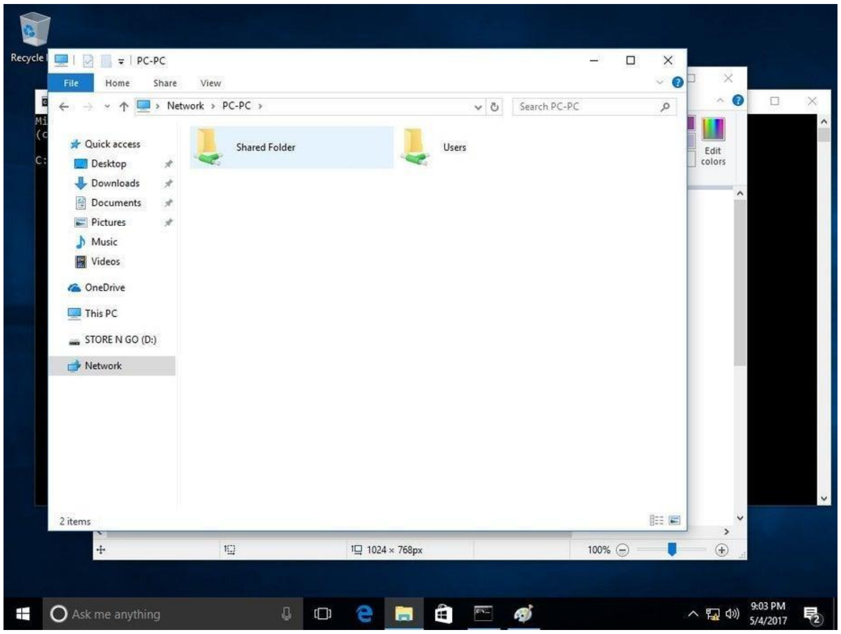
Go onto another computer and open the file explorer. Go into the Network section found on the left hand side at the bottom.

Step 13: Find the Device



Find the original device that the file was shared from.

Step 14: Find the Folder That Was Shared



Once you click on the device you will find all the files that were shared from it. You can tell that the folder is shared over the network because it has the green crossroads looking thing under its name.

Source:

https://techterms.com/definition/p2p

https://www.instructables.com/id/Peer-to-Peer-Network-Sharing/