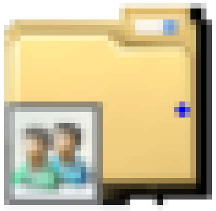
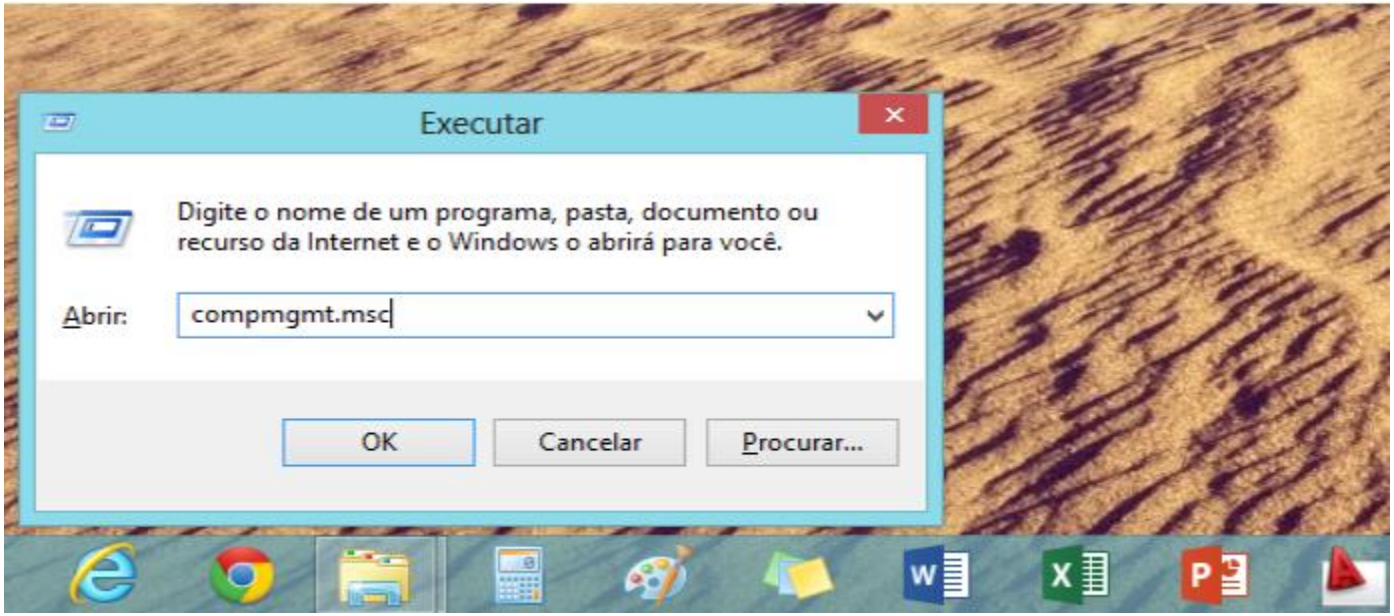
Pastas Compartilhadas

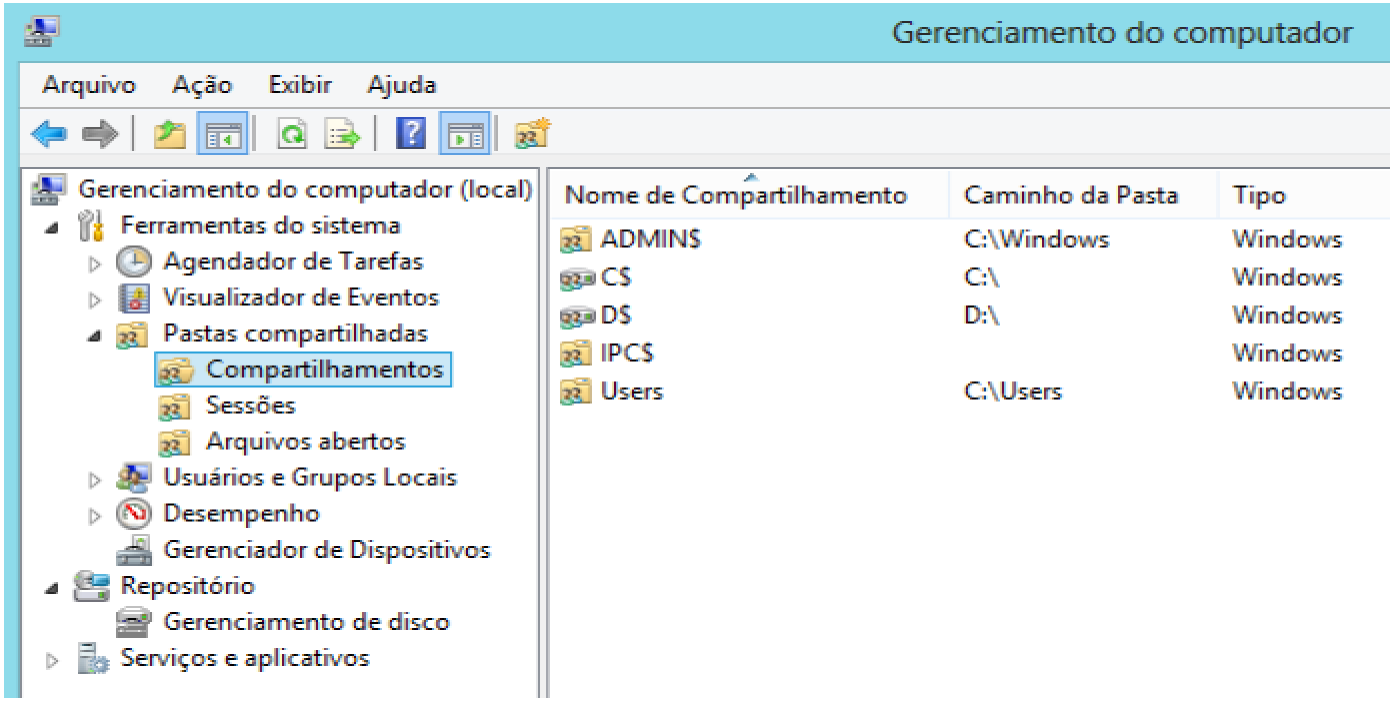
- **Pastas** definidas como **compartilhadas** podem ser acessadas por outros usuários conectados na mesma rede.
- Por padrão, o **Windows** conta com algumas **pastas** públicas que pode ser acessada por outros computadores, mas existe a possibilidade de compartilhar qualquer **pasta** do disco rígido.




Executar
Digite o nome de um programa, pasta, documento ou recurso da Internet e o Windows o abrirá para você.
Abrir:

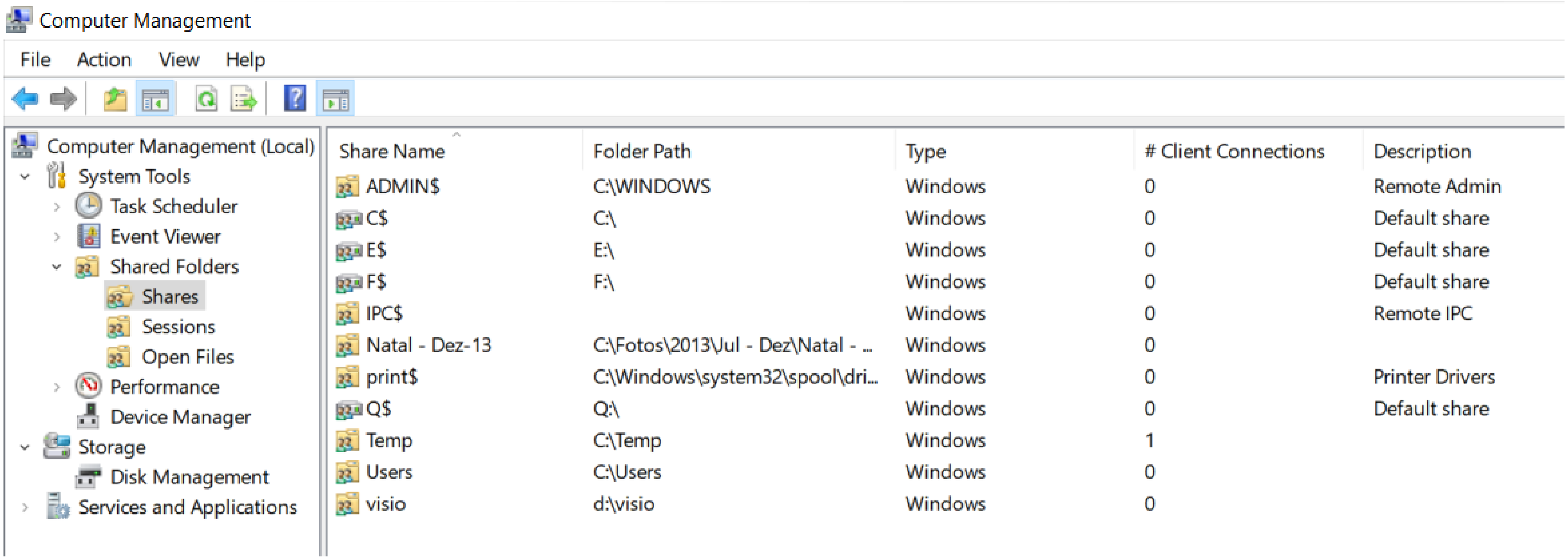
```
compmgmt.msc
```

Compartilhamentos



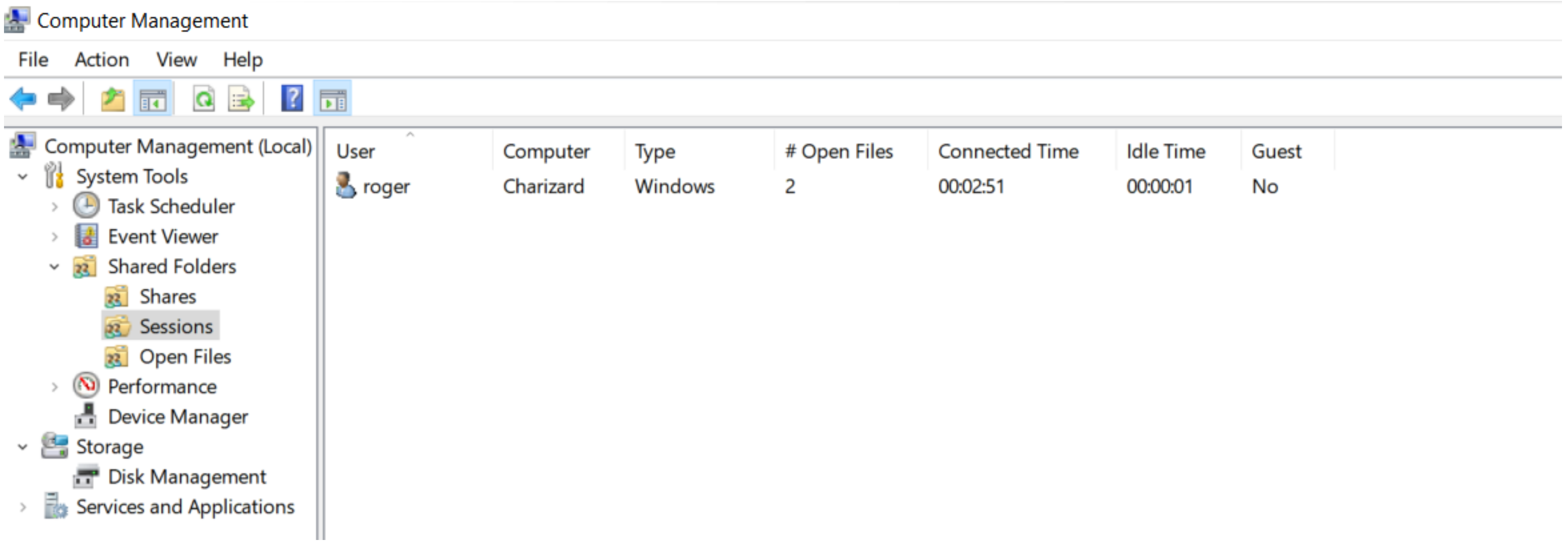
Nome de Compartilhamento	Caminho da Pasta	Tipo
ADMIN$	C:\Windows	Windows
C$	C:\	Windows
D$	D:\	Windows
IPC$		Windows
Users	C:\Users	Windows

Shares



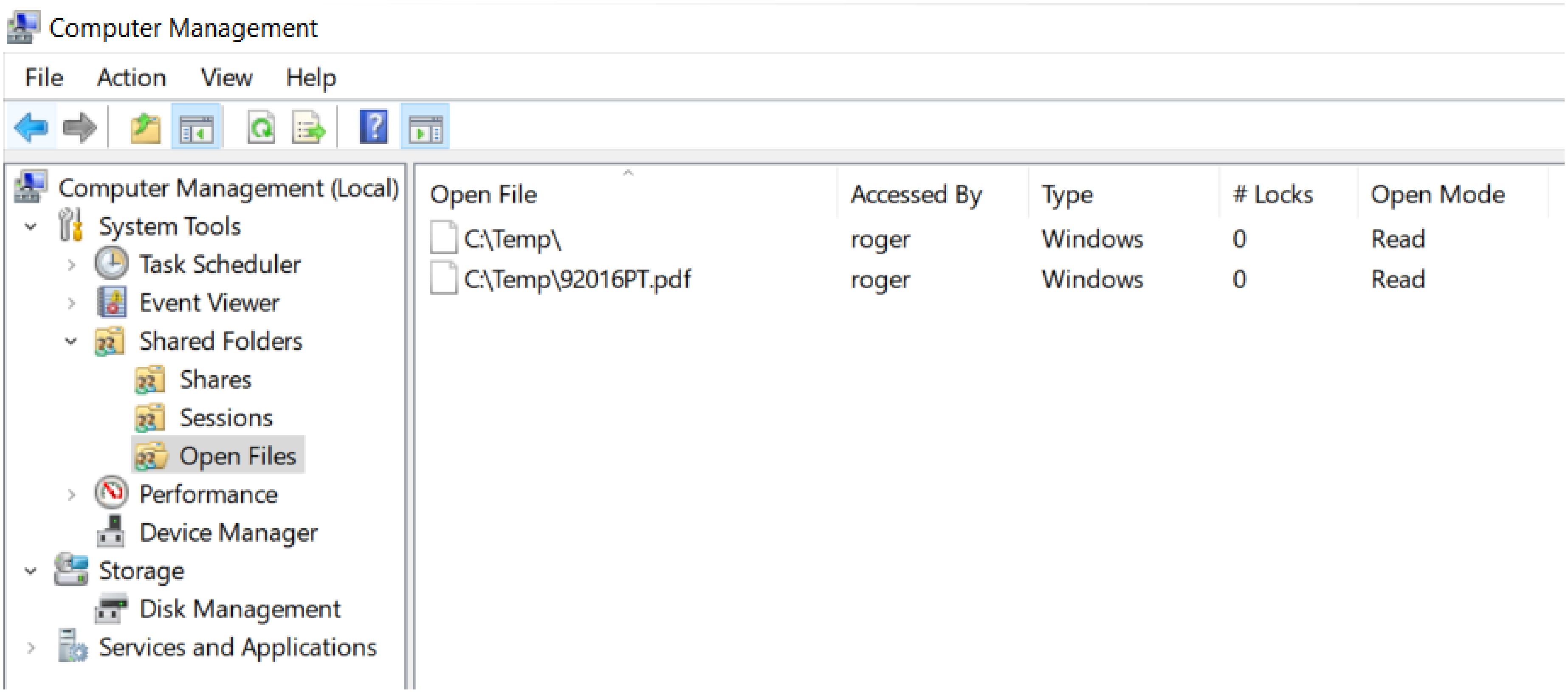
Share Name	Folder Path	Type	# Client Connections	Description
ADMIN$	C:\WINDOWS	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
E$	E:\	Windows	0	Default share
F$	F:\	Windows	0	Default share
IPC$		Windows	0	Remote IPC
Natal - Dez-13	C:\Fotos\2013\Jul - Dez\Natal - ...	Windows	0	
print$	C:\Windows\system32\spool\dri...	Windows	0	Printer Drivers
Q$	Q:\	Windows	0	Default share
Temp	C:\Temp	Windows	1	
Users	C:\Users	Windows	0	
visio	d:\visio	Windows	0	

Sessions



User	Computer	Type	# Open Files	Connected Time	Idle Time	Guest
roger	Charizard	Windows	2	00:02:51	00:00:01	No

Open Files



Open File	Accessed By	Type	# Locks	Open Mode
C:\Temp\	roger	Windows	0	Read
C:\Temp\92016PT.pdf	roger	Windows	0	Read

Administrative shares

Administrative shares are hidden network shares that exist on all Windows Servers.

The root of every volume is shared as a hidden share, and you name shares by appending a drive letter and a dollar sign.

For example, on LON-DC1 the root of the C:\ drive is shared as \\LON-DC1\C$. If there are multiple drives, each drive letter is a separate share.

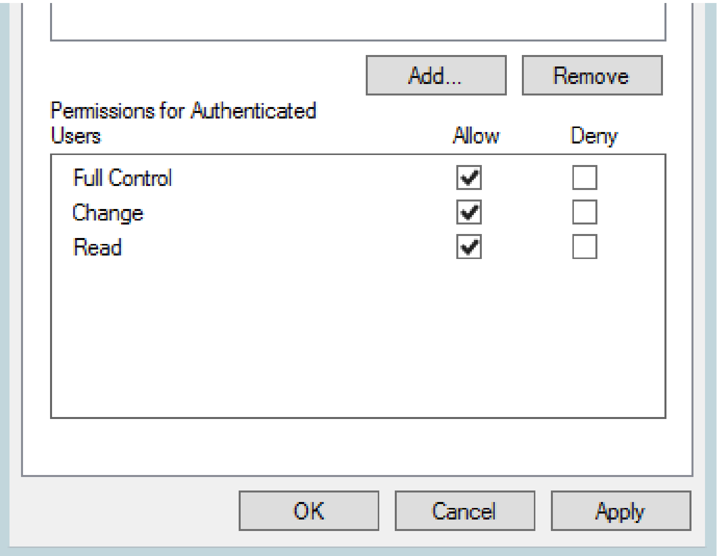
Administrative shares

- **Note:** In the past, administrative shares were available on client operating systems.
- However, beginning with Windows® 8, administrative shares were disabled by default on client systems.
- By default, only members of the Administrators group have permission to these shared folders.

Shared Folder Permissions

- You can assign shared folder permissions to users, groups, or computers. You cannot configure shared folder permissions for individual files or folders in the shared folder. Shared folder permissions are set for the shared folder itself, and apply universally to the entire contents of the shared folder for users who access the folder over the network.
- When you create a shared folder, the default assigned shared permission for the Everyone group is set to Read.

Note: Shared folder permissions apply only to users who access the folder over the network. They do not affect users who access the folder locally on the computer that stores the folder.

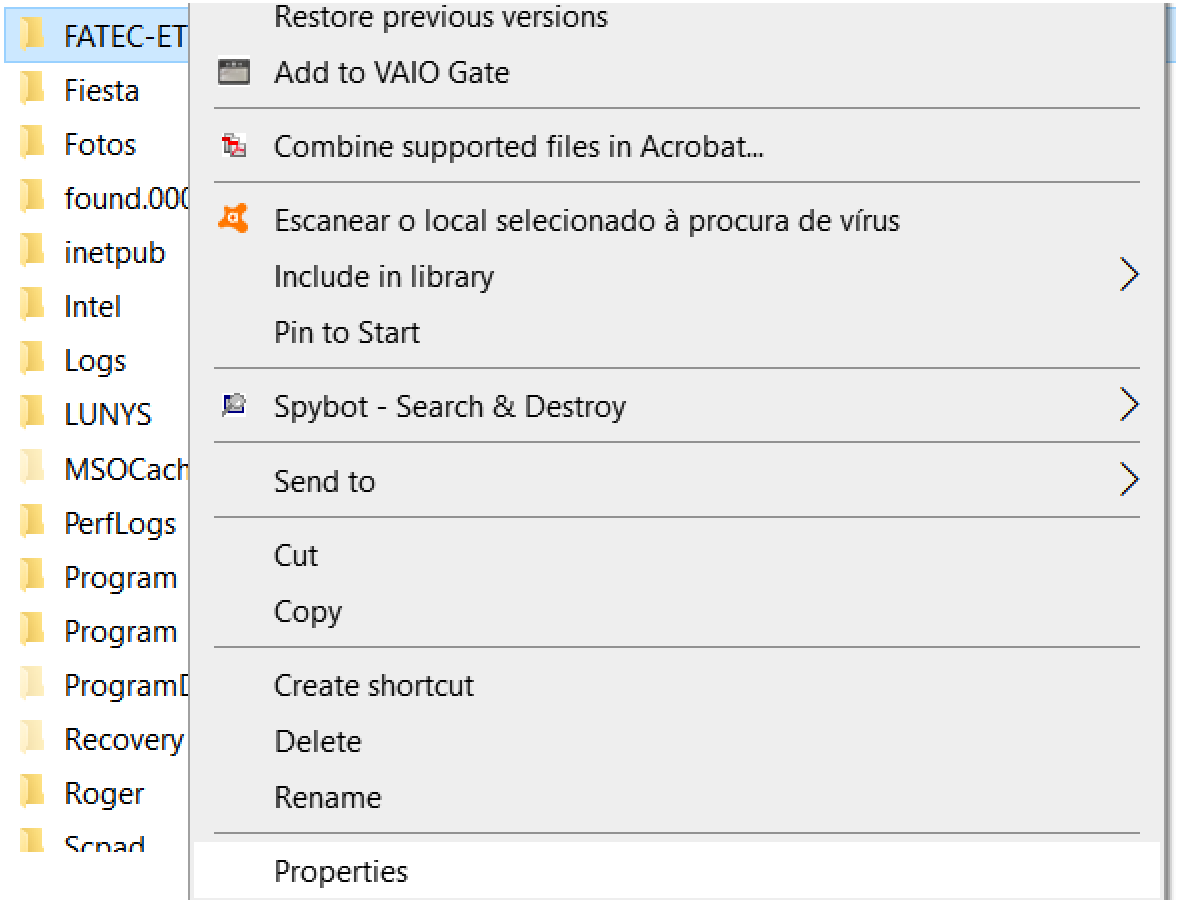


Permissions for Authenticated Users	Allow	Deny
Full Control	☑	□
Change	☑	□
Read	☑	□

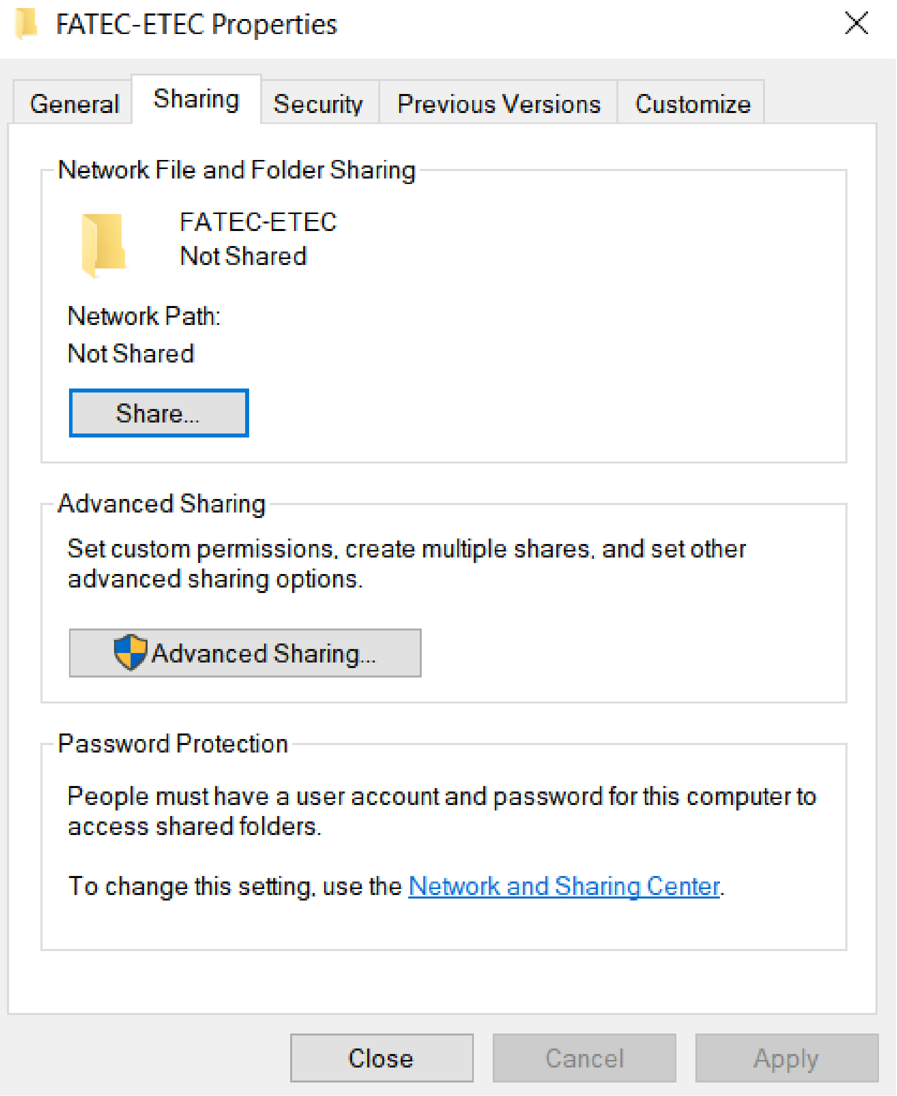
There are three types of share permissions: Full Control, Change, and Read.

1. **Full Control:** Enables users to “read,” “change,” as well as edit permissions and take ownership of files.
2. **Change:** Change means that user can read/execute/write/delete folders/files within share.
3. **Read:** Read allows users to view the folder’s contents.

Compartilhando Pasta



Compartilhando Pasta



FATEC-ETEC Properties

Network File and Folder Sharing

FATEC-ETEC
Not Shared

Network Path:
Not Shared

Advanced Sharing

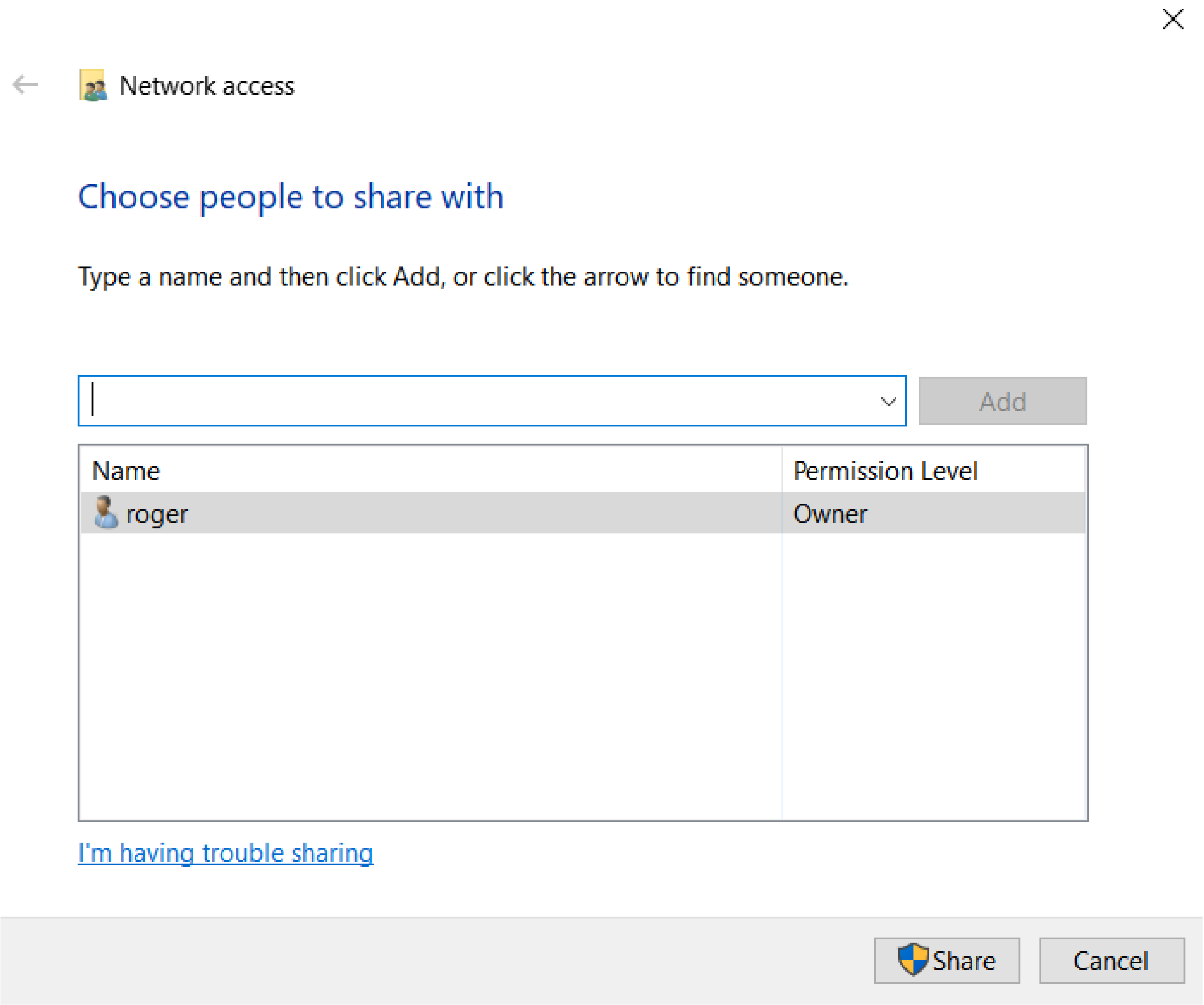
Set custom permissions, create multiple shares, and set other advanced sharing options.

Password Protection

People must have a user account and password for this computer to access shared folders.

To change this setting, use the Network and Sharing Center.

Compartilhando Pasta



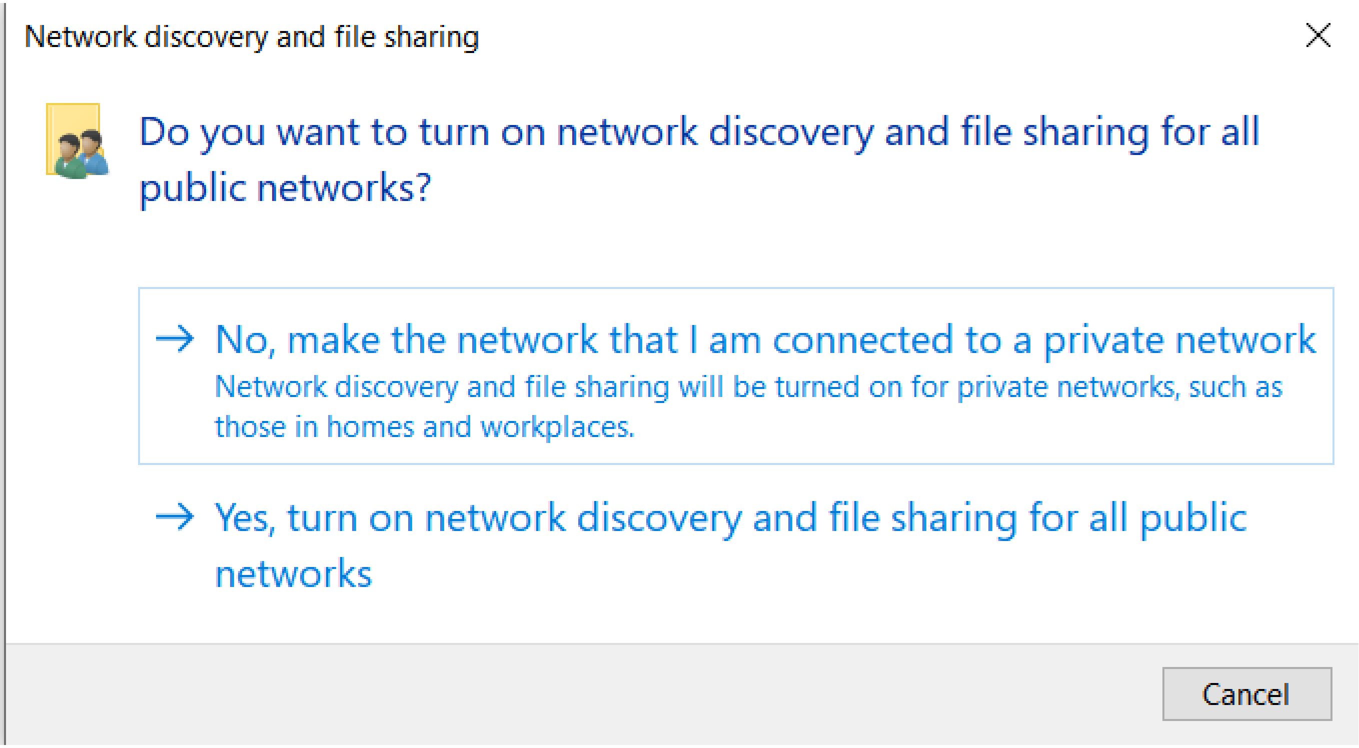
Network access

Choose people to share with

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

Name	Permission Level
roger	Owner

Compartilhando Pasta



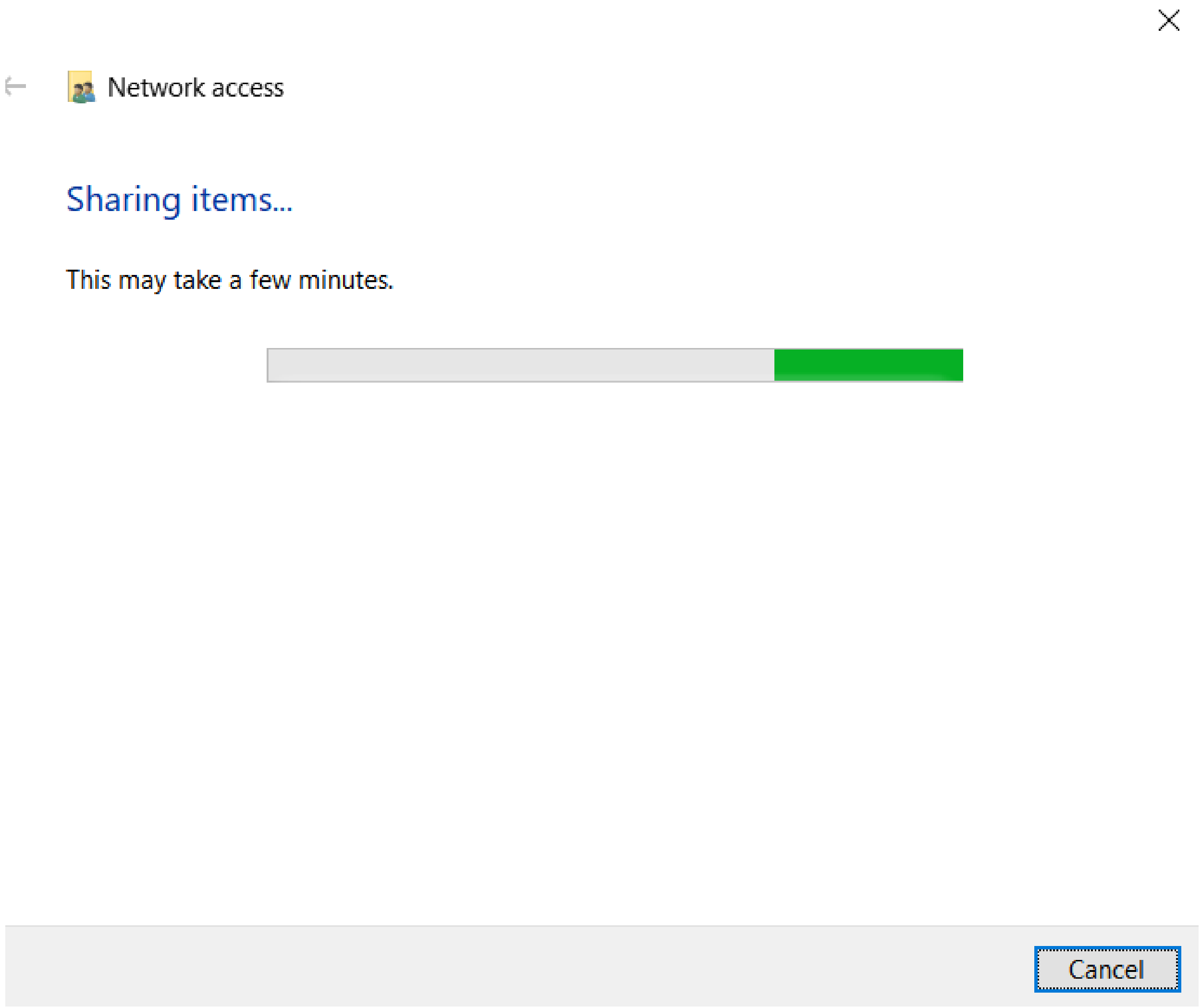
Network discovery and file sharing

Do you want to turn on network discovery and file sharing for all public networks?

→ No, make the network that I am connected to a private network
Network discovery and file sharing will be turned on for private networks, such as those in homes and workplaces.

→ Yes, turn on network discovery and file sharing for all public networks

Compartilhando Pasta

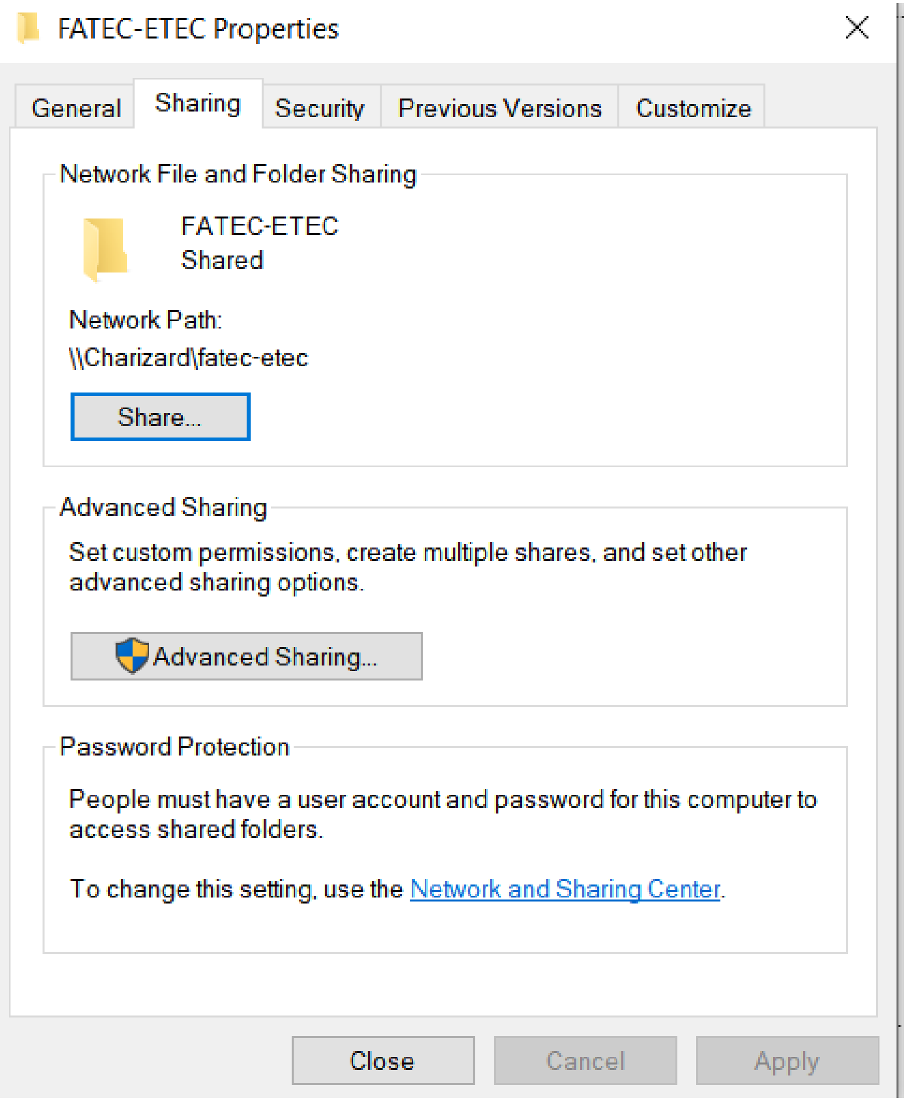


Network access

Sharing items...

This may take a few minutes.

Ver permissões Share



FATEC-ETEC Properties

Network File and Folder Sharing

FATEC-ETEC
Shared

Network Path:
\\Charizard\fatec-etec

Advanced Sharing

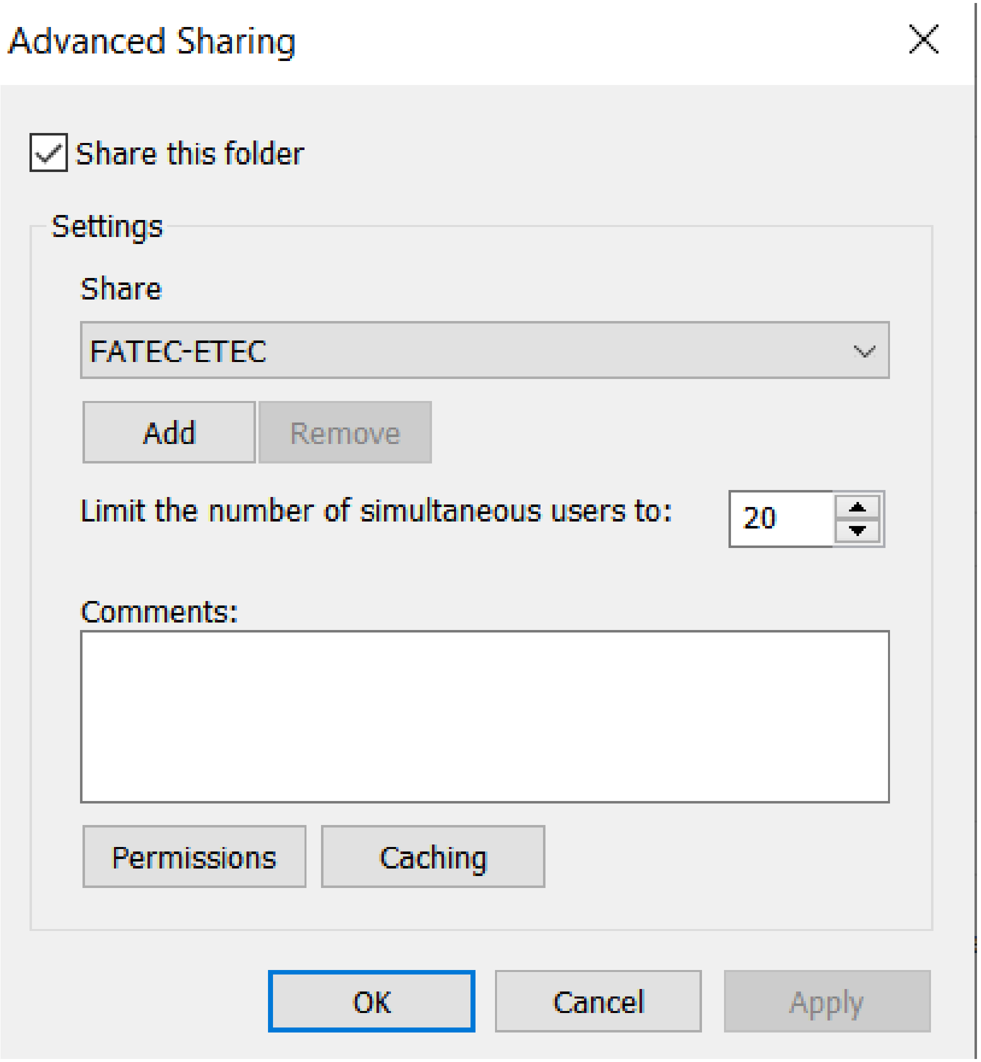
Set custom permissions, create multiple shares, and set other advanced sharing options.

Password Protection

People must have a user account and password for this computer to access shared folders.

To change this setting, use the Network and Sharing Center.

Ver permissões Share



Advanced Sharing

☑ Share this folder

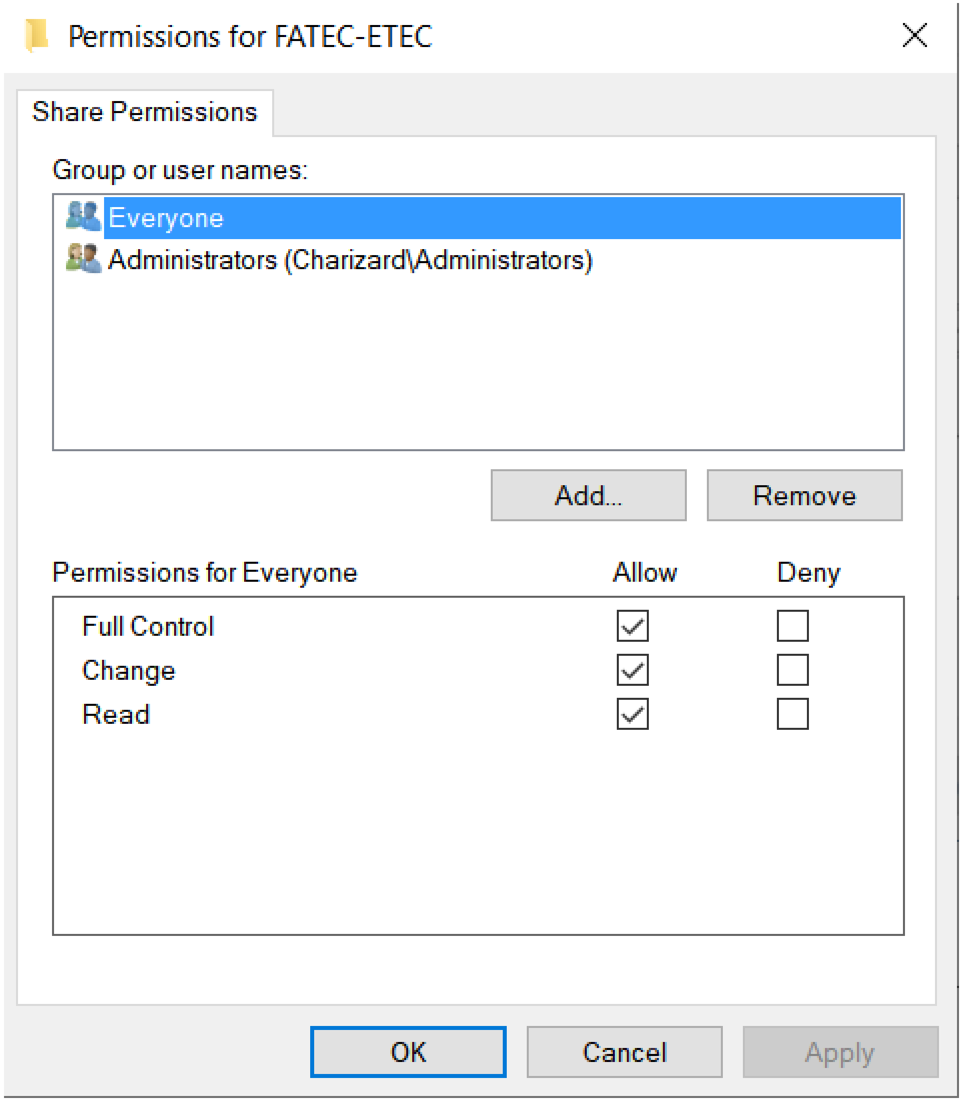
Settings

Share: FATEC-ETEC

Limit the number of simultaneous users to: 20

Comments:

Ver permissões Share



Permissions for FATEC-ETEC

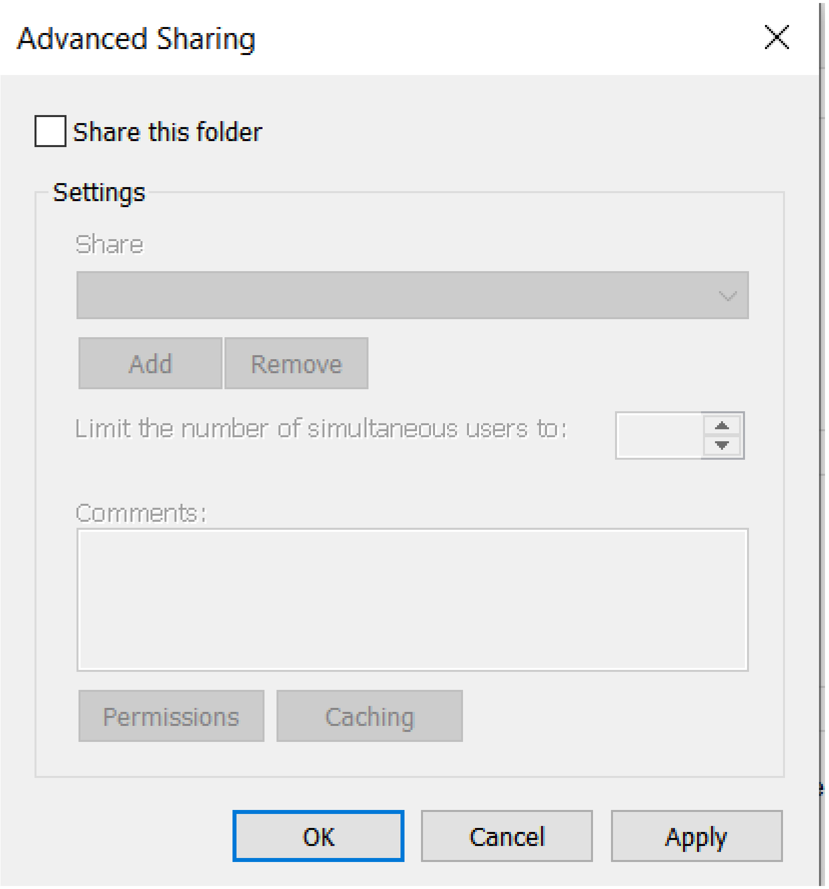
Share Permissions

Group or user names:

- Everyone
- Administrators (Charizard\Administrators)

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

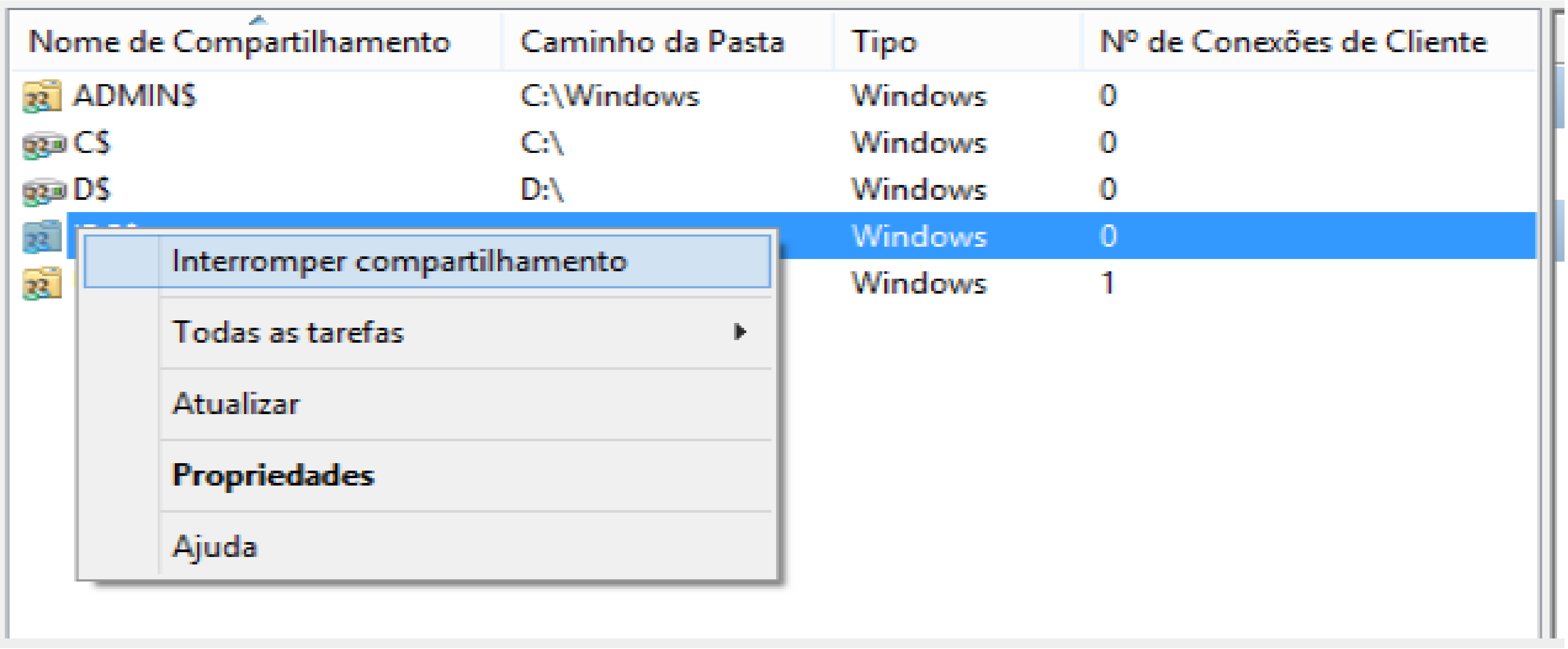
Parar compartilhamento



Advanced Sharing

□ Share this folder

Parar compartilhamento



Nome de Compartilhamento	Caminho da Pasta	Tipo	Nº de Conexões de Cliente
ADMIN$	C:\Windows	Windows	0
C$	C:\	Windows	0
D$	D:\	Windows	0
		Windows	0
		Windows	1

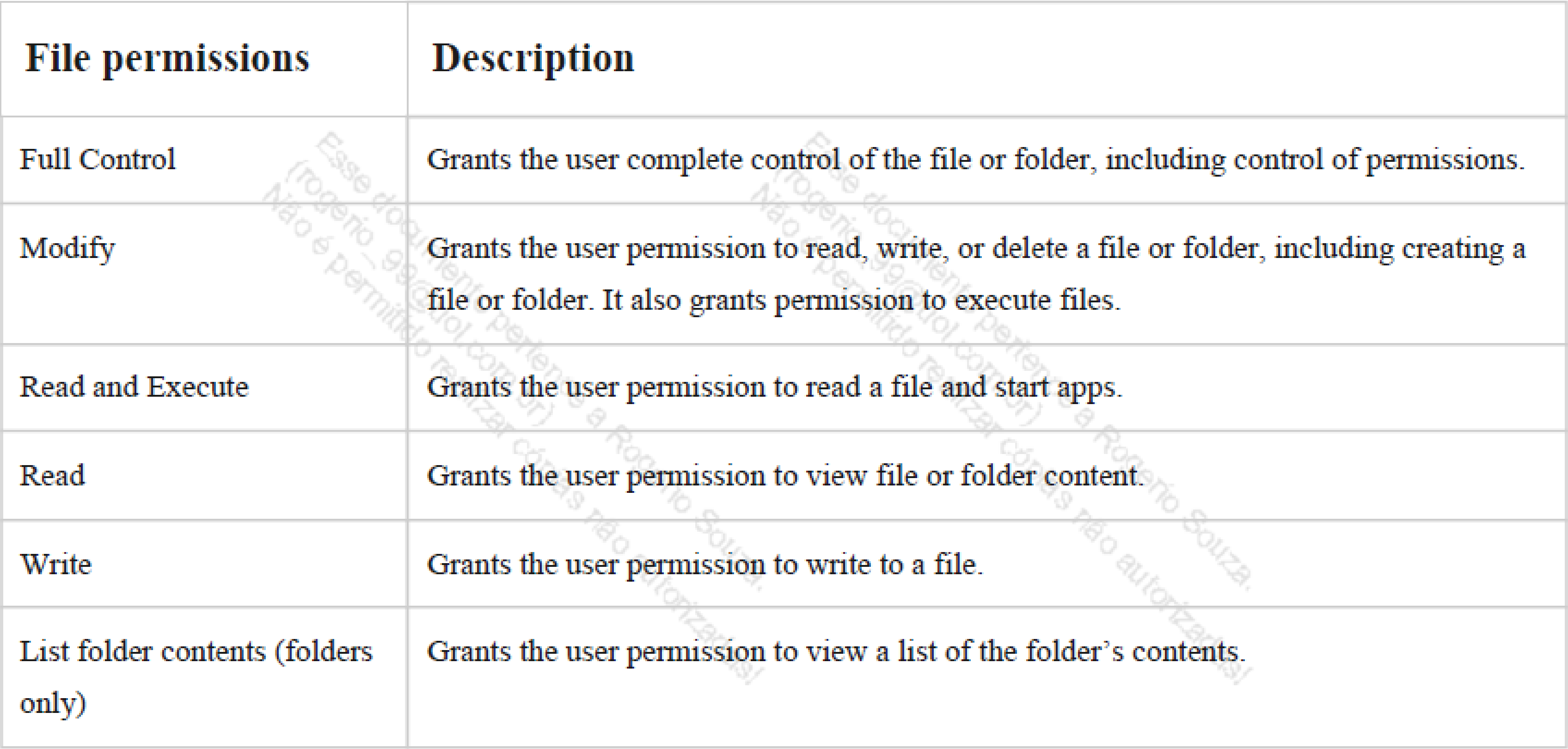
What Are File Permissions?

- You assign file permissions to files or folders on a storage volume that you format with NTFS. The permissions that you assign to files and folders govern user access to them.
- There are several key points to remember, with respect to file permissions, including that you can:
  - Configure file permissions for an individual file or folder, or sets of files or folders.
  - Assign file permissions individually, to objects that include users, groups, and computers.
  - Control file permissions by granting or denying specific types of file and folder access, such as Read or Write.
  - Configure inheritance of file permissions from parent folders. By default, the file permissions that you assign to a folder also are assigned to new folders or files within that parent folder.

Standard permissions

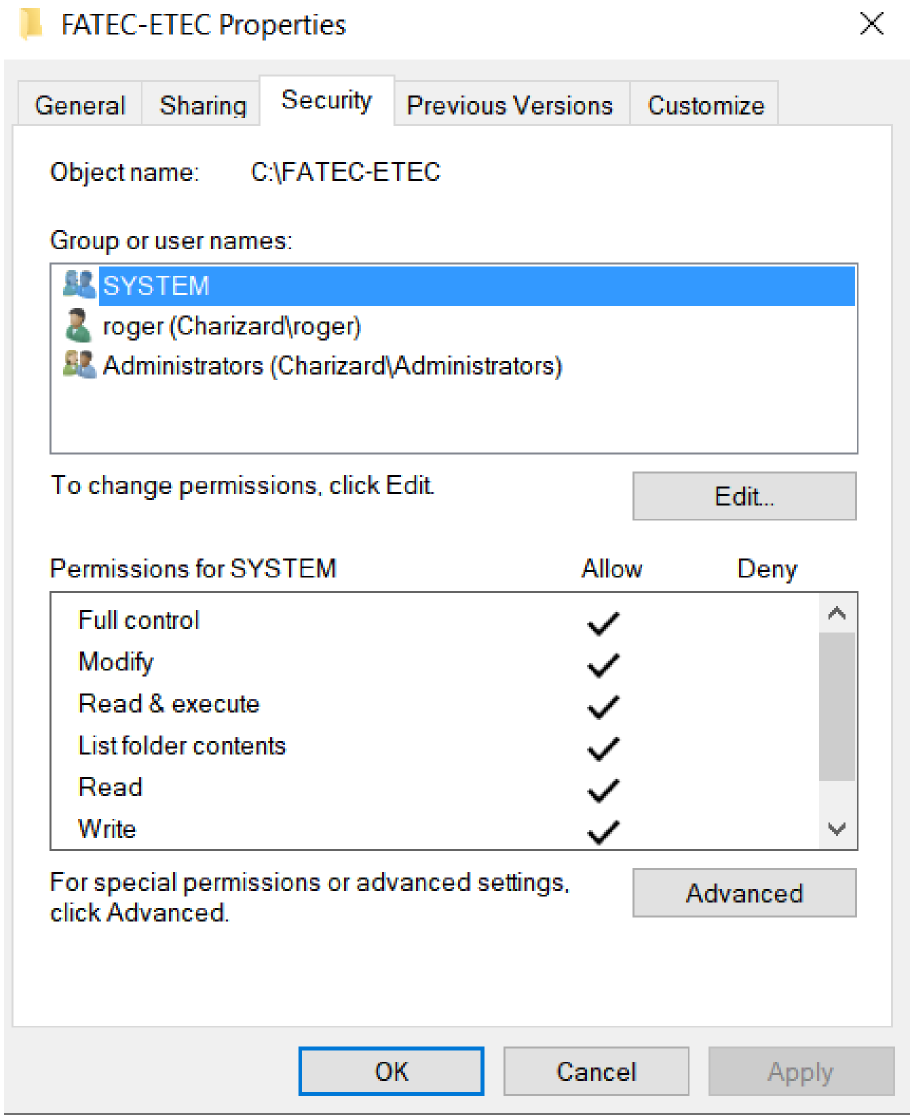
- Standard permissions provide the most commonly used permission settings for files and folders. You assign standard permissions in the Permissions for *folder name* dialog box.
- The following table lists the standard permissions options for files and folders.

Standard permissions



File permissions	Description
Full Control	Grants the user complete control of the file or folder, including control of permissions.
Modify	Grants the user permission to read, write, or delete a file or folder, including creating a file or folder. It also grants permission to execute files.
Read and Execute	Grants the user permission to read a file and start apps.
Read	Grants the user permission to view file or folder content.
Write	Grants the user permission to write to a file.
List folder contents (folders only)	Grants the user permission to view a list of the folder’s contents.

Permissão de Arquivos



FATEC-ETEC Properties

Object name: C:\FATEC-ETEC

Group or user names:

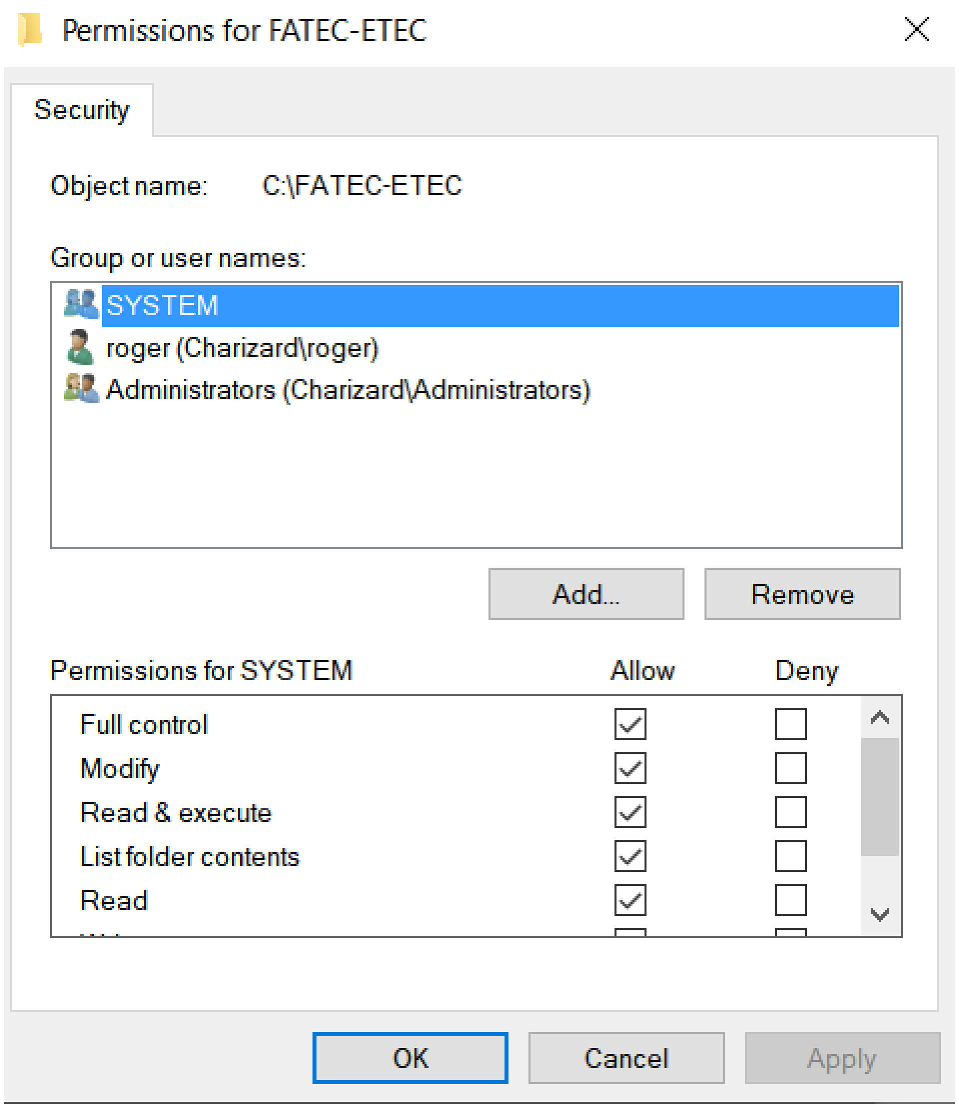
- SYSTEM
- roger (Charizard\roger)
- Administrators (Charizard\Administrators)

To change permissions, click Edit.

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

For special permissions or advanced settings, click Advanced.

Permissão de Arquivos



Permissions for FATEC-ETEC

Object name: C:\FATEC-ETEC

Group or user names:

- SYSTEM
- roger (Charizard\roger)
- Administrators (Charizard\Administrators)

Permissions for SYSTEM	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

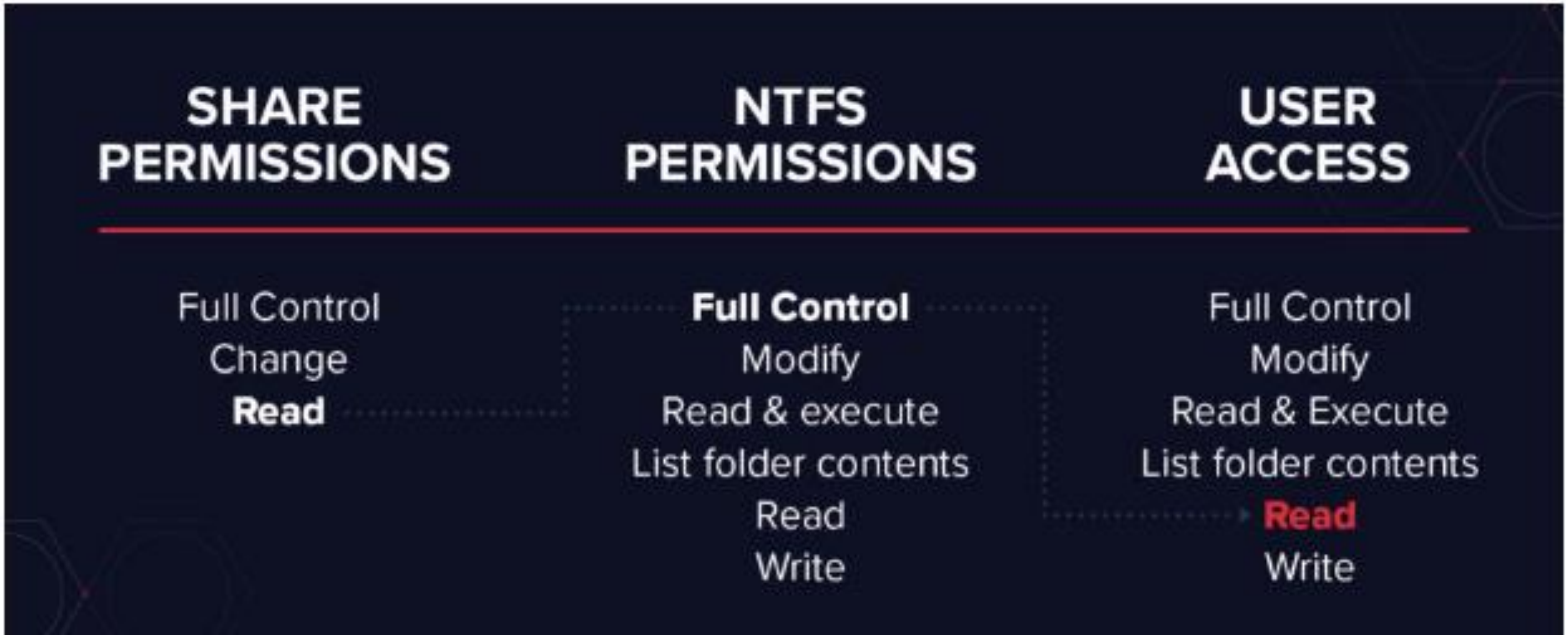
Combining File Permissions and Shared Folder Permissions

- File permissions and shared folder permissions work together to control access to file and folder resources that users access from a network.
- When you configure access to network resources on an NTFS volume, use the most restrictive file permissions to control access to folders and files, and combine them with the most restrictive shared folder permissions to control access to the network.

How Combining File and Shared Folder Permissions Works

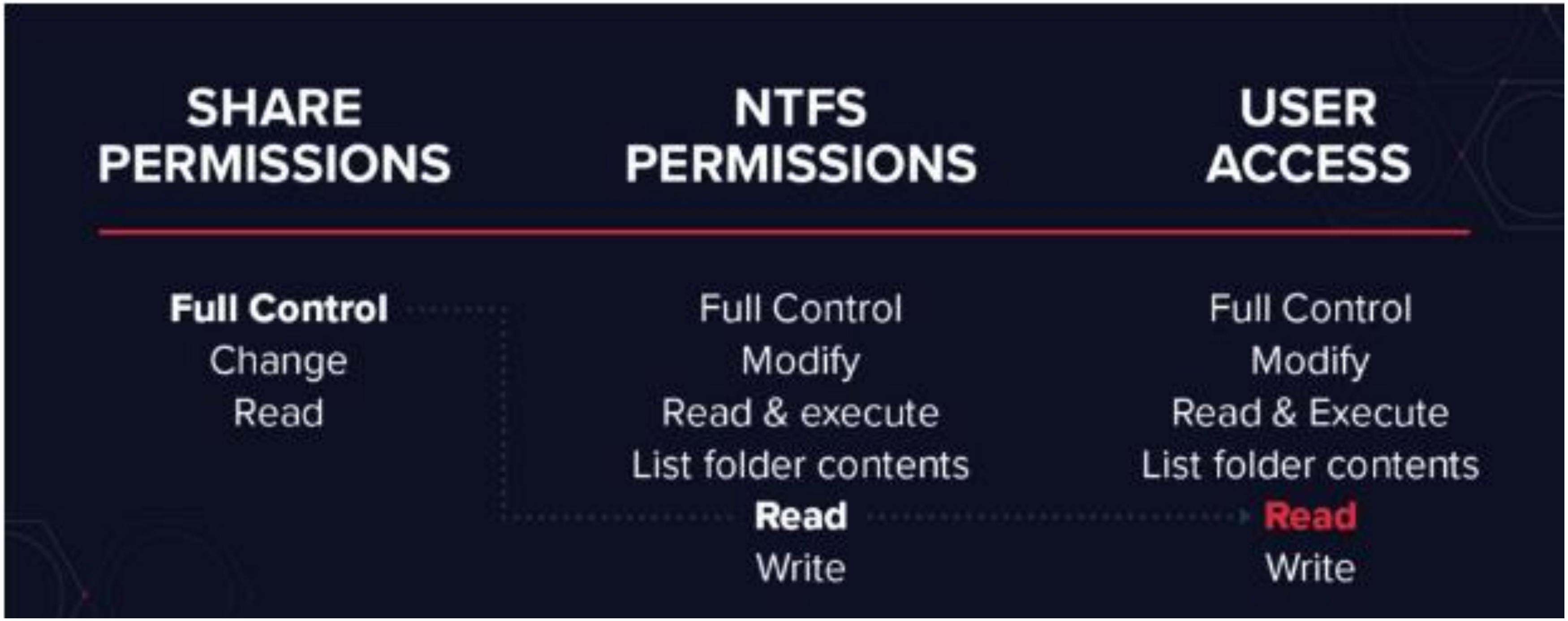
- When you apply both file and shared folder permissions, remember that the more restrictive of the two permissions dictates what access a user has to a file or folder. The following two examples explain this further:
- The user must have both file permissions and shared folder permissions. If no permissions exist for the user (either as an individual or as the member of a group) on either resource, access is denied.

Exemplo



SHARE PERMISSIONS	NTFS PERMISSIONS	USER ACCESS
Full Control	**Full Control**	Full Control
Change	Modify	Modify
Read	Read & execute	Read & Execute
	List folder contents	List folder contents
	Read	**Read**
	Write	Write

Exemplo



SHARE PERMISSIONS

Full Control
Change
Read

NTFS PERMISSIONS

Full Control
Modify
Read & execute
List folder contents
Read
Write

USER ACCESS

Full Control
Modify
Read & Execute
List folder contents
Read
Write

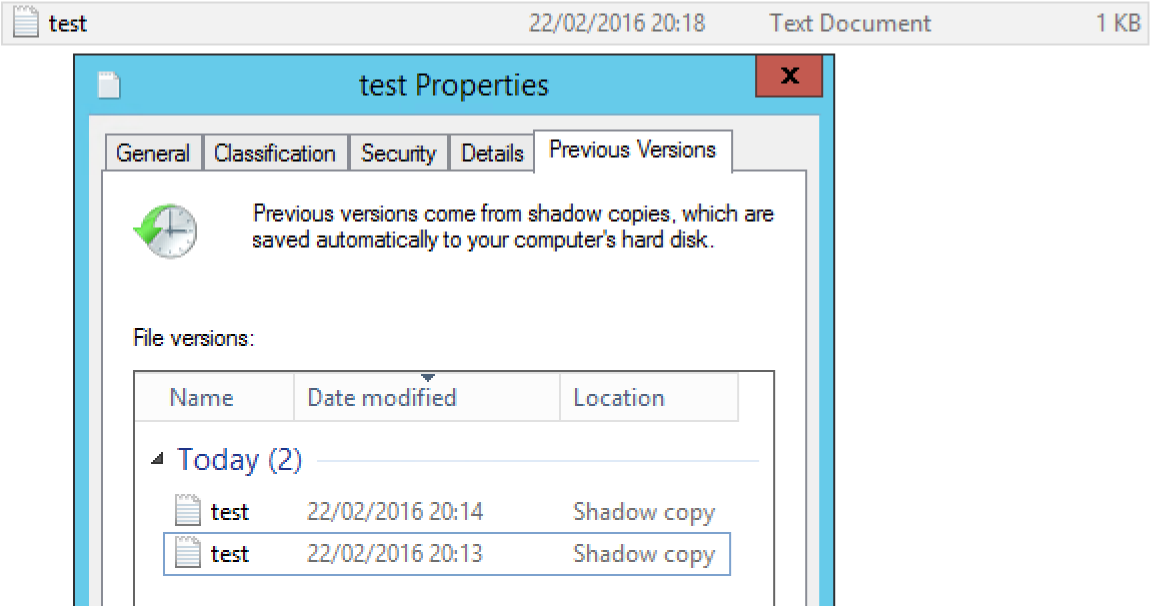
What Are Shadow Copies?

- A *shadow copy* is a static image, or snapshot, of a set of data, such as a file or folder. Shadow copies provide the capability to recover files and folders based on snapshots of storage drives.
- After a snapshot is taken, you can view and potentially restore previous versions of files and folders from that snapshot.
- A shadow copy does not make a complete copy of all files for each snapshot. Instead, after a snapshot is taken, Windows Server tracks changes to the drive. A specific amount of disk space is allocated for tracking the changed disk blocks. When you access a previous version of a file, some of the content might be in the current version of the file, and some might be in the snapshot.

What Are Shadow Copies?

- By default, the changed disk blocks are stored on the same drive as the original file, but you can modify where they are stored. You also can define how much disk space is allocated for shadow copies. Multiple snapshots are retained until the allocated disk space is full, after which, older snapshots are removed to make room for new snapshots. The amount of disk space that a snapshot uses is based on how much has changed in the files since the previous snapshot.
- Because a snapshot is not a complete copy of files, you cannot use shadow copies as a replacement for traditional backups. If the disk containing a drive is lost or damaged, then the snapshots of that drive are also lost.
- Shadow copies are suitable for recovering data files, but not for more complex data (such as databases), that need to be logically consistent before a backup is performed. A database that you restore from previous versions is likely to be corrupt and require database repairs.

Previous Versions



test	22/02/2016 20:18	Text Document	1 KB

Previous versions come from shadow copies, which are saved automatically to your computer's hard disk.

File versions:

Name	Date modified	Location
Today (2)		
test	22/02/2016 20:14	Shadow copy
test	22/02/2016 20:13	Shadow copy

Considerations for Scheduling Shadow Copies

- The default schedule for creating shadow copies is Monday through Friday at 07:00 A.M., and again at noon. You can modify the default schedule as desired for your organization.
- When scheduling shadow copies:
  - Consider that increasing the frequency of shadow copies increases the load on the server. As a best practice, you should not schedule drive shadow copies more than once each hour.
  - Increase the frequency of shadow copies for frequently changing data. This increases the likelihood that a shadow copy will capture recent file changes.
  - Increase the frequency of shadow copies for important data. This increases the likelihood that a shadow copy will capture important file changes.

Shadow copies

- Shadow copies.mp4

- https://www.youtube.com/watch?v=ONLMVXzgkDA