- 1. 4. 3. Advanced networking -

Sharing resources with other users

The simplest way to share files, digital media, printers, and other resources in a small network is with HomeGroup.

Convenient as it is, however, HomeGroup isn’t appropriate for all networks.

First, it’s designed for use in a home, where you fully trust everybody.

Hence, it has limited abilities for applying different access requirements to various objects and for various users.

Second, HomeGroup works only on computers running Windows 7 and later.

Computers running earlier versions of Windows or other operating systems must use different methods for sharing and accessing network resources.

These other methods are fully supported in Windows 10, and you can use them alongside HomeGroup if you want to.

The underlying system of share permissions and NTFS permissions for controlling access to objects remains in Windows 10, working much like it has in previous versions of Windows going all the way back to Windows NT in the early ’90s.

Understanding sharing and security models in Windows

Windows 10 offers two ways (aside from HomeGroup) to share file resources, whether you’re doing so locally or over the network:

1. Public folder sharing.

When you place files and folders in your Public folder or its subfolders, those files are available to anyone who has a user account on your computer.

Each person who signs in has access to his or her own profile folders (Documents, Music, and so on), and everyone who signs in has access to the Public folder.

You need to dig a bit to find the Public folder, which doesn’t appear by default in the left pane of File Explorer.

Navigate to C:\Users\Public.

If you use the Public folder often, pin it to the Quick Access list in File Explorer.

By default, all users with an account on your computer can sign in and create, view, modify, and delete files in the Public folders.

The person who creates a file in a Public folder (or copies an item to a Public folder) is the file's owner and has Full Control access.

All others who sign in locally have Modify access.

Settings in Advanced Sharing Settings (accessible from Settings > Network & Internet) determine whether the contents of your Public folder are made available on your network and whether entering a user name and password is required for access.

If you turn on password-protected sharing, only network users who have a user account on your computer (or those who know the user name and password for an account on your computer) can access files in the Public folder.

Without password-protected sharing, everyone on your network has access to your Public folder files if you enable network sharing of the Public folder.

You can't select which network users get access, nor can you specify different access levels for different users. Sharing via the Public folder is quick and easy—but it's inflexible.

2. Advanced sharing.

By choosing to share folders or files outside the Public folder, you can specify precisely which user accounts are able to access your shared data, and you can specify the types of privileges those accounts enjoy.

You can grant different access privileges to different users.

For example, you might enable some users to modify shared files and create new ones, enable other users to read files without changing them, and lock out still other users altogether.

You don't need to decide between sharing the Public folder and sharing specific folders because you can use both methods simultaneously.

You might find that a mix of sharing styles works best for you; each has its benefits:

- Sharing specific folders is best for files you want to share with some users but not with others—or if you want to grant different levels of access to different users.
- Public folder sharing provides a convenient, logical way to segregate your personal documents, pictures, music, and so on from those you want to share with everyone who uses your computer or your network.

Configuring your network for sharing

If you plan to share folders and files with other users on your network through options other than those available in the HomeGroup feature, you need to take a few preparatory steps.

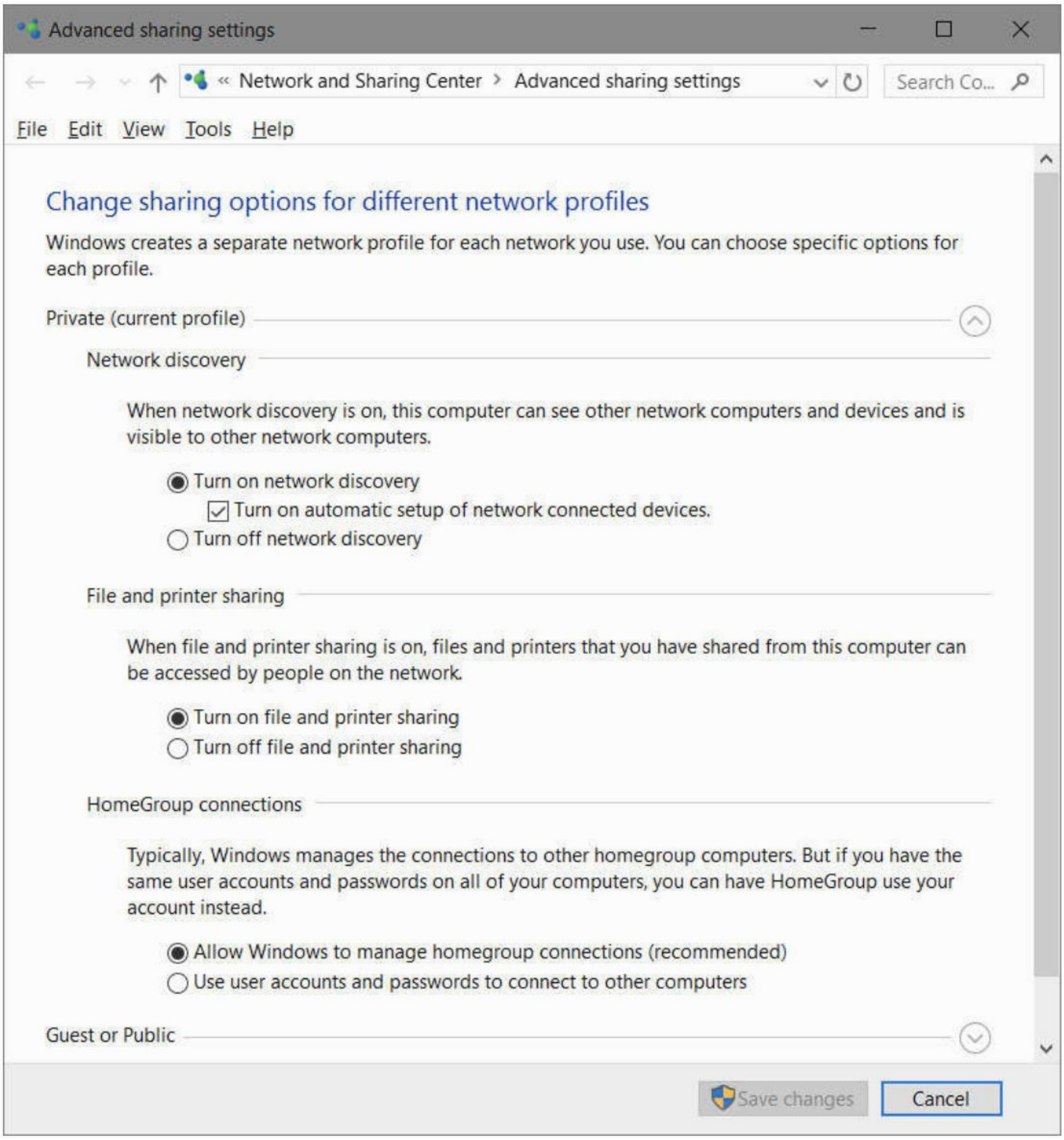
If you plan to share only through HomeGroup and with others who use your computer by signing in locally, you can skip these steps.

And if your computer is part of a domain, some of these steps—or their equivalent in the domain world—must be done by an administrator on the domain controller.

1. Be sure that all computers use the same workgroup name. With versions of Windows newer than Windows XP, this step isn’t absolutely necessary, although it does improve network discovery performance.

2. Be sure that your network’s location is set to Private. This setting provides appropriate security for a network in a home or an office.

3. Be sure that Network Discovery is turned on. This should happen automatically when you set the network location to Private, but you can confirm the setting—and change it if necessary—in Advanced Sharing Settings, which is shown in the following figure. To open Advanced Sharing Settings, go to Settings > Network & Internet > Sharing Options. Alternatively, open Network And Sharing Center and click Change Advanced Sharing Options.



Advanced sharing settings
« Network and Sharing Center › Advanced sharing settings
Search Co...
File Edit View Tools Help

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.

Private (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.

● Turn on network discovery
☑ Turn on automatic setup of network connected devices.
○ 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

HomeGroup connections

Typically, Windows manages the connections to other homegroup computers. But if you have the same user accounts and passwords on all of your computers, you can have HomeGroup use your account instead.

● Allow Windows to manage homegroup connections (recommended)
○ Use user accounts and passwords to connect to other computers

Guest or Public

4. Select your sharing options. In Advanced Sharing Settings, make a selection for each of the following network options. You'll find the first two options under the Private profile; to view the remaining settings, expand All Networks.

- File And Printer Sharing. Turn on this option if you want to share specific files or folders, the Public folder, or printers; it must be turned on if you plan to share any files (other than media streaming) over your network.
  The mere act of turning on file and printer sharing does not expose any of your computer's files or printers to other network users; that occurs only after you make additional sharing settings.
- HomeGroup Connections. If you use a homegroup for sharing, it's generally best to use the default setting, Allow Windows To Manage Homegroup Connections (Recommended). With this setting, when a user at a computer that's also part of a homegroup attempts to use a shared resource on your

computer, Windows connects using the HomeGroupUser$ account.
When a user connects from a computer that's not a member of the homegroup, Windows first tries to authenticate using that person's sign-in credentials; if that fails, Windows uses the built-in Guest account (if password-protected sharing is off) or prompts for credentials (if password-protected sharing is on). If you select Use User Accounts And Passwords To Connect To Other Computers, homegroup computers work like non-homegroup computers instead of using the HomeGroupUser$ account.

- Public Folder Sharing. If you want to share items in your Public folder with all network users (or, if you enable password-protected sharing, all users who have a user account and password on your computer), turn on Public folder sharing. If you do so, network users will have read/write access to Public folders. With Public folder sharing turned off, anyone who signs in to your computer locally has access to Public folders, but network users do not.
- Media Streaming. Turning on media streaming provides access to pictures, music, and video through streaming protocols that can send media to computers or to other media playback devices.
- File Sharing Connections. Unless you have very old computers on your network, leave this option set to 128-bit encryption, which has been the standard for most of this century.
- Password Protected Sharing. When password-protected sharing is turned on, network users cannot access your shared folders (including Public folders, if shared) or printers unless they can provide the user name and password of a user account on your computer. With this setting enabled, when another user attempts to access a shared resource, Windows sends the user name and password that the person used to sign in to her own computer. If that matches the credentials for a local user account on your computer, the user gets immediate access to the shared resource (assuming permissions to use the particular resource have been granted to that user account). If either the user name or the password does not match, Windows asks the user to provide credentials.
  With password-protected sharing turned off, Windows does not require a user name and password from network visitors. Instead, network access is provided by using the Guest account. This account isn't available for interactive use but can handle these tasks in the background.
- Configure user accounts. If you use password-protected sharing, each person who accesses a shared resource on your computer must have a user account on your computer. Use the same user name as that person uses on his or her own computer and the same password as well. If you do that, network users will be able to access shared resources without having to enter their credentials after they've signed in to their own computer.

Renaming your workgroup

A workgroup is identified by a name; all computers in a workgroup must be in the same local area network and subnet, and all must share the same workgroup name.

In Windows 10, the workgroup name is largely invisible and irrelevant; when you open the Network folder or look at a network map, Windows displays all computers in the network, regardless of which workgroup they're in.

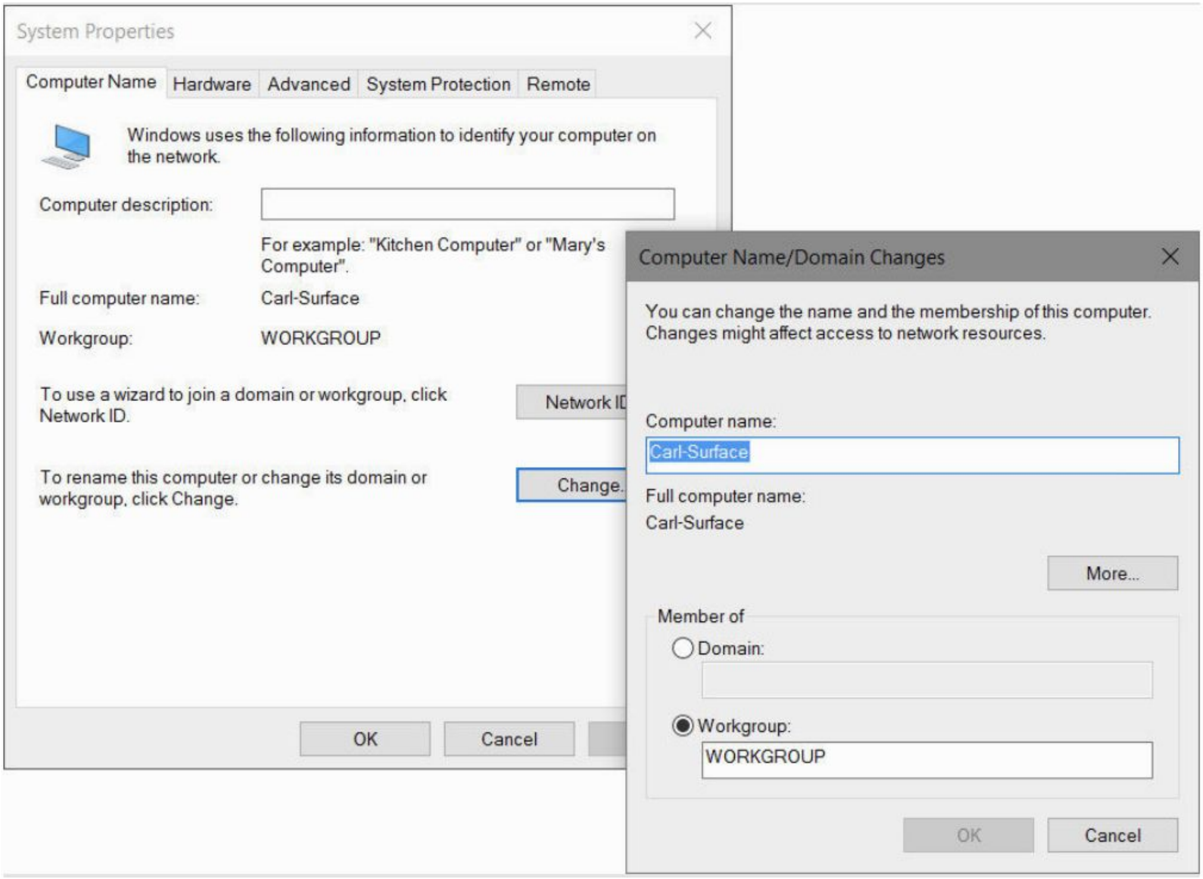
However, network discovery is faster when all computers are in the same workgroup.

The default name for a workgroup in recent Windows versions is WORKGROUP.

To set the workgroup name, follow these steps:

1. In the search box or in Control Panel, type workgroup, and then click Change Workgroup Name.

2. On the Computer Name tab of the System Properties dialog box, click Change, which displays the following dialog box:



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: Carl-Surface

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: Carl-Surface

Full computer name: Carl-Surface

Member of

○ Domain:

● Workgroup: WORKGROUP

3. In the Computer Name/Domain Changes dialog box, select Workgroup and type the name of the workgroup (which has a 15-character maximum and can't include any of these characters: ; : < > * + = \ | / ? ,). Then click OK in each dialog box.

4. Restart your computer.

Sharing files and folders from any folder

Whether you plan to share files and folders with other people who share your computer or those who connect to your computer over the network (or both), the process for setting up shared resources is the same as long as the Sharing Wizard is enabled.

We recommend you use the Sharing Wizard even if you normally disdain wizards.

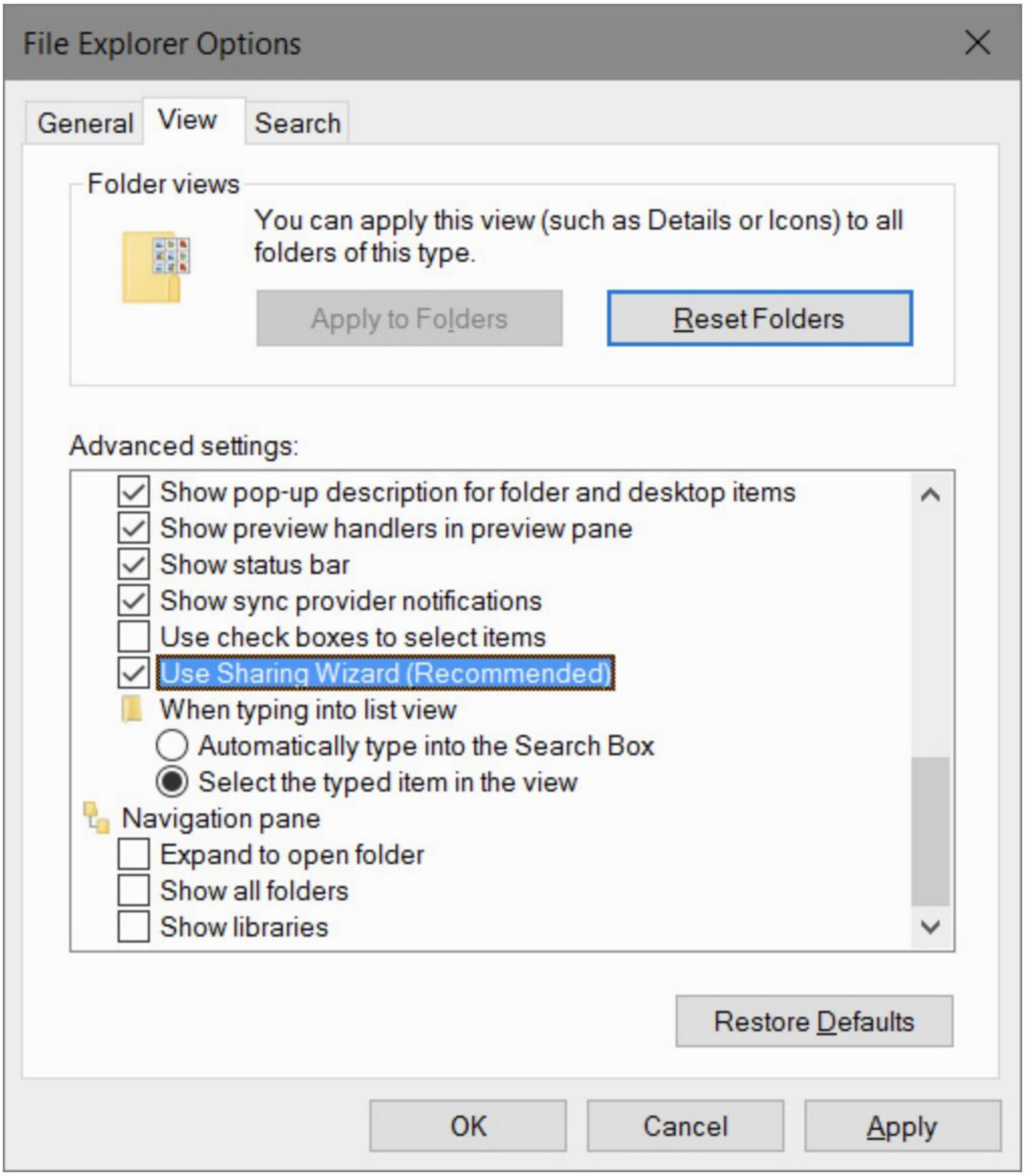
It's quick, easy, and certain to make all the correct settings for network shares and NTFS permissions—a sometimes daunting task if undertaken manually.

After you configure shares with the wizard, you can always dive in and make changes manually if you need to.

To be sure the Sharing Wizard is enabled, open File Explorer Options.

Type "folder" in the search box, and choose File Explorer Options. Or, in File Explorer, click View > Options.

In the dialog box that appears, shown next, click the View tab. Near the bottom of the Advanced Settings list, see that Use Sharing Wizard (Recommended) is selected:



Folder views

You can apply this view (such as Details or Icons) to all folders of this type.

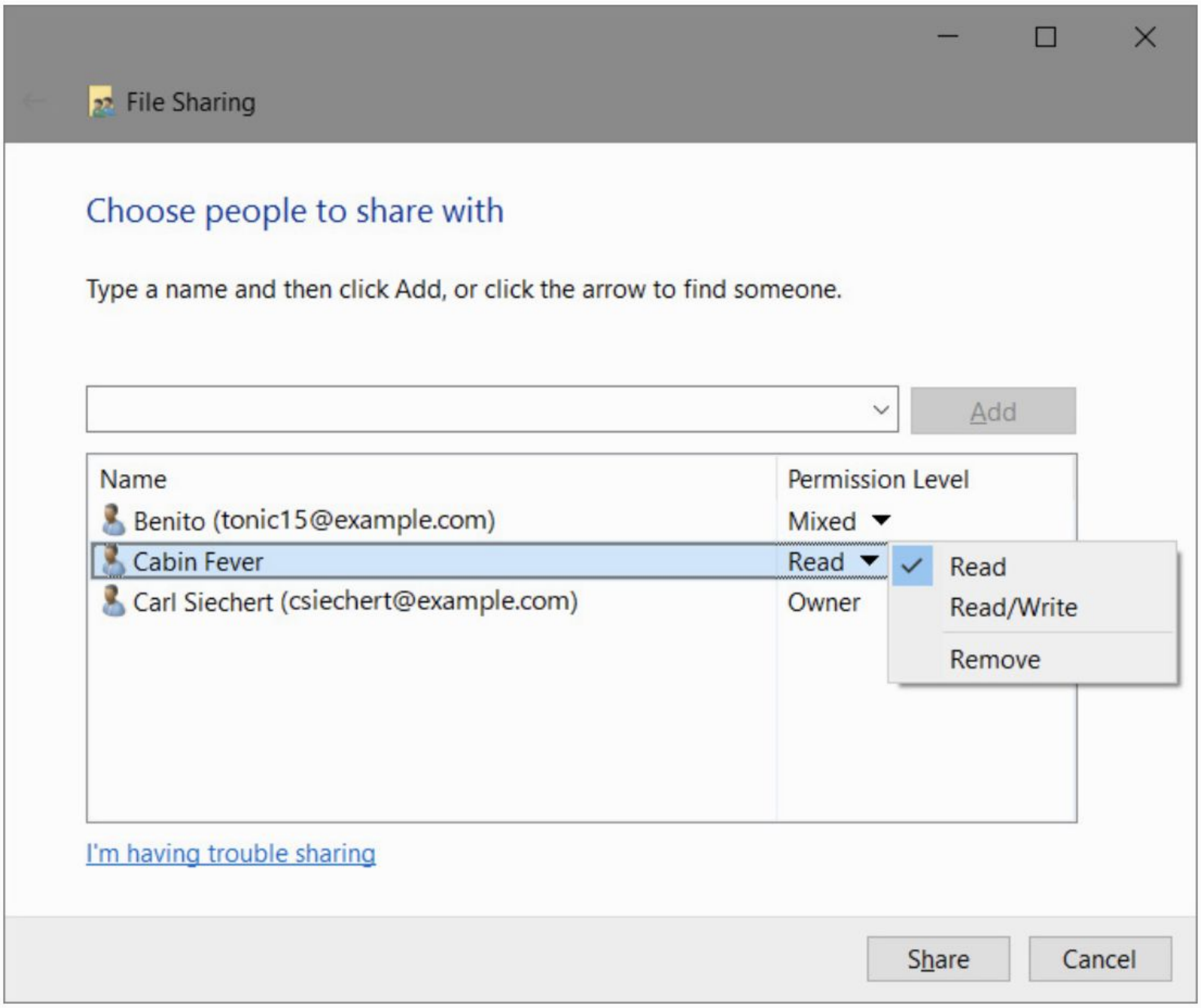
Advanced settings:

- ☑ Show pop-up description for folder and desktop items
- ☑ Show preview handlers in preview pane
- ☑ Show status bar
- ☑ Show sync provider notifications
- □ Use check boxes to select items
- ☑ Use Sharing Wizard (Recommended)
- When typing into list view
  - ○ Automatically type into the Search Box
  - ● Select the typed item in the view
- Navigation pane
  - □ Expand to open folder
  - □ Show all folders
  - □ Show libraries

With the Sharing Wizard at the ready, follow these steps to share a folder or files:

1. In File Explorer, select the folders or files you want to share. You can select multiple objects.

2. Right-click and choose Share With > Specific People. Alternatively, click or tap the Share tab and then click Specific People in the Share With box. You might need to click the arrow in the Share With box to display Specific People. The File Sharing dialog box appears:



Choose people to share with

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

Name	Permission Level
Benito (tonic15@example.com)	Mixed
Cabin Fever	Read
Carl Siechert (csiechert@example.com)	Owner

3. In the entry box, enter the name or Microsoft account for each user with whom you want to share. You can type a name in the box or click the arrow to display a list of available names; then click Add. Repeat this step for each person you want to add.

The list includes all users who have an account on your computer, plus Everyone. If you've joined a homegroup, the list also includes any Microsoft accounts that have been linked to user accounts on any PC that's part of the homegroup. Guest is included if password-protected sharing is turned off. If you want to grant access to someone who doesn't appear in the list, click Create A New User, which takes you to User Accounts in Control Panel. This option appears only if your computer is not joined to a homegroup.

If you select Everyone and you have password-protected sharing enabled, the user must still have a valid account on your computer. However, if you turned off password-protected sharing, network users can gain access only if you grant permission to Everyone or to Guest.

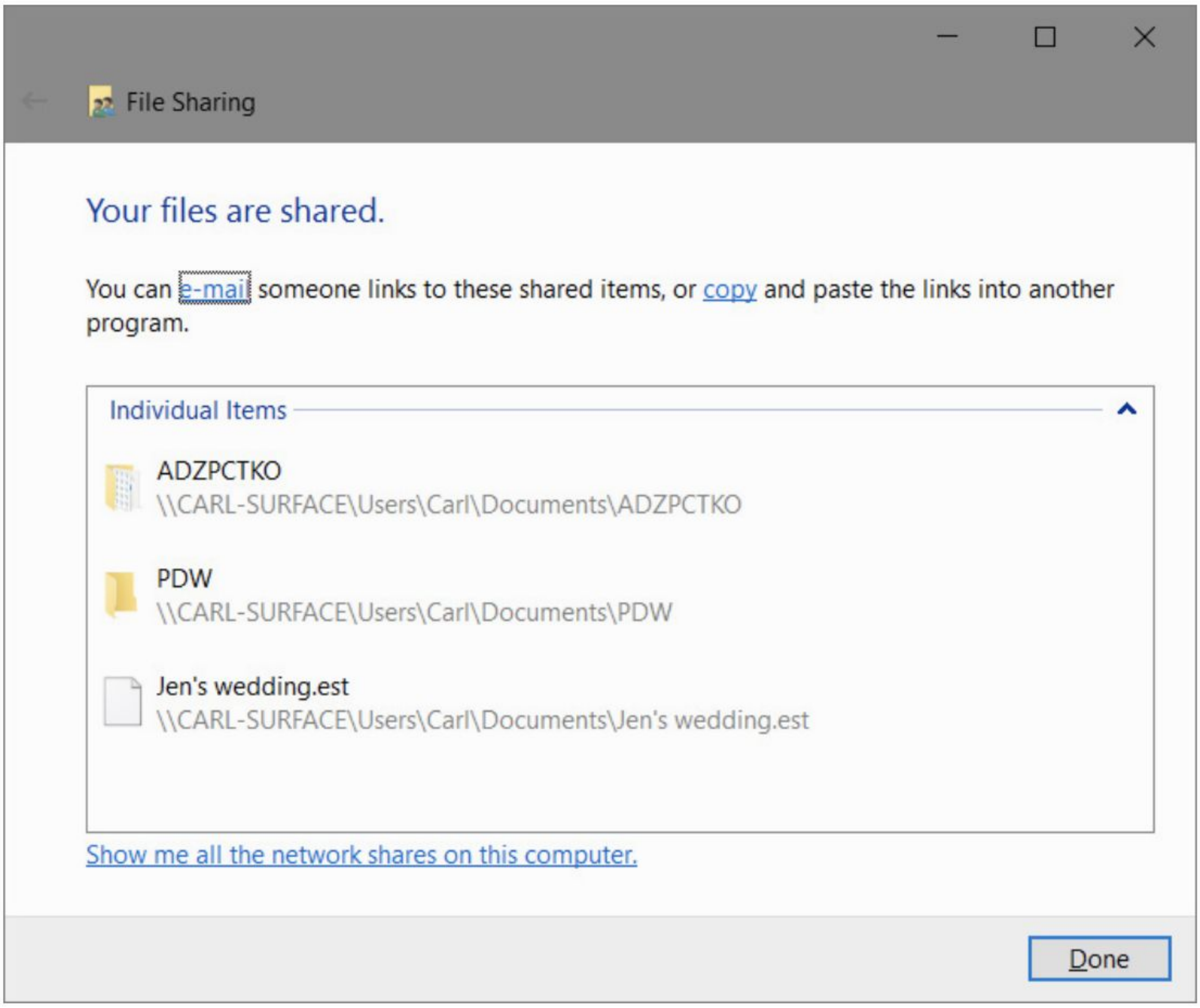
4. For each user, select a permission level. Your choices are:

- Read. Users with this permission level can view shared files and run shared programs, but they cannot change or delete files. Selecting Read in the Sharing Wizard is equivalent to setting NTFS permissions to Read & Execute.

- Read/Write. Users assigned the Read/Write permission have the same privileges you do as owner: they can view, change, add, and delete files in a shared folder. Selecting Read/Write sets NTFS permissions to Full Control for this user.

You might see other permission levels if you return to the Sharing Wizard after you set up sharing. Contribute indicates Modify permission. Custom indicates NTFS permissions other than Read & Execute, Modify, or Full Control. Mixed appears if you select multiple items and they have different sharing settings. Owner, of course, identifies the owner of the item.

5. Click Share. After a few moments, the wizard displays a page like the one shown in the next figure:



Your files are shared.

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

Individual Items

ADZPCTKO
\\CARL-SURFACE\Users\Carl\Documents\ADZPCTKO

PDW
\\CARL-SURFACE\Users\Carl\Documents\PDW

Jen's wedding.est
\\CARL-SURFACE\Users\Carl\Documents\Jen's wedding.est

Show me all the network shares on this computer.

6. In the final step of the wizard, you can do any of the following:

- Send an email message to the people with whom you're sharing. The message includes a link to the shared items.
- Copy the network path to the Clipboard. This is handy if you want to send a link via another application, such as a messaging app. To copy the link for a single item in a list, right-click the share name and choose Copy Link.
- Double-click a share name to open the shared item.

- Open File Explorer with your computer selected in the Network folder, showing each network share on your computer.
- When you're finished with these tasks, click Done.

Creating a share requires privilege elevation, but after a folder has been shared, the share is available to network users no matter who is signed in to your computer—or even when nobody is signed in.

Stopping or changing sharing of a file or folder

If you want to stop sharing a particular shared file or folder, select it in File Explorer and on the Share tab, click Stop Sharing.

Or right-click and choose Share With > Stop Sharing.

Doing so removes access control entries that are not inherited.

In addition, the network share is removed; the folder will no longer be visible in another user's Network folder.

To change share permissions, right-click and choose Share With > Specific People.

In the File Sharing dialog box, you can add users, change permissions, or remove users.

To stop sharing with a particular user, click the permission level by the user's name and choose Remove.

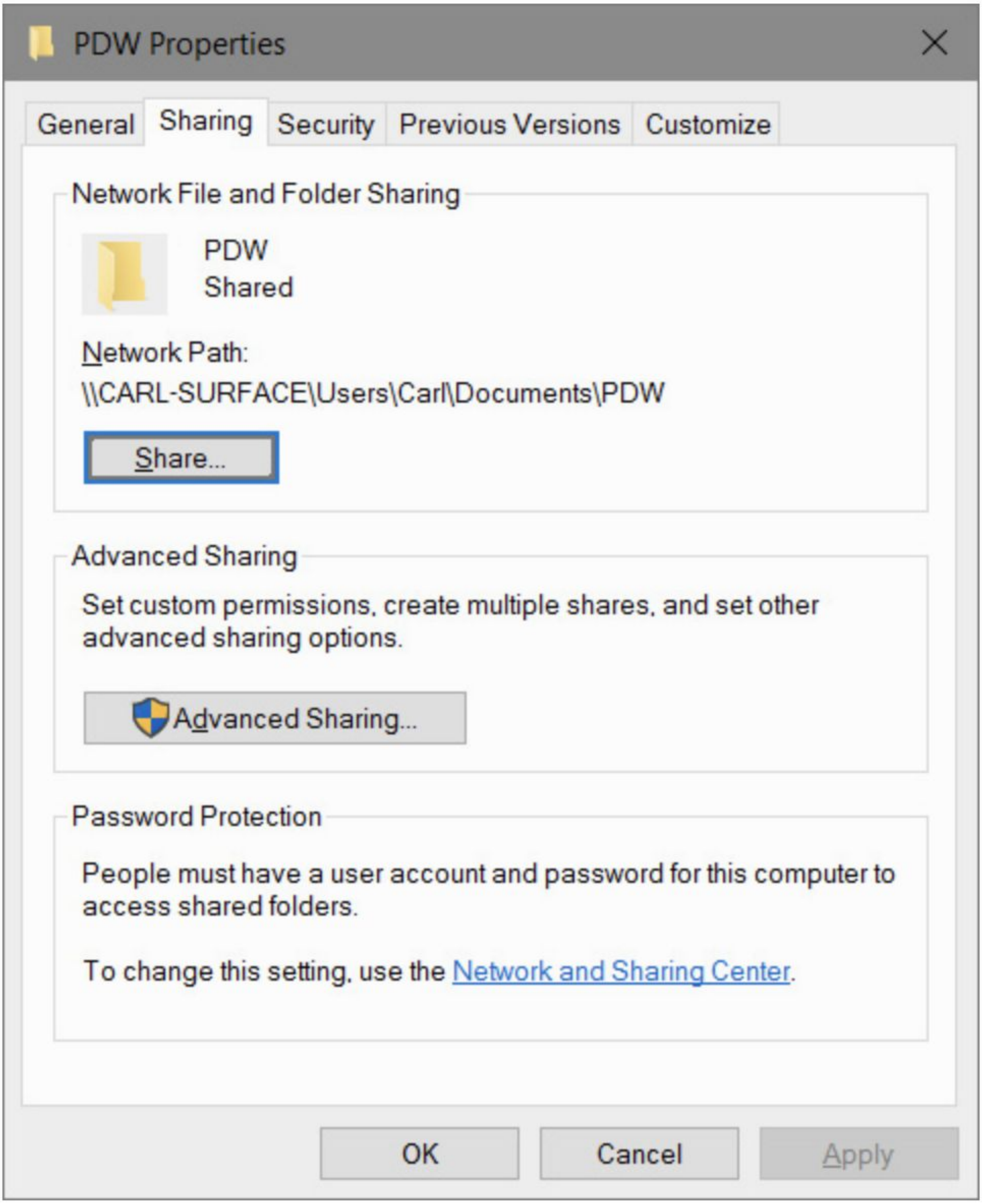
Setting advanced sharing properties

With Advanced Sharing, you configure network shares independently of NTFS permissions.

To open Advanced Sharing, right-click a folder, choose Properties, and click the Sharing tab.

Or, if the Sharing Wizard is disabled, select a folder in File Explorer and on the ribbon's Share tab (or the right-click Share With menu) choose Advanced Sharing.

Both methods display the Sharing tab:



Network File and Folder Sharing

PDW
Shared

Network Path:
\\CARL-SURFACE\Users\Carl\Documents\PDW

Advanced Sharing

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

Password Protection

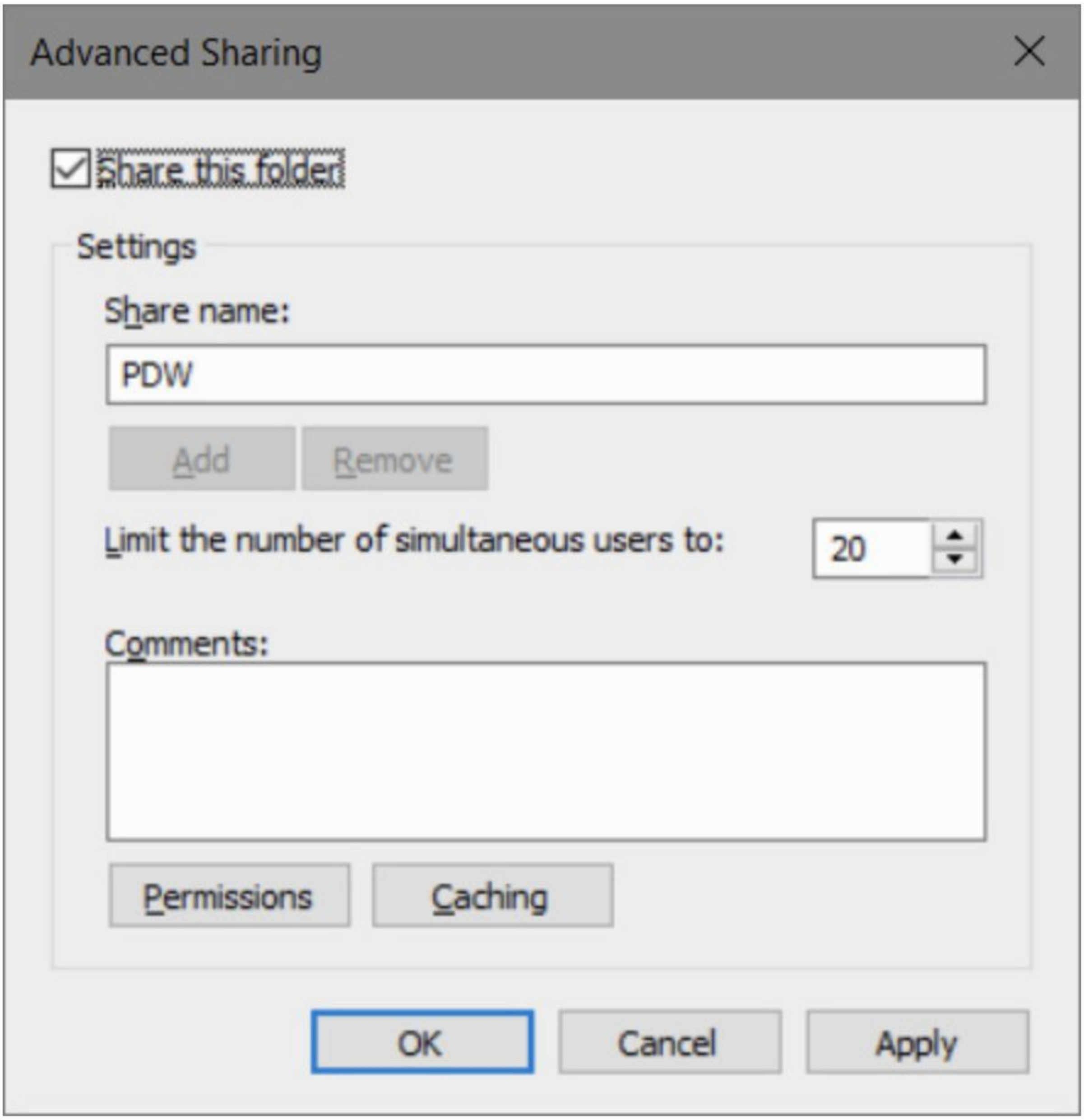
People must have a user account and password for this computer to access shared folders.

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

To create or modify a network share using advanced settings, follow these steps:

1. On the Sharing tab, click Advanced Sharing to display the Advanced Sharing dialog box.

2. Select Share This Folder, as shown next:



Advanced Sharing

☑ Share this folder

Settings

Share name: PDW

Limit the number of simultaneous users to: 20

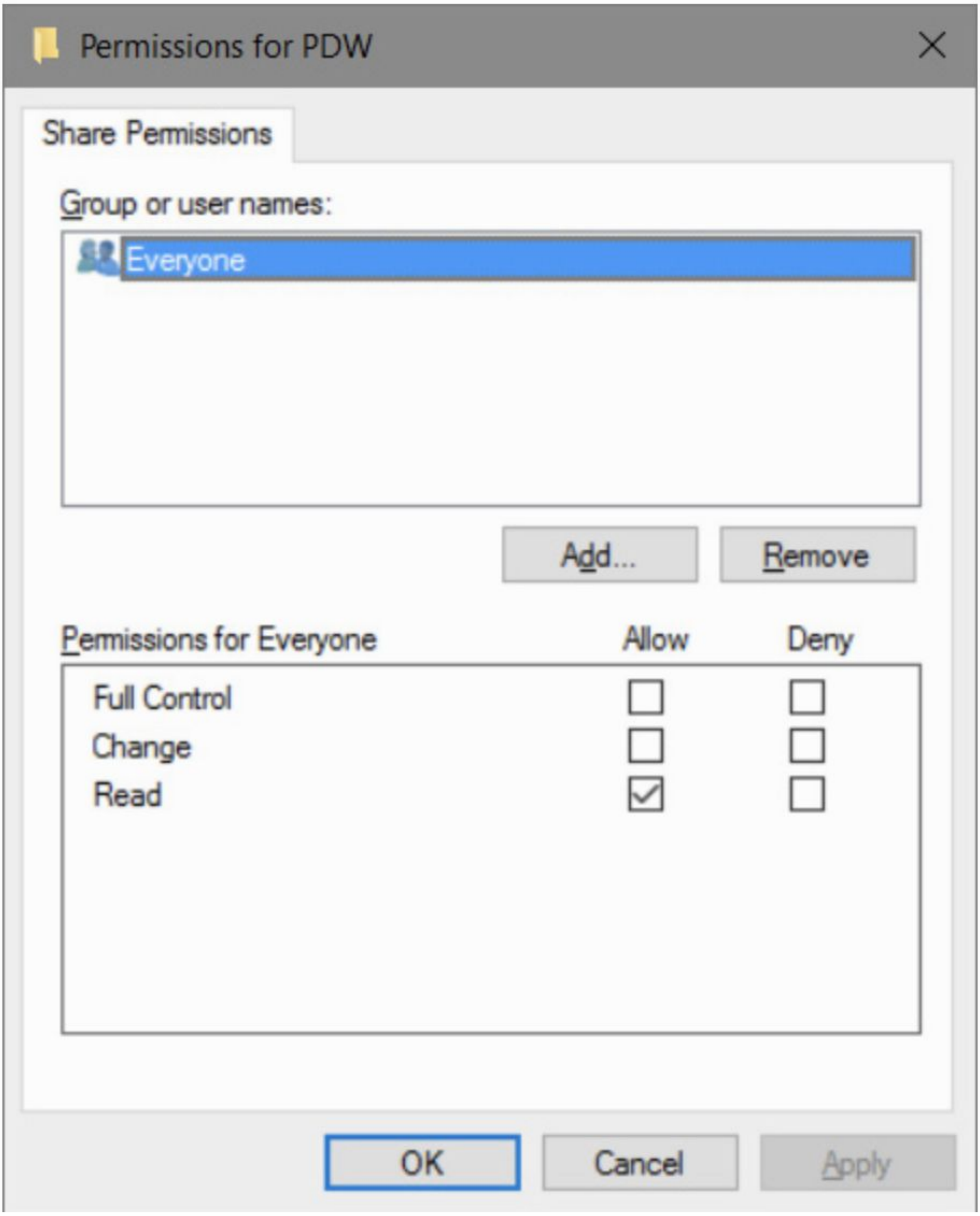
Comments:

4. Type a description of the folder’s contents in the Comments box.

Other users will see this description when they inspect the folder’s properties dialog box in their Network folder (or use Details view).

5. To limit the number of users who can connect to the shared folder concurrently, specify a number in the box. Windows 10 permits up to 20 concurrent network connections. If you need to share a resource with more users, you must use Windows Server.

6. Click Permissions.



Group or user names:

Everyone

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

The default shared resource permission associated with a new share is Read access to Everyone.

7.In the Group Or User Names list, select the name of the user or group you want to manage.

The shared resource permissions for the selected user or group appear below in the permissions list.

8. Select Allow, Deny, or neither for each access control entry:

- Full Control. Allows users to create, read, write, rename, and delete files in the folder and its subfolders. In addition, users can change permissions and take ownership of files on NTFS volumes.
- Change. Allows users to read, write, rename, and delete files in the folder and its subfolders but not create new files.
- Read. Allows users to read files but not write to them or delete them.

If you select neither Allow nor Deny, it's still possible that the user or group can inherit the permission through membership in another group that has the permission.

If the user or group doesn't belong to another such group, the user or group is implicitly denied permission.

To remove a name from the Group Or User Names list, select it and click Remove.

To add a name to the list, click Add to open the Select Users Or Groups dialog box, where you can enter the names of the users and groups you want to add.

Caution!

When you share a folder, you also make that folder's subfolders available on the network.

If the access permissions you set for the folder aren't appropriate for any of its subfolders, either reconsider your choice of access permissions or restructure your folders to avoid the problem.

How shared resource permissions and NTFS permissions work together

The implementation of shared resource permissions and NTFS permissions is confusingly similar, but you need to recognize that these are two separate levels of access control.

Only connections that successfully pass through both gates are granted access.

Shared resource permissions control network access to a particular resource.

Shared resource permissions do not affect users who sign in locally.

You set shared resource permissions in the Advanced Sharing dialog box, which you access from the Sharing tab of a folder's properties dialog box.

NTFS permissions (also known as discretionary access control lists, DACLs) apply to folders and files on an NTFS-formatted drive.

For each user to whom you want to grant access, you can specify exactly what that user is allowed to do: run programs, view folder contents, create new files, change existing files, and so on.

You set NTFS permissions on the Security tab of the properties dialog box for a folder or file.

Keep in mind that the two types of permissions are combined in the most restrictive way.

If, for example, a user is granted Read permission on the network share, even if the account has Full Control NTFS permissions on the same folder, the user gets only read access when connecting over the network.

In effect, the two sets of permissions act in tandem as “gatekeepers” that winnow out incoming network connections.

An account that attempts to connect over the network is examined first by the shared resource permissions gatekeeper.

The account is either rejected or allowed to enter with certain permissions.

It’s then confronted by the NTFS permissions gatekeeper, which might strip away (but not add to) some or all the permissions granted at the first doorway.

In many advanced sharing scenarios, it’s common practice to simply configure the shared folder with Full Control permissions for Everyone and then configure NTFS permissions to control access as desired.

In determining the effective permission for a particular account, you must also consider the effect of group membership.

Permissions are cumulative; an account that’s a member of one or more groups is granted all the permissions that are granted explicitly to the account as well as all permissions granted to each group of which it’s a member.

The only exception to this rule is Deny permissions, which take precedence over any conflicting Allow permissions.

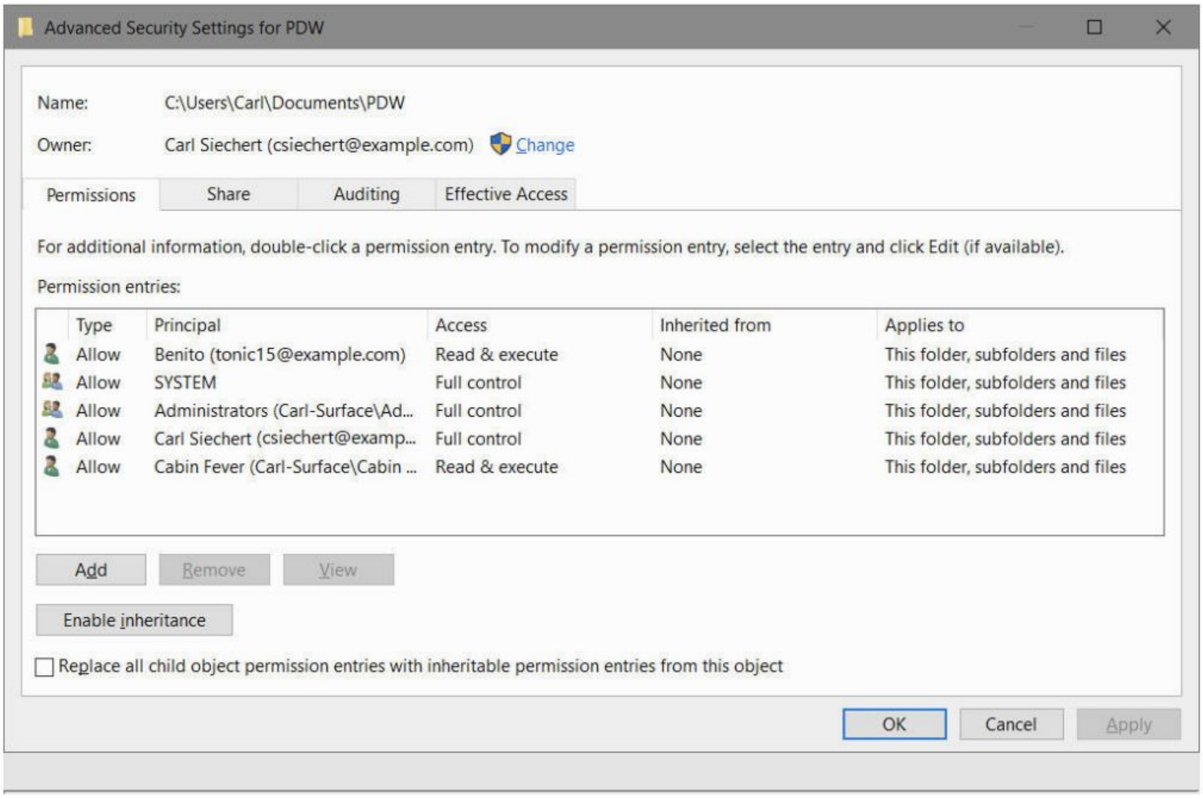
Review and change your sharing and NTFS permissions settings

A tool in File Explorer opens a dialog box, shown next, that displays NTFS permissions and share permissions in a format that’s sometimes easier to decipher than the properties dialog box.

Select a single folder or file in File Explorer and then, on the ribbon’s Share tab, click Advanced Security.

Here, in addition to viewing each type of permission, you can determine the effective access, which shows for a specific user or group the cumulative effect of various permissions and group memberships.

On a small network, the easiest way to specify a user on the Effective Access tab is to click Select A User > Advanced > Find Now.



Name: C:\Users\Carl\Documents\PDW

Owner: Carl Siechert (csiechert@example.com)

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Benito (tonic15@example.com)	Read & execute	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Administrators (Carl-Surface\Ad...	Full control	None	This folder, subfolders and files
Allow	Carl Siechert (csiechert@examp...	Full control	None	This folder, subfolders and files
Allow	Cabin Fever (Carl-Surface\Cabin ...	Read & execute	None	This folder, subfolders and files

□ Replace all child object permission entries with inheritable permission entries from this object

Sharing a printer

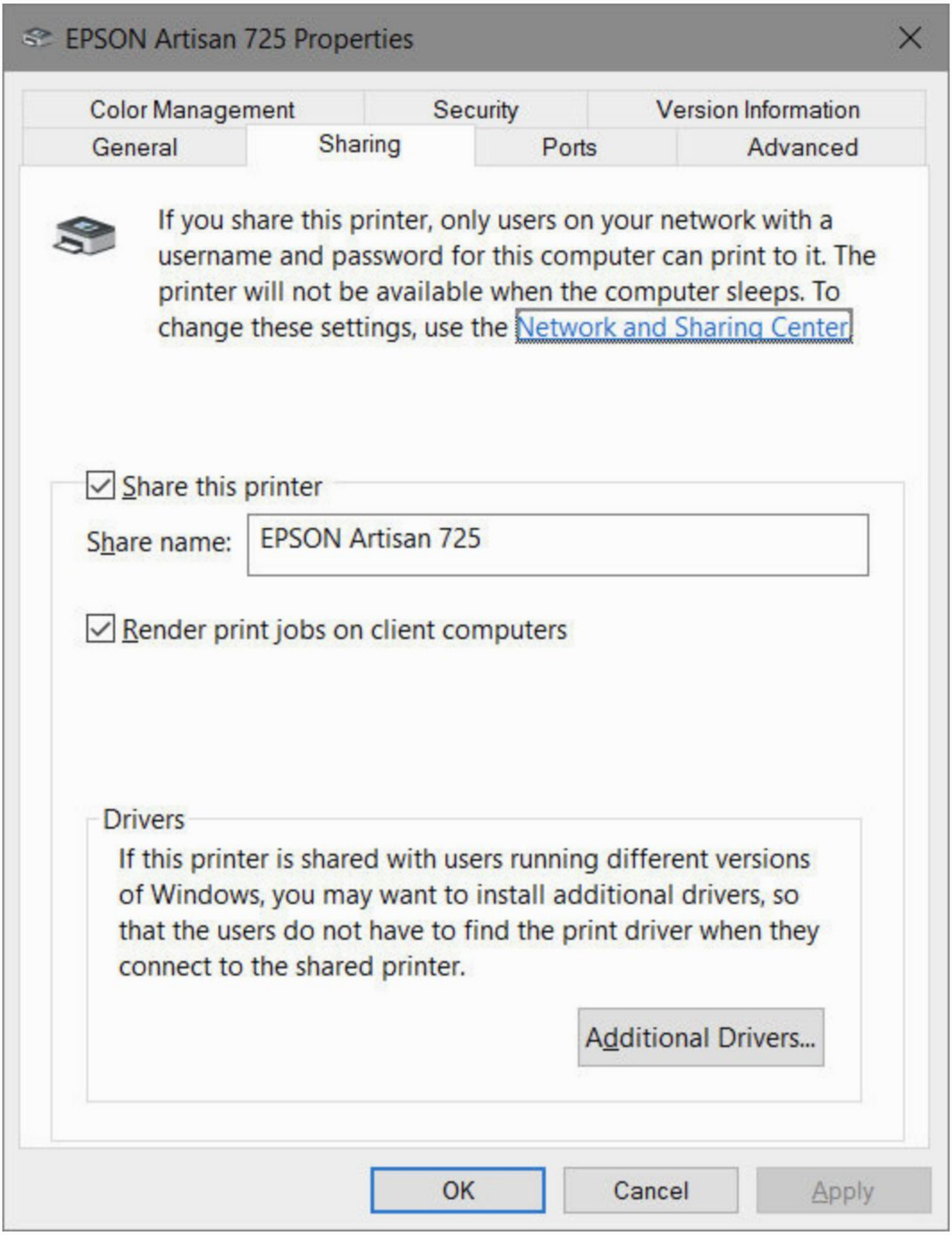
Although Windows doesn’t have a wizard for sharing a printer over the network, the process is pretty simple.

You configure all options for a printer—whether you plan to share it or not—by using the printer’s properties dialog box, which you access from Devices And Printers in Control Panel.

To make a printer available to other network users, right-click a printer and click Printer Properties. (

f you prefer Settings over Control Panel, you can reach this same dialog box by following a lengthier route: Settings > Devices > printer name > Manage > Printer Properties.

On the Sharing tab, select Share This Printer and provide a share name, as shown in the following figure:



EPSON Artisan 725 Properties

If you share this printer, only users on your network with a username and password for this computer can print to it. The printer will not be available when the computer sleeps. To change these settings, use the Network and Sharing Center.

☑ Share this printer

Share name: EPSON Artisan 725

☑ Render print jobs on client computers

Drivers

If this printer is shared with users running different versions of Windows, you may want to install additional drivers, so that the users do not have to find the print driver when they connect to the shared printer.

Unlike for shared folders, which maintain separate share permissions and NTFS permissions, a single set of permissions controls access to printers, whether by local users or by network users.

Of course, only printers that have been shared are accessible to network users.

When you set up a printer, initially all users in the Everyone group have Print permission for documents they create, which provides users access to the printer and the ability to manage their own documents in the print queue.

By default, members of the Administrators group also have Manage Printers permission—which allows them to share a printer, change its properties, remove a printer, and change its permissions—and Manage Documents permission, which lets them pause, restart, move, and remove all queued documents.

As an administrator, you can view or modify permissions on the Security tab of the printer properties dialog box.

Setting print server properties

In addition to setting properties for individual printers by using their properties dialog boxes, you can set other properties by visiting the Print Server Properties dialog box.

To get there, select a printer in the Devices And Printers folder, and then click Print Server Properties.

The first three tabs control the list of items you see in the properties dialog box for a printer:

- The Forms tab controls the list of forms you can assign to trays using the Device Settings tab in a printer's properties dialog box. You can create new form definitions and delete any you create, but you can't delete any of the predefined forms.
- On the Ports tab, you can conFigure the ports that appear on the Ports tab in a printer's properties dialog box.
- The Drivers tab offers a list of all the installed printer drivers and provides a centralized location where you can add, remove, or update drivers.

On the Advanced tab, you can specify the location of spool files.

You might want to change to a folder on a different drive if, for example, you frequently run out of space on the current drive when you attempt to print large documents.

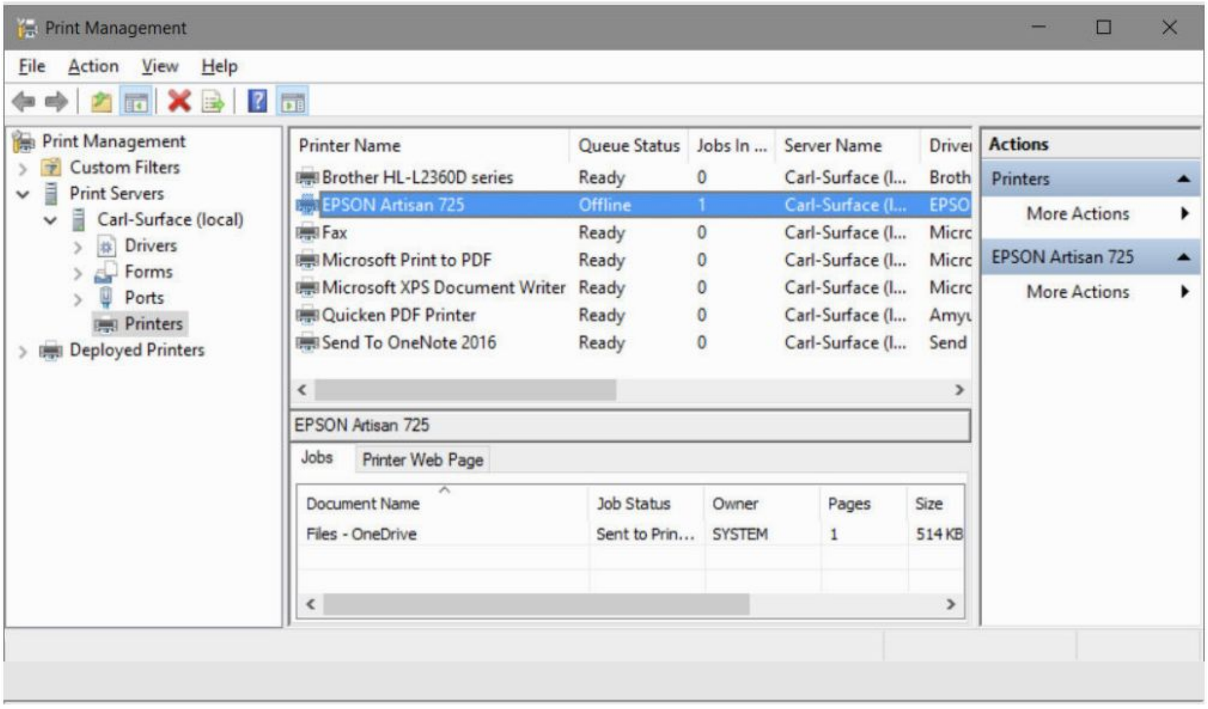
You can also set notification options on this tab.

Use the Print Management console

Users of Windows 10 Pro and Enterprise editions have a tool that places all print management tasks in one convenient console.

Print Management (Printmanagement.msc) provides a place for managing printers, drivers, queues, and shares.

If your edition includes Print Management, you can start it by typing "print" in the search box and then clicking Print Management.



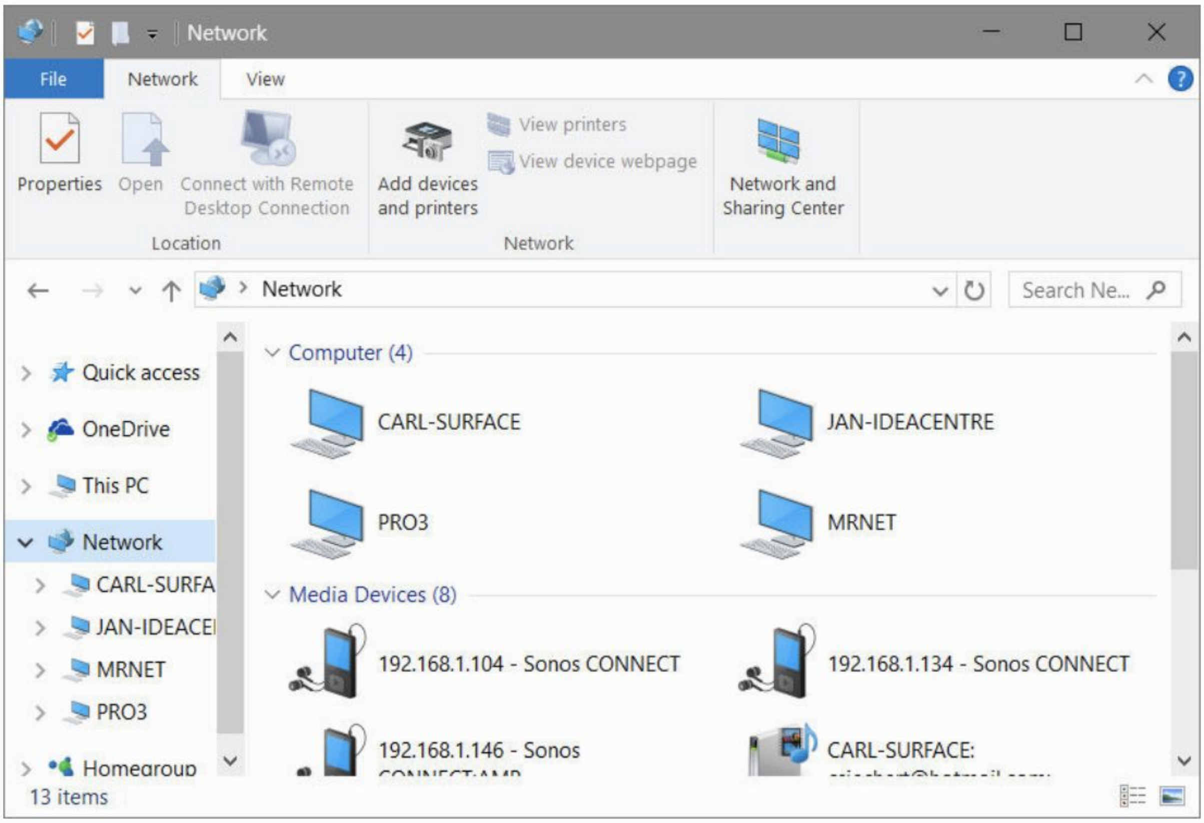
Printer Name	Queue Status	Jobs In ...	Server Name	Driver
Brother HL-L2360D series	Ready	0	Carl-Surface (l...	Broth
EPSON Artisan 725	Offline	1	Carl-Surface (l...	EPSO
Fax	Ready	0	Carl-Surface (l...	Micrc
Microsoft Print to PDF	Ready	0	Carl-Surface (l...	Micrc
Microsoft XPS Document Writer	Ready	0	Carl-Surface (l...	Micrc
Quicken PDF Printer	Ready	0	Carl-Surface (l...	Amyu
Send To OneNote 2016	Ready	0	Carl-Surface (l...	Send

Document Name	Job Status	Owner	Pages	Size
Files - OneDrive	Sent to Prin...	SYSTEM	1	514 KB

Finding and using shared resources on a Windows network

The Network folder is your gateway to all available network resources, just as This PC is the gateway to resources stored on your own system.

The Network folder (shown in the next image) contains an icon for each computer that Windows discovers on your network; double-click a computer icon to see that computer's shared resources, if any.



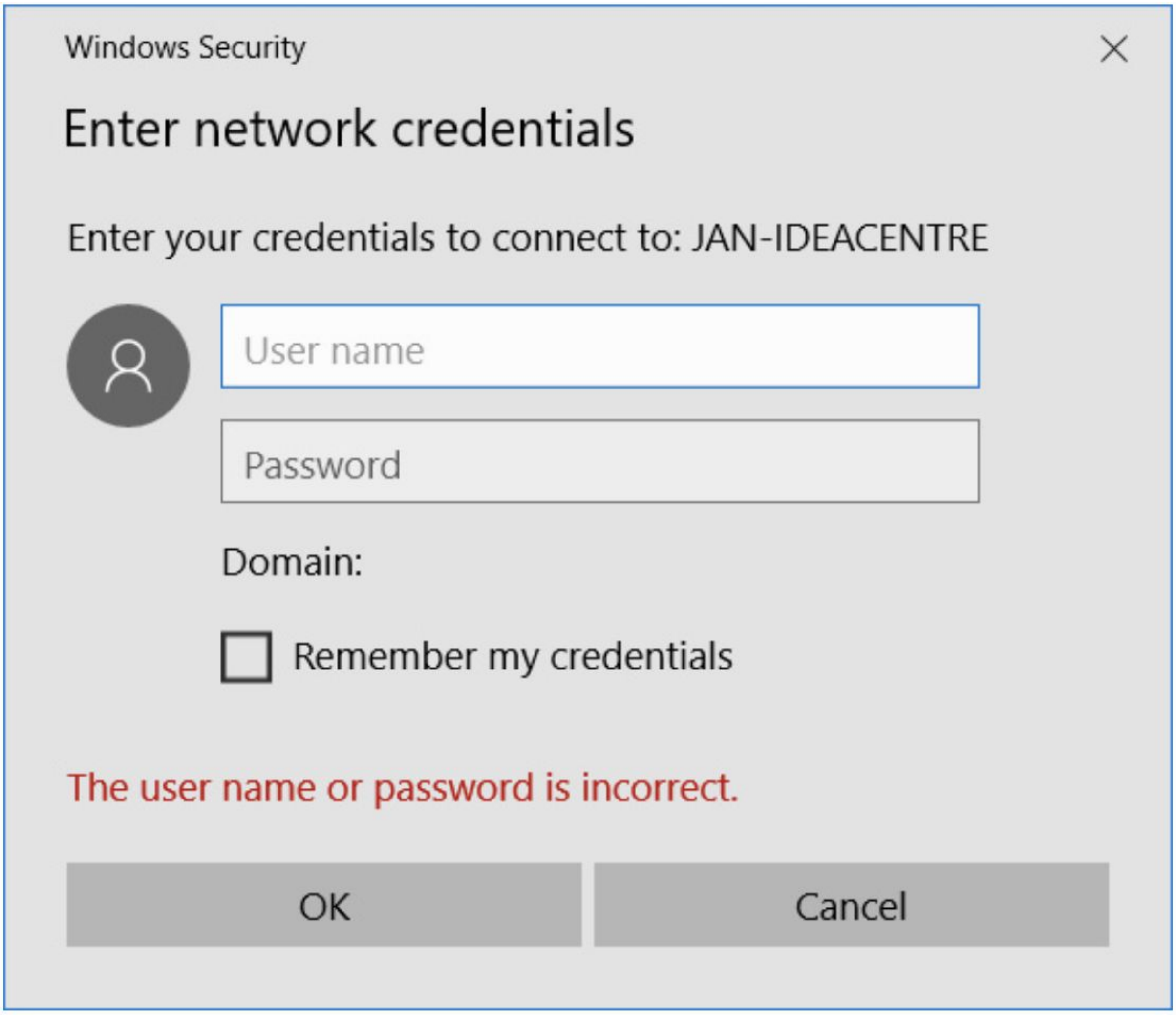
To open a shared folder on another computer, double-click its icon in the Network folder.

If you have the proper permissions, this action displays the folder's contents in File Explorer.

It's not always that easy, however.

If the user account with which you signed in doesn't have permission to view a network computer or resource you select, a dialog box (shown next) asks you to provide the name of an account (and its password, of course) that has permission.

Don't be fooled by the Domain reference below the User Name and Password boxes; in a workgroup, that value refers to the local computer.



Windows Security

Enter network credentials

Enter your credentials to connect to: JAN-IDEACENTRE

Domain:

□ Remember my credentials

The user name or password is incorrect.

Perhaps the trickiest part of using shared folders is fully understanding what permissions have been applied to a folder and which credentials are in use by each network user.

It's important to recognize that all network access is controlled by the computer with the shared resources; regardless of what operating system runs on the computer attempting to connect to a network share, it must meet the security requirements of the computer where the shared resource is actually located.

Working with mapped network folders

Mapping a network folder makes it appear to applications as though the folder is part of your own computer.

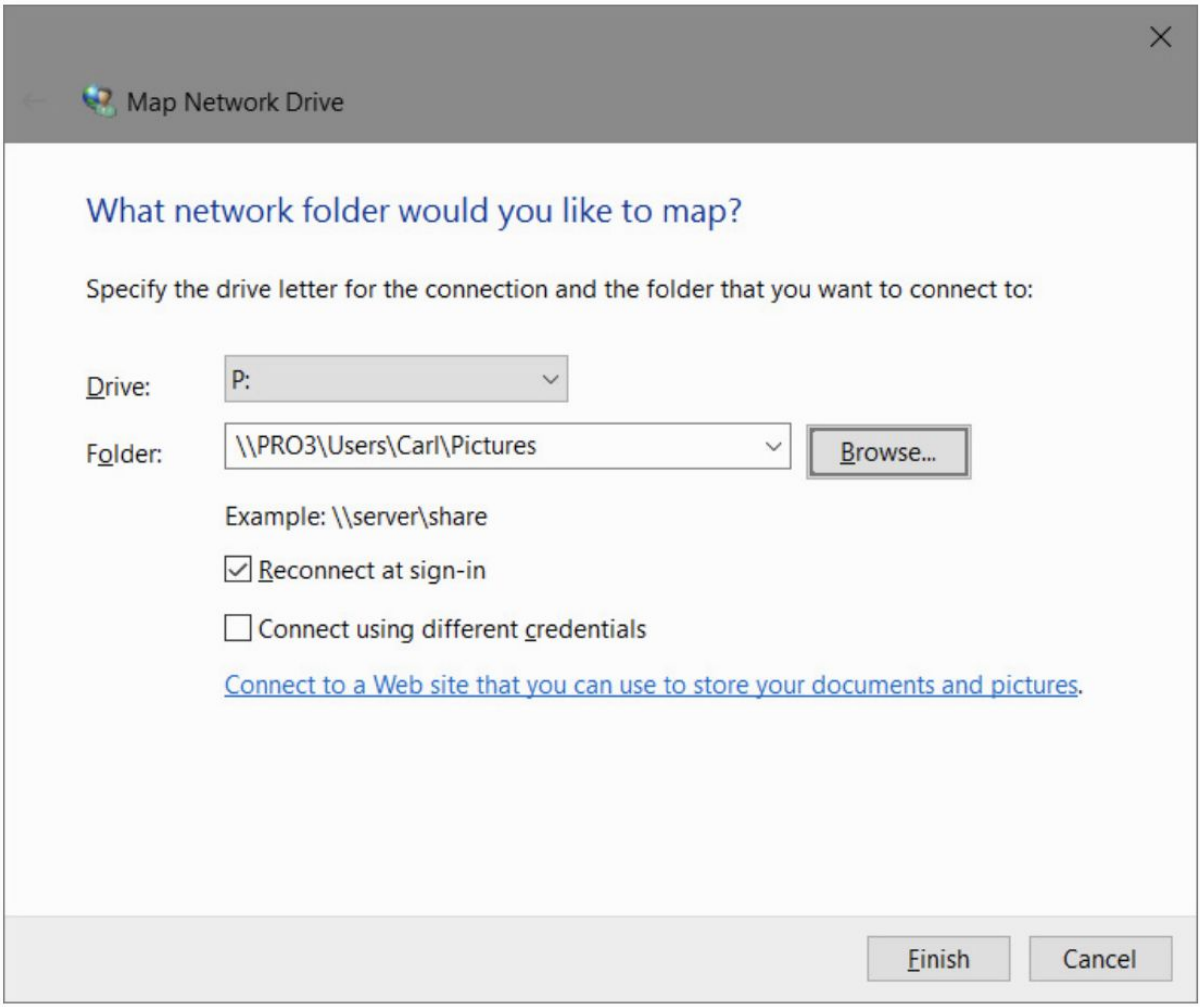
Windows assigns a drive letter to the mapped folder, making the folder appear like an additional hard drive.

You can still access a mapped folder in the conventional manner by navigating to it through the Network folder.

But mapping gives the folder an alias—the assigned drive letter—that provides an alternative means of access.

To map a network folder to a drive letter, follow these steps:

1. Open This PC in File Explorer, and on the ribbon's Computer tab, click Map Network Drive. Alternatively, after you open a computer in the Network folder, right-click a network share and choose Map Network Drive.



What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: P:

Folder: \\PRO3\Users\Carl\Pictures

Example: \\server\share

☑ Reconnect at sign-in

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

2. Select a drive letter from the Drive list. You can choose any letter that's not already in use.

3. In the Folder box, type the path to the folder you want or, more easily, click Browse and navigate to the folder.

4. Select Reconnect At Sign-In if you want Windows to connect to this shared folder automatically at the start of each session.

5. If your regular sign-in account doesn't have permission to connect to the resource, select Connect Using Different Credentials. After you click Finish, Windows asks for the user name and password you want to use for this connection.

6. Click Finish.

In File Explorer, the “drive” appears under This PC.

If you change your mind about mapping a network folder, right-click the folder’s icon in your This PC folder.

Choose Disconnect on the resulting shortcut menu, and the connection will be severed.

Connecting to a network printer

To use a printer that has been shared, open the Network folder in File Explorer and double-click the name of the server to which the printer is attached.

If the shared printers on that server are not visible, return to the Network folder, click to select the server, and then, on the ribbon’s Network tab, click View Printers.

Right-click the printer and choose Connect.

Alternatively, from the Devices And Printers folder, click Add A Printer and use the Add Printer Wizard to add a network printer.

Connecting to another computer with Remote Desktop

Sharing computer resources over a network, when properly configured, gives you access to all the files you might need, wherever they’re stored.

But sometimes even that’s not enough.

You might need to run a program that’s installed only on another computer, or you might need to conFigure and manage another computer’s files and settings in ways that can be done only by sitting down in front of that computer.

As it turns out, there’s an alternative to direct physical access: Remote Desktop.

By using a Remote Desktop session, you can operate a computer by remote control over a local network or over the internet.

Windows includes a desktop program for remote access called Remote Desktop Connection.

Although this program’s appearance remains largely unchanged since its inclusion in Windows XP, it’s still perfectly suitable for remote connections.

A newer alternative, called Remote Desktop, is available through the Store.

This Universal Windows Platform app works on a wide variety of Windows 10 device types, and it includes some capabilities not available in Remote Desktop Connection.

With Remote Desktop, applications run on the remote computer; your computer is effectively used as a dumb terminal.

You can use a low-powered computer—an inexpensive laptop or an old desktop clunker—and enjoy the speed and power of the remote computer.

With the Remote Desktop app, you can even use your phone or other mobile device to connect to a remote computer.

Remote Desktop connections are encrypted, so your information is secure, even if you're making a connection over the internet.

The basic requirements for using Remote Desktop are pretty simple: you need two computers that are connected via a local area network, the internet, or a dial-up connection.

The computer that you want to control—the one at the remote location—is called the remote computer.

The computer you want to use to control the remote computer is called the client computer.

These are the requirements for the two computers:

- Remote computer. You need a computer running Windows 10 Pro, Enterprise, or Education. Windows 10 Home does not include the software required for hosting Remote Desktop sessions. The remote computer can also use Windows 8 or 8.1 (Pro or Enterprise editions), Windows 7 (Professional, Enterprise, or Ultimate editions), Windows Vista (Business, Enterprise, or Ultimate editions), Windows XP Professional (or Windows XP Media Center or Tablet PC editions), Windows Home Server, or Windows Server. This computer must have a connection to a local area network or to the internet. If you're going to connect to this computer over the internet, its internet connection must have a known, public IP address.
- Client computer. You can access Remote Desktop from a computer running any version of Windows or Windows Phone. Remote Desktop client software from Microsoft is also available for iOS, OS X, and Android; third-party apps are available for Linux and other operating systems. To find one, search for "RDP apps." RDP is short for Remote Desktop Protocol, the networking protocol that enables Remote Desktop.

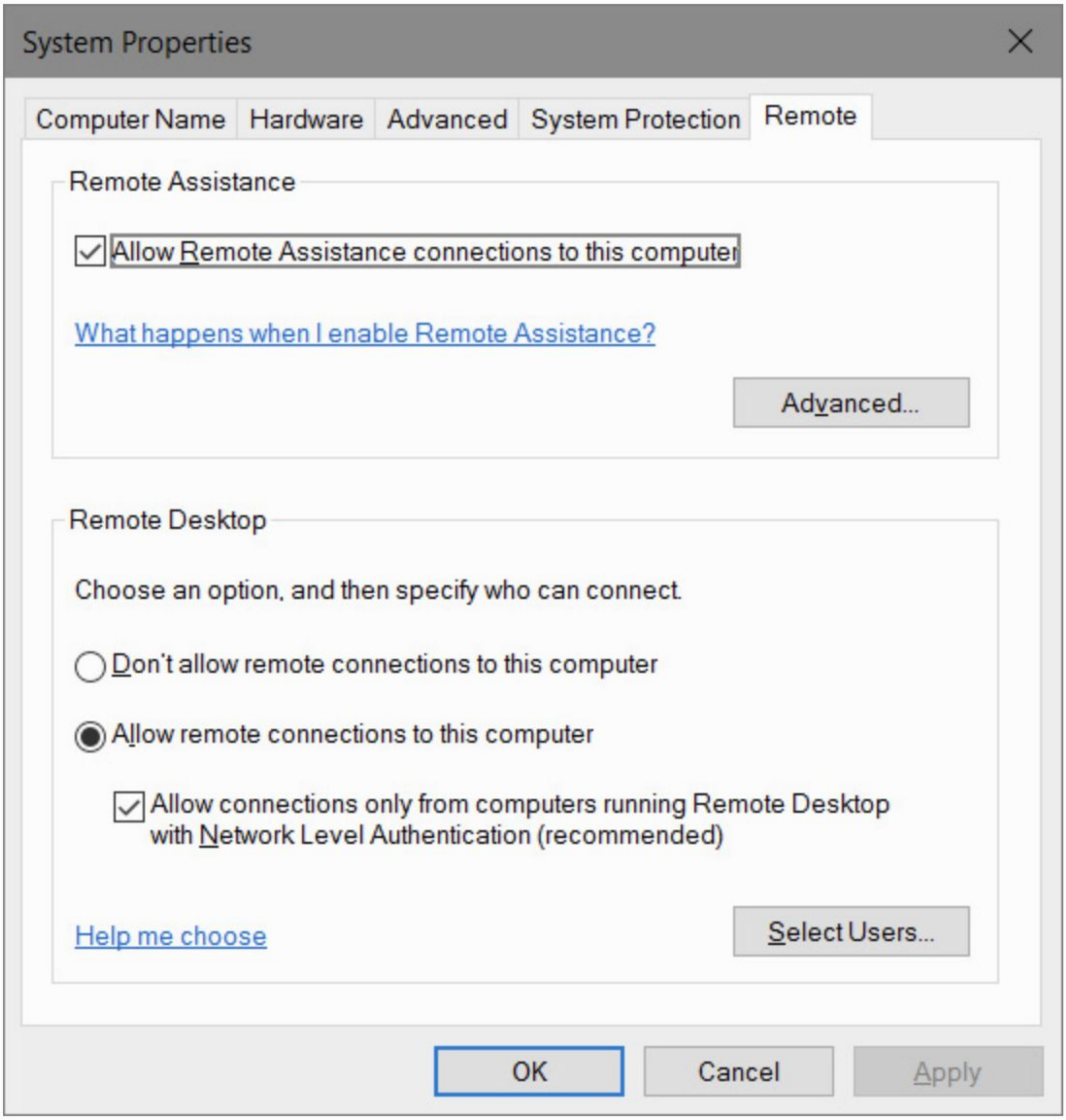
Enabling inbound remote desktop connections

If you intend to connect to a remote computer—whether it's at home while you're away, at work when you're out of the office, or just down the hall—you must first enable Remote Desktop on that computer.

To set up a computer running Windows 10 Pro, Enterprise, or Education to accept Remote Desktop connections, follow these steps:

1. Open Control Panel > System And Security > System, or use this shortcut to get to the same place: Right-click the Start button and choose System. In the left pane, click Remote Settings. Or use the undocumented command "systempropertiesremote".

2. Under Remote Desktop, select Allow Remote Assistance Connections To This Computer, as shown next.



System Properties

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

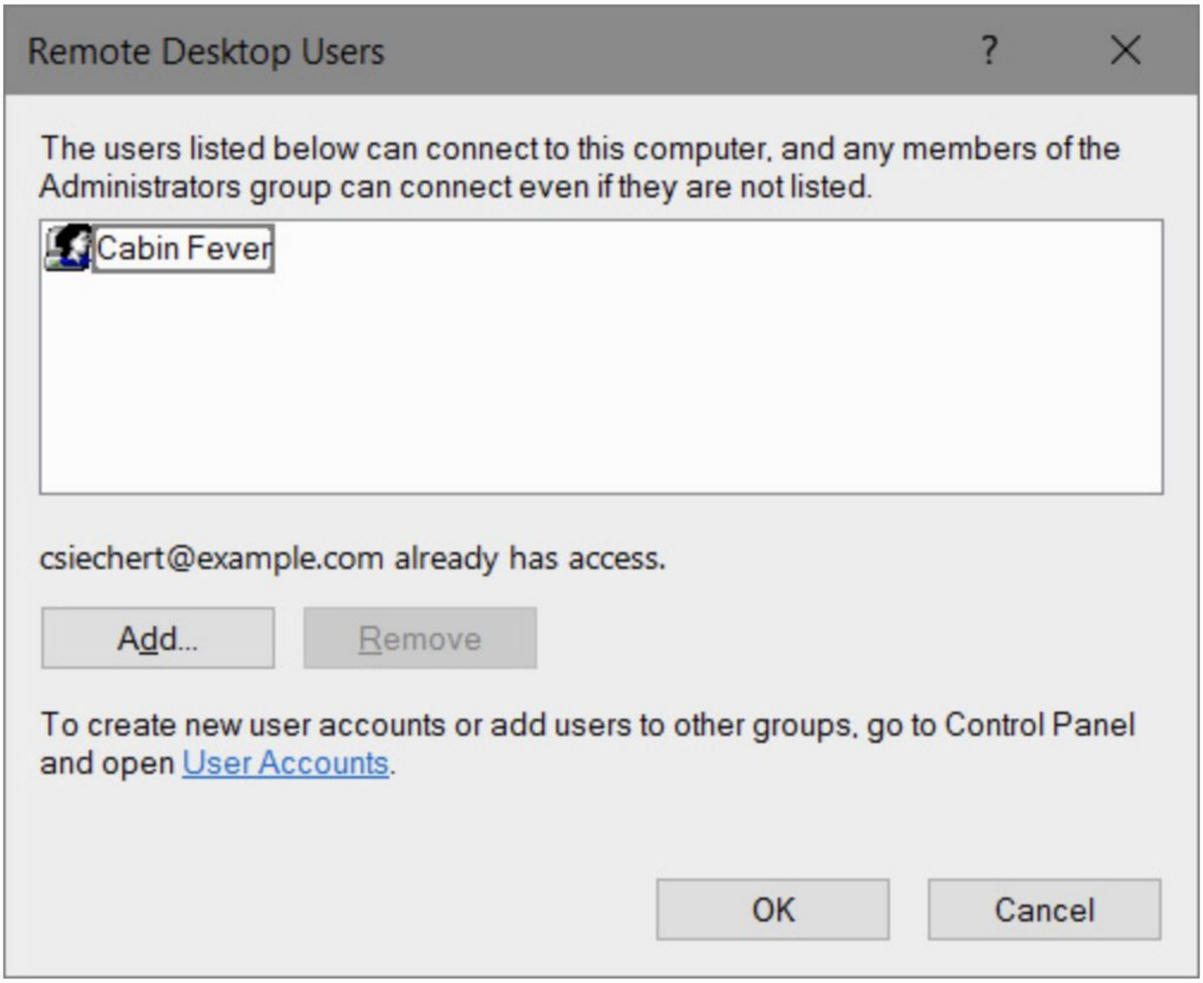
☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

Unless you anticipate you'll need to access your computer from a computer running an ancient version of Remote Desktop Connection, leave Allow Connections Only From Computers Running Remote Desktop With Network Level Authentication (Recommended) selected.

At this point, the current user account and any user account that's a member of the local Administrators group can be used to connect remotely to the computer, provided that the account has a sign-in password. As a security precaution, accounts that use a blank password cannot be enabled for remote connections.

3. If you want to change which users can connect remotely, click Select Users. The Remote Desktop Users dialog box appears:



Remote Desktop Users

The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

Cabin Fever

csiechert@example.com already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

- To add a user to the Remote Desktop Users group, click Add. Then type the user's name in the Select Users dialog box that appears (or click Advanced, Find Now to select names from a list). You can type the name of any local user account or, if your computer is in a domain, any domain user account. You can add multiple users by separating each user name with a semicolon.
- To delete a user from the Remote Desktop Users group, select the user's name in the Remote Desktop Users dialog box and click Remove.

That's all you need to do to set up the remote computer. Windows configures rules for Remote Desktop in Windows Firewall when Remote Desktop is enabled, allowing connection requests on port 3389 to be received from any IP address.

If your connection has to pass through a router to get to your computer, be sure you take the additional steps outlined earlier in “Configuring your network for Remote Desktop connections.”

If you replaced Windows Firewall with a third-party software firewall, you need to conFigure it to allow incoming access to TCP port 3389.

Using the Remote Desktop app

Remote Desktop is a modern app that’s not included with Windows; it is, however, available as a free download via the Store.

Remote Desktop offers several features not found in Remote Desktop Connection.

Its visual approach shows all your remote connections on the home screen, allowing you to open one with a single click or tap.

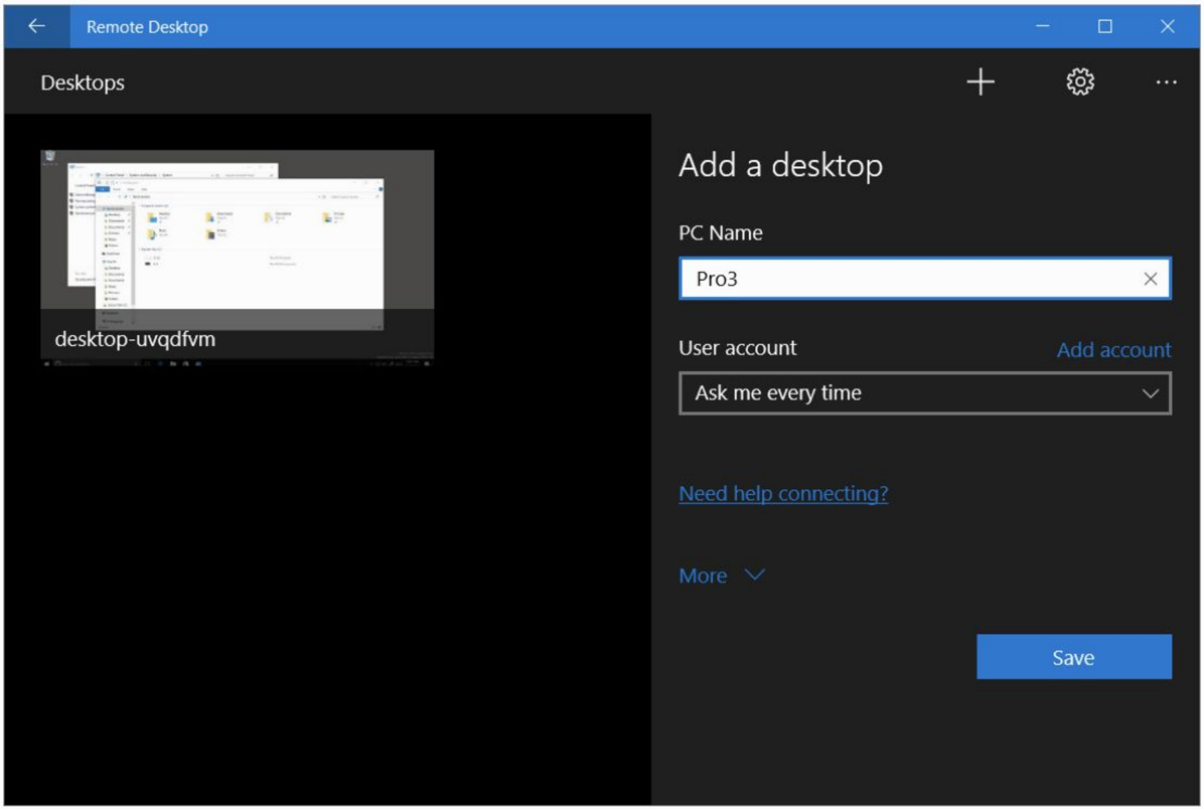
In addition, Remote Desktop includes several performance enhancements that optimize your connection quality.

And, of course, as a modern app, it’s touch friendly.

Install the Remote Desktop app, and after you’ve enabled incoming remote connections on your PC at home or in the office and verified that your network and firewall have the welcome mat out (for visitors with suitable credentials only, of course), you’re ready to begin using Remote Desktop.

To begin using Remote Desktop, click the Add (+) button and then click Desktop.

Add A Desktop appears in the right pane, as shown in the next picture.



Add a desktop

PC Name: Pro3

User account: Ask me every time

Add account

To set up a connection to a remote desktop, enter this information in the Add A Desktop pane:

- PC Name Enter the name or IP address of the remote computer.
- User Account Select Ask Me Every Time to be prompted for your user name and password each time you connect to the desktop. Alternatively, you can click the arrow at the right side and select a user account, and Remote Desktop uses that account without asking for credentials. If the account you want to use doesn't appear in the list, click Add Account.

At this point you've entered all the information necessary to make the connection and you can click Save.

However, you can set additional parameters, including some that come into view when you click More:

- Display Name You can provide a friendly name that appears under the icon for a remote computer in the main Remote Desktop window.
- Audio Here you choose where sounds should emanate from when an app on the remote computer plays audio. You can have it play on the remote computer, on your client computer, or nowhere.
- Switch Mouse Buttons This option, sure to induce confusion, swaps the functionality of the left and right mouse buttons while you work in the remote desktop. They maintain their normal functionality while you work in your own local desktop.

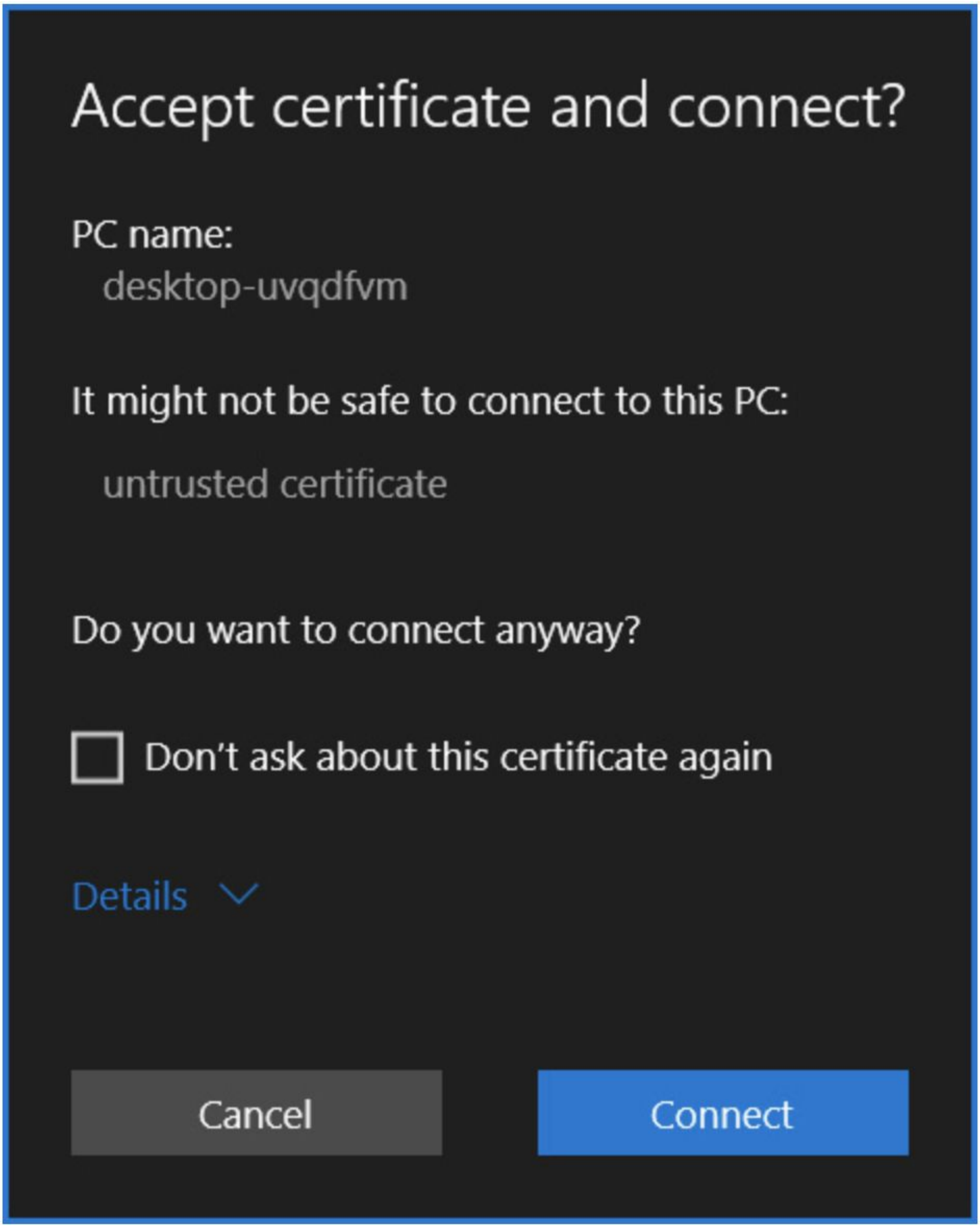
Working in a Remote Desktop session

After you save a connection in the Add A Desktop pane, an icon for that connection appears in Remote Desktop.

Click the icon to open a connection to the remote computer.

Along the way, you might encounter a couple of obstacles:

- If you specified Ask Me Every Time in the User Account box, Remote Desktop asks for the user name and password of an account authorized on the remote computer to make a connection. Select Remember Me, and you won’t need to enter this information in future sessions.
- If the remote computer doesn’t have a digital certificate that’s trusted by your computer to positively identify it, you’ll be asked whether you want to accept the untrusted certificate, as shown next. If you’re certain that you’re connecting to the right computer, select the check box (so you won’t be bothered in future sessions) and click Connect, as shown next.



Accept certificate and connect?

PC name:
desktop-uvqdfvm

It might not be safe to connect to this PC:
untrusted certificate

Do you want to connect anyway?

□ Don’t ask about this certificate again

After bounding past those hurdles, Remote Desktop attempts to open a connection.

If the account you use for the remote connection is already signed in to the remote computer—or if no one is signed in to the remote computer—the remote computer’s desktop then appears on your computer.

If a different user account is signed in to the remote computer, Windows lets you know that you’ll be forcing that person to sign out and gives you a chance to cancel the connection.

On the other end, the signed-in user sees a similar notification that offers a short time to reject the remote connection before it takes over.

Note that only one user at a time can control the desktop of a computer running Windows.

Whoever is currently signed in has the final say on whether someone else can sign in.

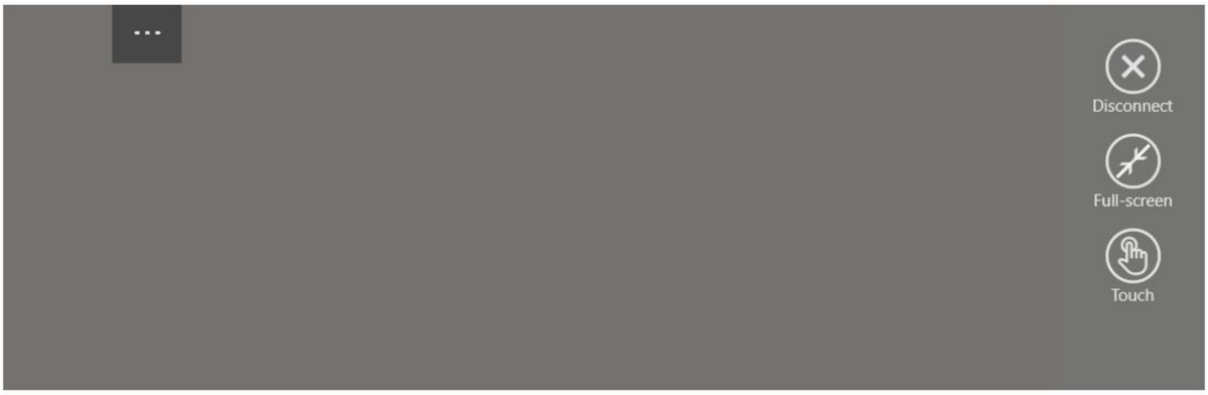
While you're connected to the remote computer, the local display on that computer (if it's turned on) does not show what you see on the client computer but instead shows the lock screen.

A person who has physical access to the remote computer can't see what you're doing (other than the fact that you're signed in remotely).

When you connect to a remote computer using the universal Remote Desktop app, the remote computer takes over your entire screen.

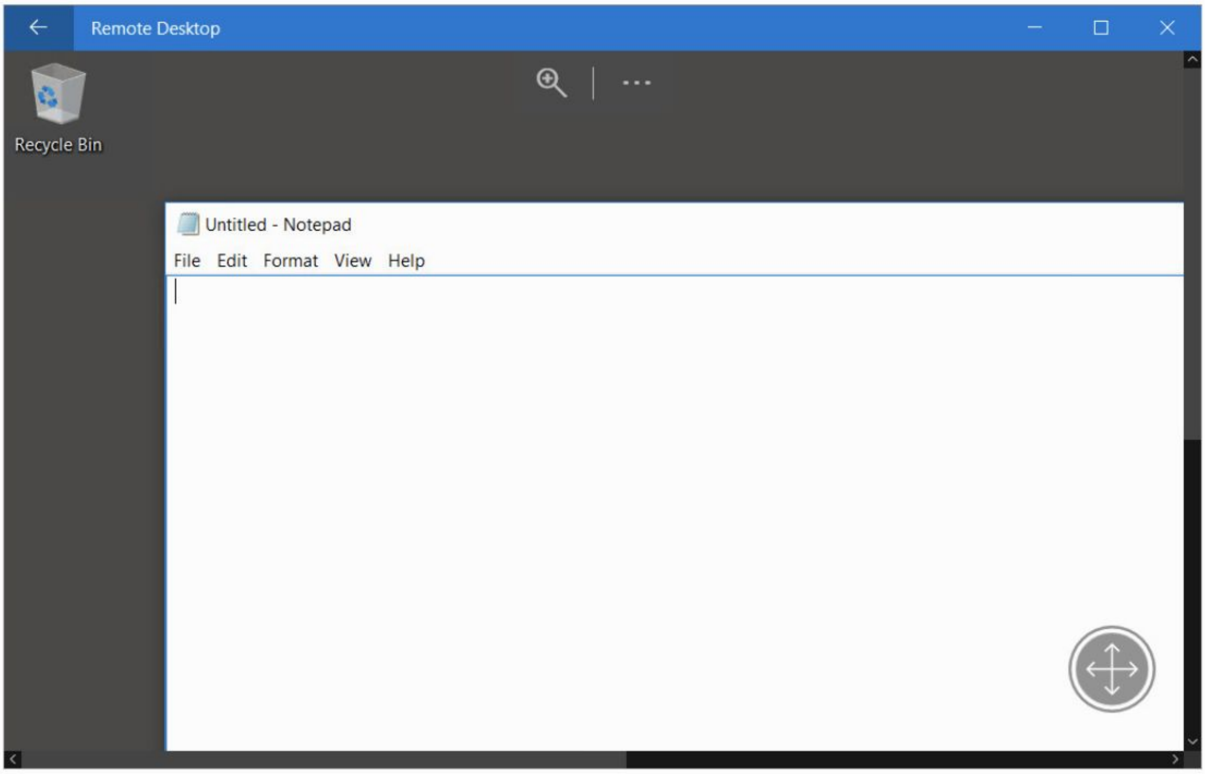
It uses the resolution of the client computer, regardless of the resolution set on the remote computer.

At the top of the screen, in the center, a button with three dots appears, as shown in the next figure:



The buttons that appear on the right side offer these functions:

- Disconnect. Clicking this button ends your remote session and returns you to the main Remote Desktop window. The remote computer remains locked, ready for someone to sign in locally.
- Full-Screen. This button toggles between full-screen and windowed views of the remote desktop. The next picture shows a Remote Desktop window.



- Touch. If your client computer has a touchscreen, clicking this button enables touch control of the remote computer. When you switch to this mode, a magnifier icon appears along the top edge of the screen; use this to enlarge the display so that it's easier to hit touch targets.

While in full-screen mode, two more controls are less obvious.

Move the mouse pointer to the top edge of the screen, and a small button appears; click it to display the Remote Desktop title bar, which includes the usual window controls (minimize, resize, and close) as well as a button at the left end that disconnects your session and returns to the main window.

Move the mouse pointer to the bottom edge of the screen and a similar button appears; click it to display the taskbar for your local computer.

If your computer has a touchscreen, you can see these buttons by dragging in from the top or bottom edge of the screen.

Ending a remote session

When you're through with a Remote Desktop Connection session, you can lock, sign out, or disconnect.

If the remote computer is running Windows 10, you'll find these options in the usual places where comparable options appear on your local computer: Lock and Sign Out appear when you click the user name at the top of Start on the remote computer, and Disconnect appears when you click Power on Start.

For remote machines running earlier Windows versions, these options appear in the lower right corner of the remote session's Start menu.

You must click the arrow to see all the options.

Locking the computer keeps the remote session connected and all programs running, but it hides everything behind a sign-in screen that requests a password; this is comparable to pressing Windows key+L to lock your computer.

Signing out closes all your programs, exits your user session, and disconnects.

If you disconnect without signing out, your programs continue to run on the remote computer, but the remote connection is ended.

The sign-in screen is visible on the remote computer, and it's available for another user.

If you sign in later—either locally or through a remote connection—you can pick up right where you left off.

As an alternative to the Start commands, you can disconnect by clicking the Disconnect button, displaying the Remote Desktop title bar and clicking the Back button, or simply closing the Remote Desktop window.

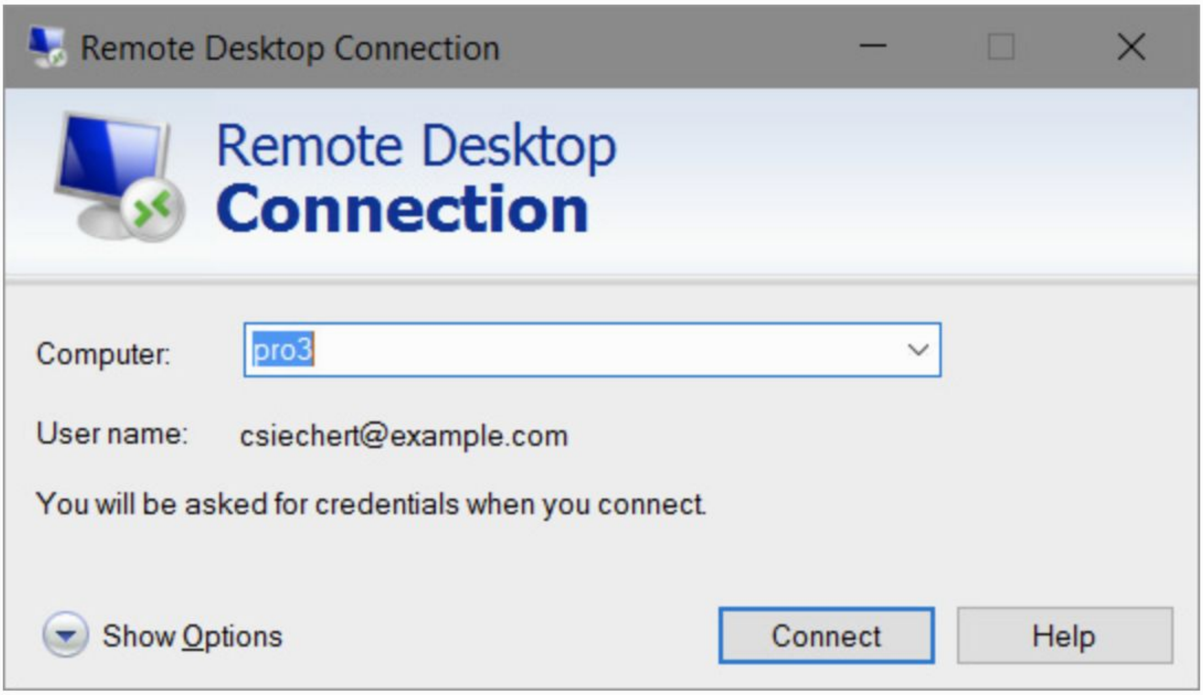
Using Remote Desktop Connection

Remote Desktop Connection is a desktop app that might be familiar to longtime remote desktop users.

To start it, in the search box, type "remote" and then click "Remote Desktop Connection".

A dialog box like the one shown in the next image appears.

In the Computer box, type the name of the remote computer or its IP address.



Computer: pro3

User name: csiechert@example.com

You will be asked for credentials when you connect.

If you’re willing to accept the default settings, you can click Connect at this point.

If you’re signed in to the client computer using an account other than one that’s authorized on the remote computer, Windows first displays a request for credentials.

After you enter your credentials and they’re approved, Windows initiates the Remote Desktop Connection session.

The remote computer’s sign-in screen then appears on your computer, either in a window or a full-screen display.

Enter your password; other sign-in options (that is, PIN, picture password, or biometric sign-in) are not available for a remote connection.

As with Remote Desktop (described in the preceding sections), Windows warns if your connection will knock off another user who’s signed in to the remote computer.

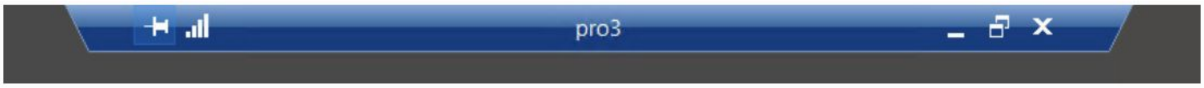
Changing screen resolutions and display settings

When you connect, the display from the remote computer fills your entire screen, using the resolution of the client computer.

Along the top of the screen, in the center, a small title bar appears, as shown next.

This title bar, dubbed the connection bar in Remote Desktop Connection, lets you switch between your own desktop and the remote desktop.

The Minimize, Maximize, and Restore buttons work as they do in other programs.



The pushpin button locks the connection bar in place.

If you click the pushpin, the connection bar disappears completely, retracting into the top of the screen.

To make the connection bar reappear, “bump” the mouse pointer to the top edge of the screen.

To keep the connection bar visible at all times, click the pushpin again.

The Close button disconnects the remote computer (but does not sign you out of the remote computer) and closes Remote Desktop Connection.

You can pick up where you left off by reopening Remote Desktop Connection and reconnecting or by signing in locally at the remote computer.

If the connection bar covers a part of the screen you need to see, you can move it instead of hiding it altogether with the pushpin button.

Simply slide it left or right.

You might prefer to use less than your full screen resolution for the remote desktop.

This option is especially useful if you have a large monitor and the work you want to do with Remote Desktop is just another task among several.

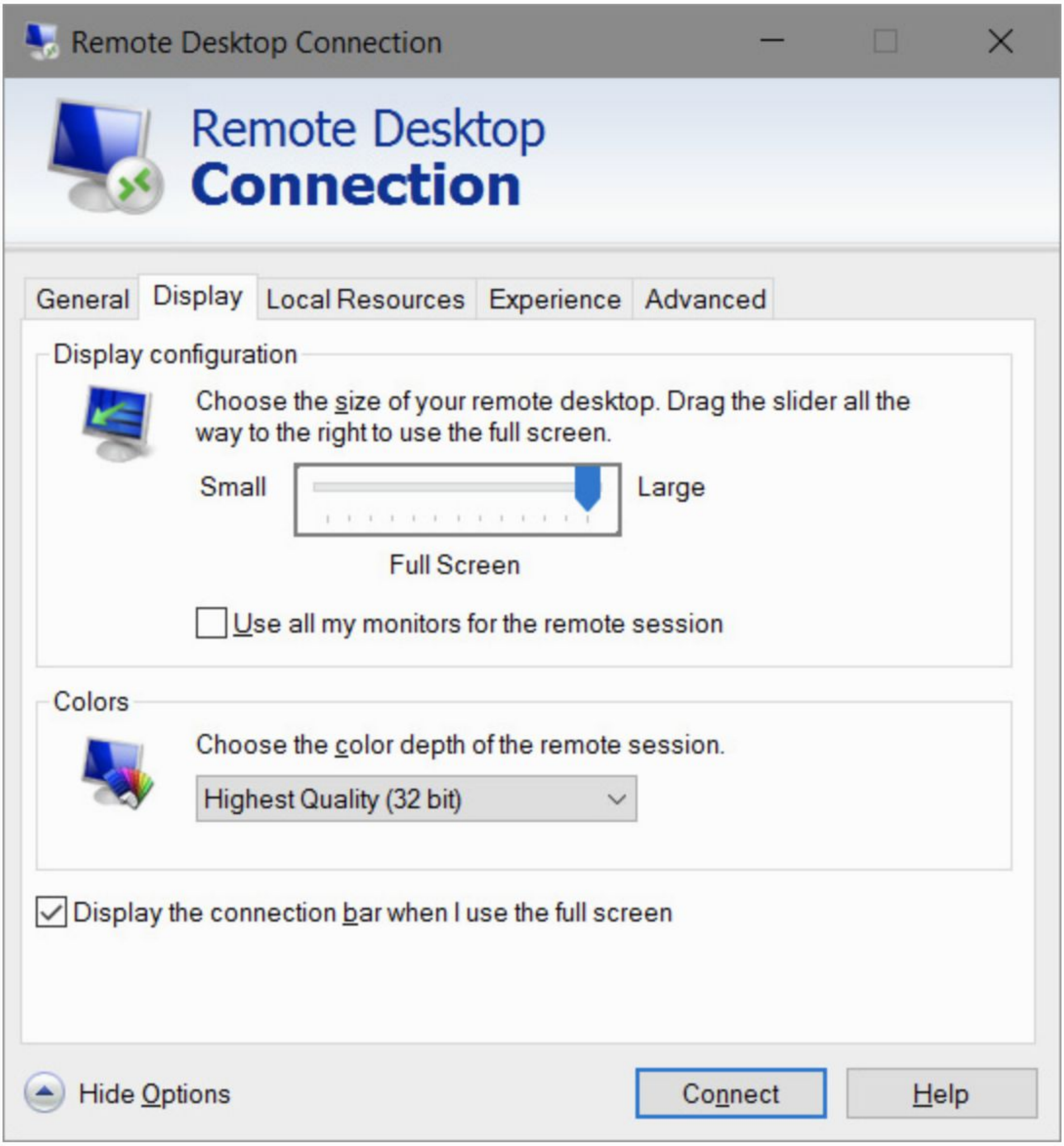
You must set the resolution—along with a number of other options—before you connect to the remote computer.

After you start Remote Desktop Connection, click the Show Options button to expand the dialog box.

Then click the Display tab, which is shown in the next image.

You can set the screen resolution to any size that’s supported on the client hardware, from 640 by 480 up to the current resolution of the client computer (not the remote computer).

Set it to full screen by moving the slider all the way to the right.



Display configuration

Choose the size of your remote desktop. Drag the slider all the way to the right to use the full screen.

Small — Large

Full Screen

□ Use all my monitors for the remote session

Colors

Choose the color depth of the remote session.

Highest Quality (32 bit)

☑ Display the connection bar when I use the full screen

Remote Desktop Connection allows the use of multiple monitors, as long as the remote computer is running Windows 7 or later.

To configure the connection for use with more than one monitor, select Use All My Monitors For The Remote Session.

Accessing local resources

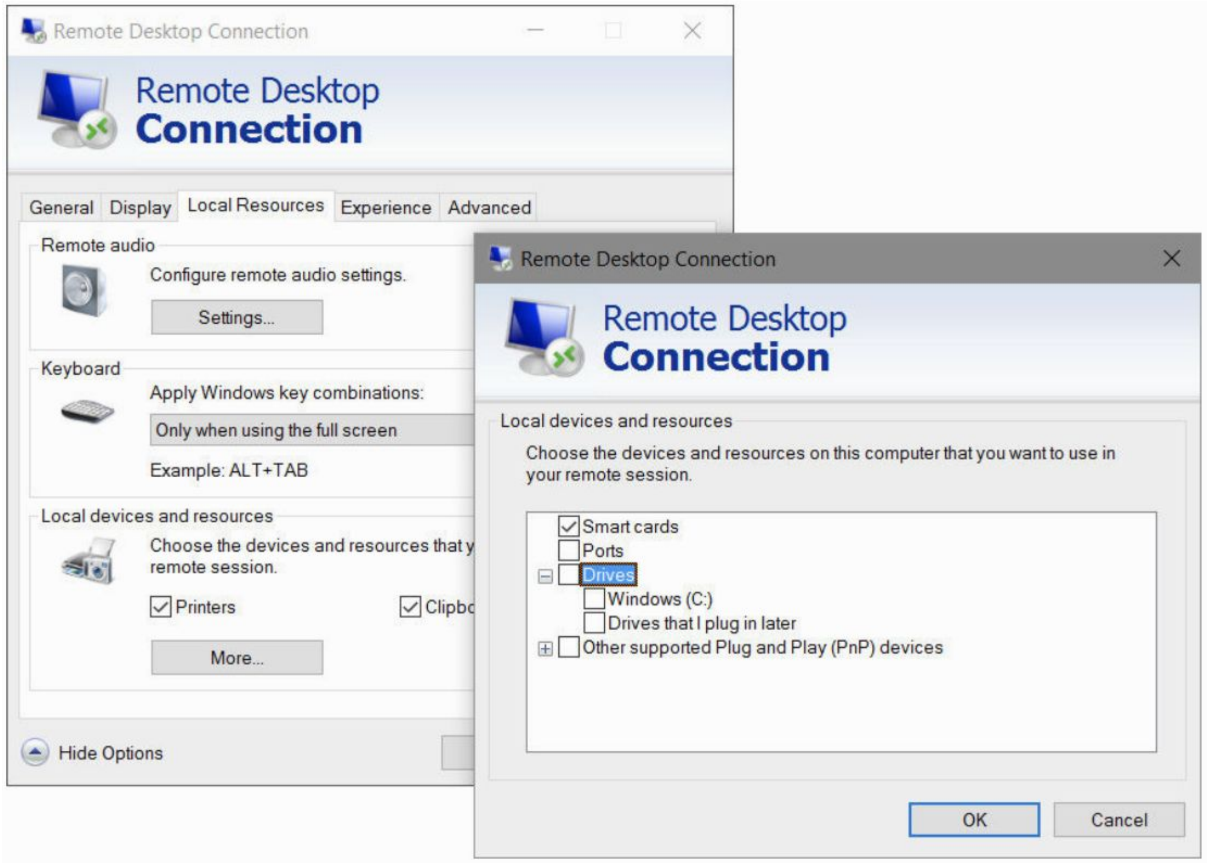
While you use Remote Desktop Connection, it's immediately apparent you have control of the remote computer.

That's terrific if the remote computer has everything you need.

But you'll often want to use local resources and information from the client computer as well as from the remote computer.

In addition, you might want to move information between the two computers.

With Remote Desktop Connection, you can do so easily by clicking Show Options to expand the Remote Desktop Connection dialog box and then adjusting any of the options on the Local Resources tab, shown in the next figure.



Remote audio

Configure remote audio settings.

Keyboard

Apply Windows key combinations:

Only when using the full screen

Example: ALT+TAB

Local devices and resources

Choose the devices and resources that y remote session.

☑ Printers ☑ Clipbo

Remote Desktop Connection

Local devices and resources

Choose the devices and resources on this computer that you want to use in your remote session.

☑ Smart cards
☐ Ports
⊟ ☐ Drives
☐ Windows (C:)
☐ Drives that I plug in later
⊞ ☐ Other supported Plug and Play (PnP) devices

The following options are available:

- Remote Audio. If your music collection is on the remote PC and you want some tunes at your current location, click Settings and select Play On This Computer. If you want both computers to be silent, choose Do Not Play. After clicking Settings, you can also tell Remote Desktop Connection whether to pay attention to the microphone (or other audio input) on the client computer.
- Keyboard. When you press a Windows keyboard shortcut such as Alt+Tab, do you want the shortcut to take effect on the remote machine or on your client computer?
- Printers. When this option is selected, your local printers appear in the remote computer's Printers folder. Their entries have "(from clientcomputername)" appended to each printer name. To print to a local printer, select its name in the Print dialog box from any application.
- Clipboard. When you copy or cut text or graphics on either the remote computer or the local computer, it's saved on the Clipboard in both locations. The Clipboard contents are then available for pasting in documents on either

computer. Similarly, you can cut or copy files or folders from a File Explorer window on either computer and paste them into a folder on the other computer. Clear this option if you want to keep the contents of the two Clipboards separate.

The More button leads to additional devices in the Local Devices And Resources category.

Smart cards are automatically enabled, and serial ports are disabled by default.

Local drives and Plug and Play devices are also disabled by default.

They can be enabled individually.

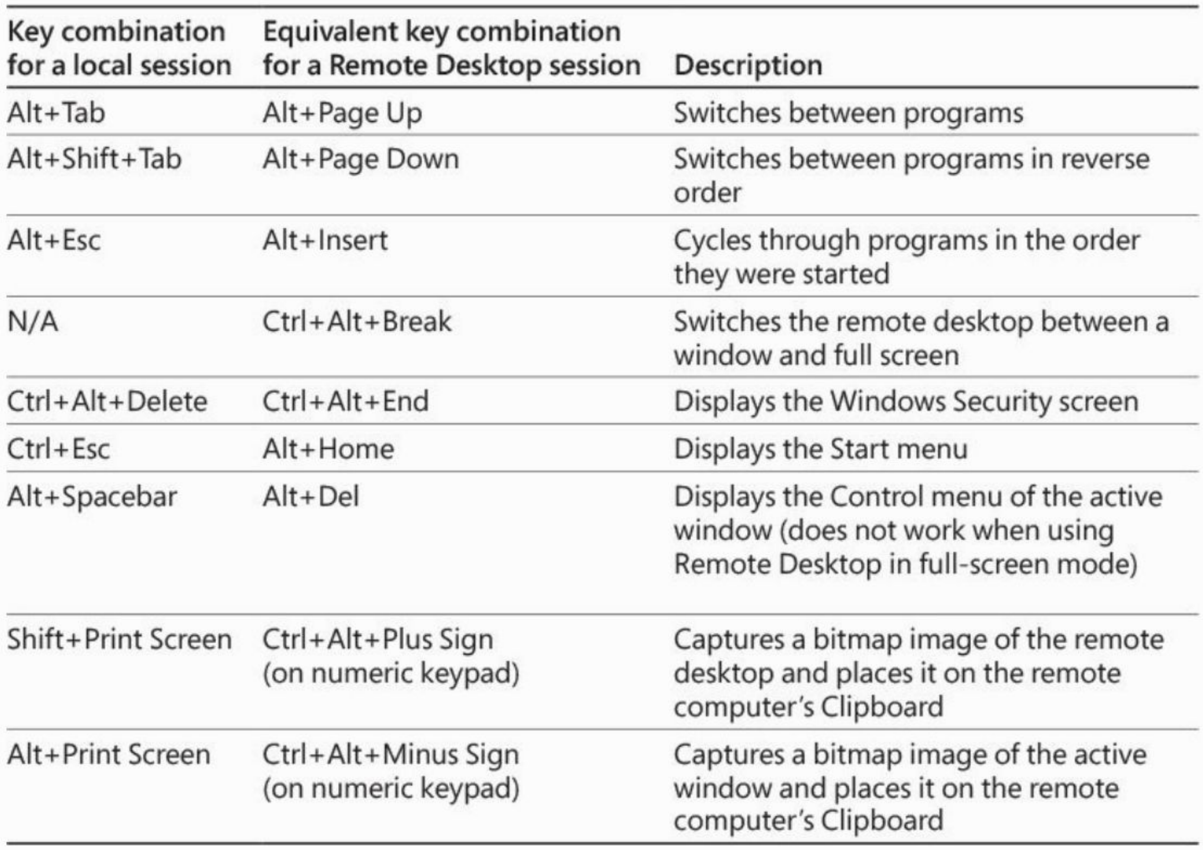
These options are most useful if you're expecting to do most or all of your work with the Remote Desktop session in full-screen view and you don't want to continually flip back to your local desktop for file-management tasks.

Using the keyboard with Remote Desktop Connection

When the Remote Desktop Connection window is active, almost every key you press is passed to the remote computer.

Certain key combinations, however, can be processed by the client computer, depending on the setting you make in the Keyboard section of the Local Resources tab of the Remote Desktop Connection dialog box.

You can specify that the key combinations shown in the first column of the following table are sent to the remote computer all the time, only when the remote desktop is displayed in full-screen mode, or never.



Key combination for a local session	Equivalent key combination for a Remote Desktop session	Description
Alt+Tab	Alt+Page Up	Switches between programs
Alt+Shift+Tab	Alt+Page Down	Switches between programs in reverse order
Alt+Esc	Alt+Insert	Cycles through programs in the order they were started
N/A	Ctrl+Alt+Break	Switches the remote desktop between a window and full screen
Ctrl+Alt+Delete	Ctrl+Alt+End	Displays the Windows Security screen
Ctrl+Esc	Alt+Home	Displays the Start menu
Alt+Spacebar	Alt+Del	Displays the Control menu of the active window (does not work when using Remote Desktop in full-screen mode)
Shift+Print Screen	Ctrl+Alt+Plus Sign (on numeric keypad)	Captures a bitmap image of the remote desktop and places it on the remote computer's Clipboard
Alt+Print Screen	Ctrl+Alt+Minus Sign (on numeric keypad)	Captures a bitmap image of the active window and places it on the remote computer's Clipboard

If you select On This Computer, key combinations from the first column of the previous table are always applied to the client computer.

To get the equivalent function on the remote computer, press the key combination shown in the second column.

The same is true if you select Only When Using The Full Screen and the remote session is displayed in a window.

If you select On The Remote Computer, key combinations from the first column are applied to the remote computer.

Key combinations in the second column are ignored (unless they have some function in the active application on the remote desktop).

The same is true if you select Only When Using The Full Screen and the remote session is displayed in full-screen mode.

One exception is the Ctrl+Alt+Delete combination, which is always applied to the client computer.

Regardless of your Local Resources tab setting, you must press Ctrl+Alt+End to obtain the same result on the remote computer.

Configuring performance options

When you first use Remote Desktop Connection, you might notice that the remote desktop doesn't display a background.

Disabling the background is one of several settings you can make that affect the perceived performance of your remote session.

How you set these options depends in large measure on the speed of the connection between the two computers.

If you're using a slow, bandwidth-challenged, or metered connection, you should disable as many features as possible to reduce the amount of information that must be transmitted across the wire and keep the mouse and windows movements responsive.

On the other hand, if you're connecting to another desktop over a fast local area network, you might as well enable all features to enjoy the full experience of working at the remote computer.

The performance-related options are on the Experience tab of the Remote Desktop Connection dialog box.

To quickly select an appropriate set of prepackaged options, select the speed of your connection from the list box. Use those settings or select your own options.

Saving a Remote Desktop configuration

Changes you make in the expanded Remote Desktop Connection dialog box are automatically saved in a hidden file named Default.rdp (stored in your default save location for documents), and they're used the next time you open Remote Desktop Connection.

But you might want to have several different Remote Desktop Connection configurations for connections to different computers.

If you have a portable computer, you might want different settings for use with different connections to the same computer (for example, a slow Wi-Fi connection from a hotel versus a fast LAN at your branch office).

You can also save your credentials (user name and password) along with the other settings.

To do so, enter your user name under Logon Settings on the General tab and select Allow Me To Save Credentials.

You'll be prompted to save the password (in encrypted form, of course) when you sign in.

Note that not all remote operating systems allow the use of saved credentials.

To save a configuration, after you make all your settings, click the General tab, and click Save As.

To reuse a stored configuration at a later time, start Remote Desktop Connection, click Show Options, click Open, and then double-click the stored file.

More simply, select it from the Jump List for Remote Desktop Connection (on the taskbar or Start menu), or double-click the stored file in File Explorer.

Troubleshooting network problems

Network connectivity problems can be a source of great frustration.

Fortunately, Windows 10 includes several tools and wizards that can help you identify and solve problems.

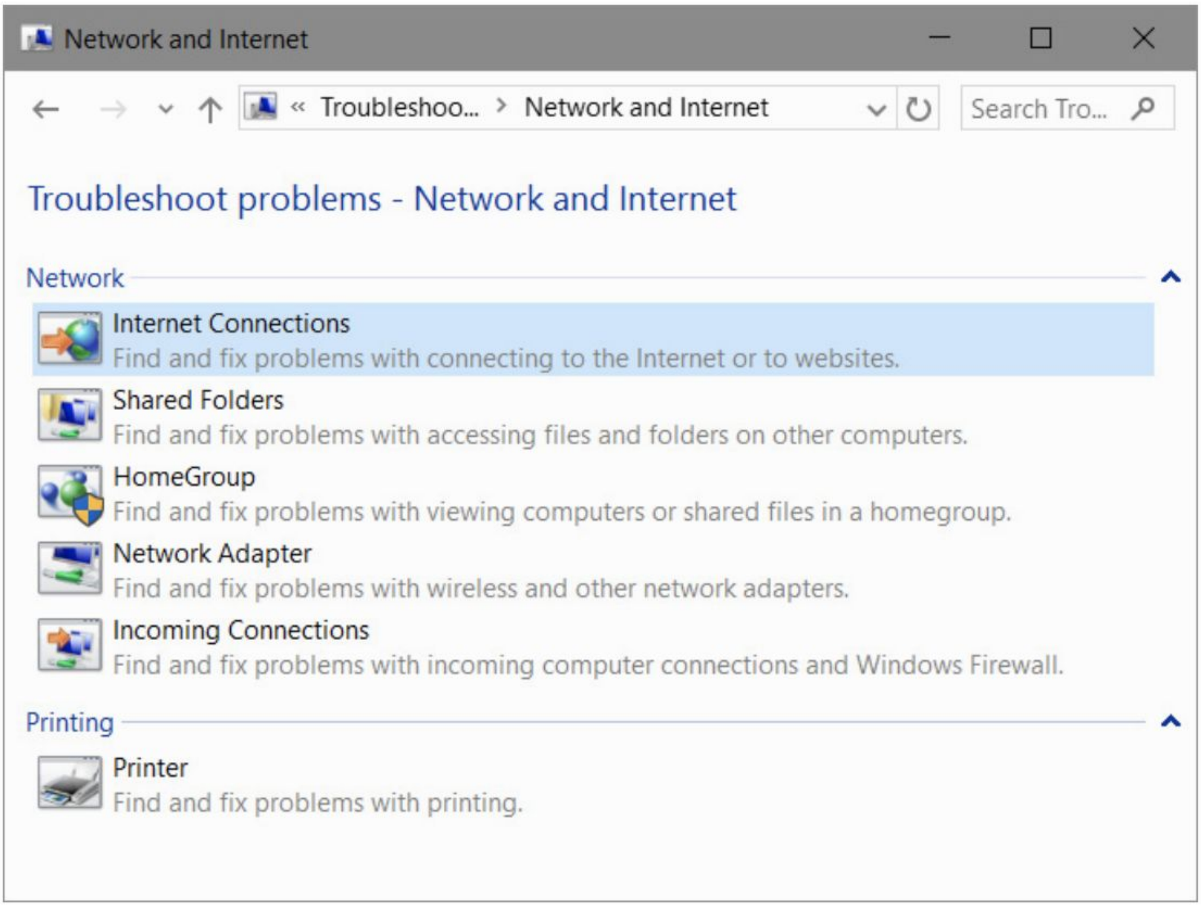
Even better, Windows has built-in network diagnostic capabilities, so in many cases, if there is a problem with your network connection, Windows knows about it before you do, displays a message, and often solves the problem.

When a network-dependent activity (for example, browsing to a website) fails, Windows works to address the most common network-related issues, such as problems with file sharing, website access, newly installed network hardware, connecting to a wireless network, and using a third-party firewall.

If you encounter network problems that don't trigger an automatic response from Windows, you should first try to detect and resolve the problem with one of the built-in troubleshooters.

Open Settings > Network & Internet > Network Troubleshooter to fix an issue.

If the options shown in that troubleshooter don't address your problem, go to Settings > Network & Internet > Network And Sharing Center > Troubleshoot Problems to display the choices shown in the following figure.



Troubleshoot problems - Network and Internet

Network

Internet Connections
Find and fix problems with connecting to the Internet or to websites.

Shared Folders
Find and fix problems with accessing files and folders on other computers.

HomeGroup
Find and fix problems with viewing computers or shared files in a homegroup.

Network Adapter
Find and fix problems with wireless and other network adapters.

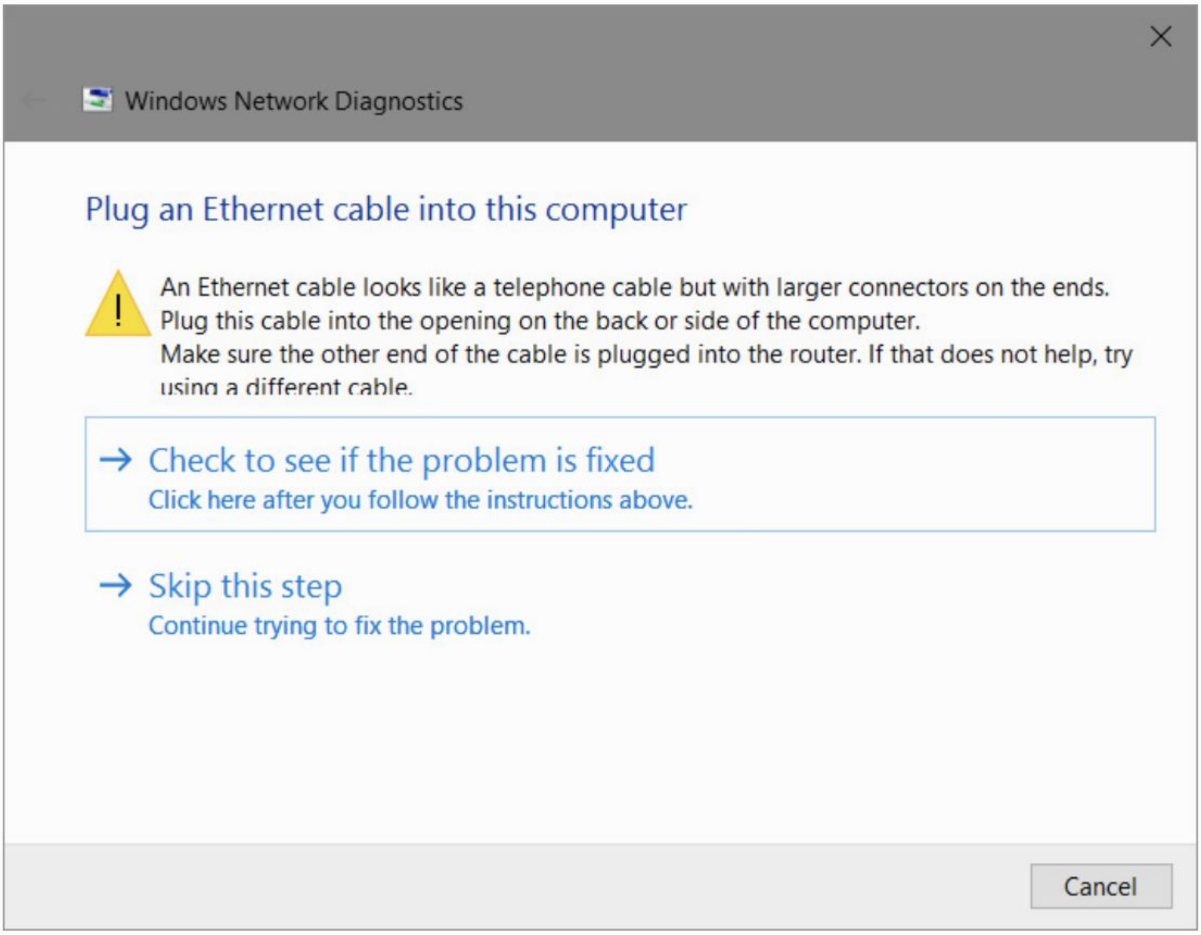
Incoming Connections
Find and fix problems with incoming computer connections and Windows Firewall.

Printing

Printer
Find and fix problems with printing.

Each of the troubleshooting wizards performs several diagnostic tests, corrects some conditions, suggests actions you can take, and ultimately displays a report that explains the wizard's findings.

Sometimes, the problem is as simple as a loose connection:



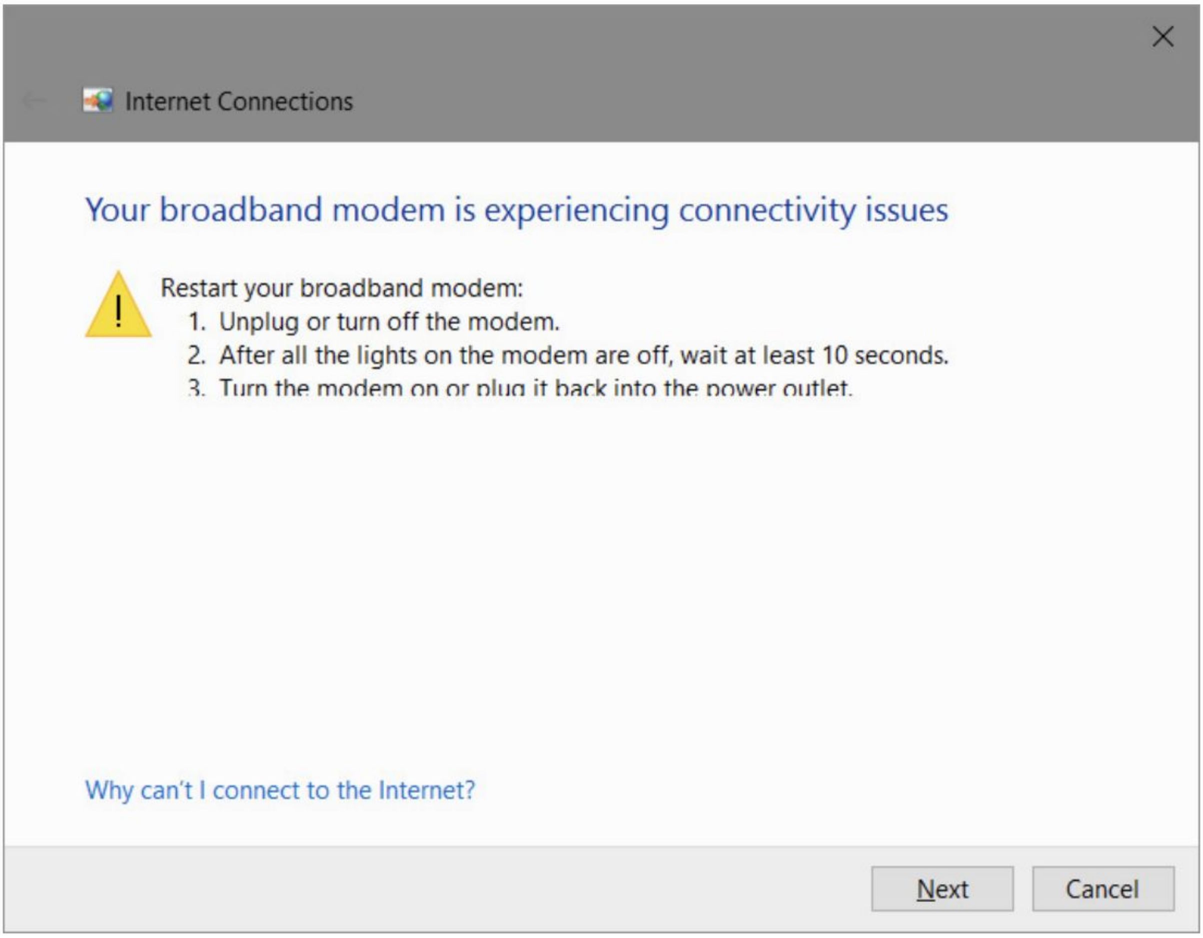
Plug an Ethernet cable into this computer

An Ethernet cable looks like a telephone cable but with larger connectors on the ends. Plug this cable into the opening on the back or side of the computer.
Make sure the other end of the cable is plugged into the router. If that does not help, try using a different cable.

→ Check to see if the problem is fixed
Click here after you follow the instructions above.

→ Skip this step
Continue trying to fix the problem.

Other situations might point to problems outside your network:



Your broadband modem is experiencing connectivity issues

Restart your broadband modem:

1. Unplug or turn off the modem.
2. After all the lights on the modem are off, wait at least 10 seconds.
3. Turn the modem on or plug it back into the power outlet.

Why can't I connect to the Internet?

If the diagnostic capabilities leave you at a dead end, you'll find that restarting the affected network hardware often resolves the problem, because the hardware is forced to rediscover the network. Here's a good general troubleshooting procedure:

1. Isolate the problem. Does it affect all computers on your network, a subset of your network, or only one computer?
2. If it affects all computers, try restarting the internet device (that is, the cable or DSL modem). If the device doesn't have a power switch, unplug it for a few moments and plug it back in.
3. If the problem affects a group of computers, try restarting the router to which those computers are connected.
4. If the problem affects only a single computer, try repairing the network connection for that computer. In Network And Sharing Center, click Change Adapter Settings. Alternatively, open Settings > Network & Internet > Change Adapter Options. Then, in Network Connections, select the connection and click Diagnose This Connection. If the troubleshooter doesn't resolve the problem, select the connection and click Disable This Network Device; then click Enable This Network Device, which causes Windows to reinitialize it.

If all else fails, open Settings > Network & Internet > Network Reset.

Network Reset removes all your network adapters, reinstalls them, sets other networking components to their default settings, and restarts your computer.

Troubleshooting HomeGroup problems

The HomeGroup troubleshooting wizard provides a good example of how these troubleshooters work.

If you're having problems seeing shared resources in a homegroup and you didn't have the benefit of the troubleshooter's assistance, you'd need to check the following settings, among others:

- The network location profile must be set to Private.
- In Windows Firewall With Advanced Security, you need to ensure the following groups of rules are enabled on private networks:
  1. Core Networking.
  2. Network Discovery.
  3. HomeGroup.
  4. File/Printer Sharing.
  5. Windows Media Player.
  6. Windows Media Player Network Sharing.
- The following services must be configured so that they can run:
  1. HomeGroup Listener.
  2. HomeGroup Provider.
  3. Function Discovery Provider Host.
  4. Function Discovery Resource Publication.
  5. Peer Name Resolution Protocol.
  6. Peer Networking Grouping.
  7. Peer Networking Identity Manager.

Running the HomeGroup troubleshooter—which you can launch from HomeGroup or by right-clicking HomeGroup in File Explorer as well as from the list of troubleshooters—checks each of these items and more.

When you get to the wizard's last window, you can click View Detailed Information to see a troubleshooting report that lists the potential problems that the wizard attempted to identify and fix.

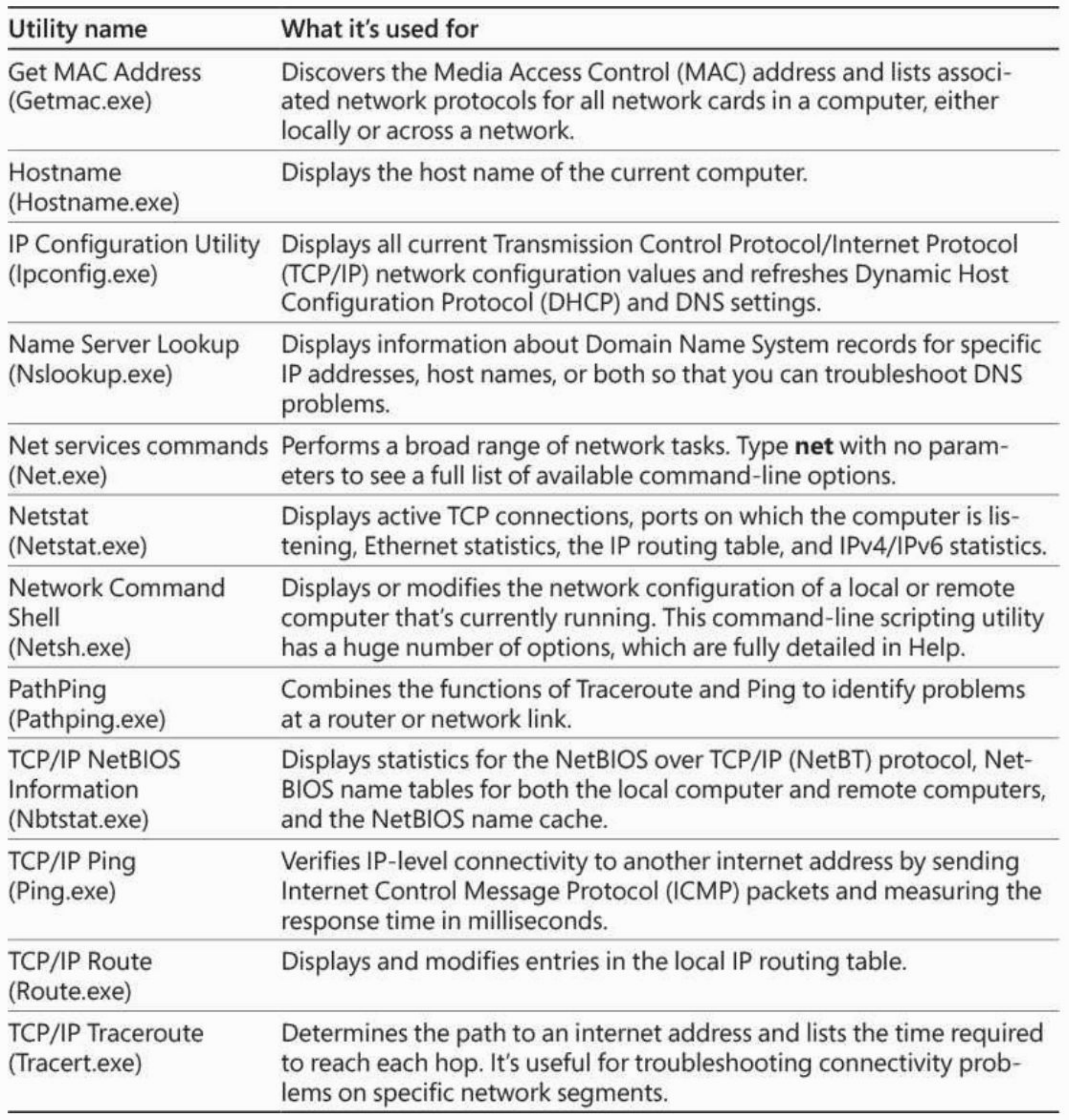
Network troubleshooting tools

When the troubleshooters don't solve the problem, it might be time to dig deeper into the Windows toolbox.

Windows contains an assortment of utilities you can use to diagnose, monitor, and repair network connections.

The next table lists the more useful networking-related command-line utilities and summarizes how you can use them.

To learn more about each utility, including its proper syntax, open a Command Prompt window and type the executable name followed by /?.



Utility name	What it's used for
Get MAC Address (Getmac.exe)	Discovers the Media Access Control (MAC) address and lists associated network protocols for all network cards in a computer, either locally or across a network.
Hostname (Hostname.exe)	Displays the host name of the current computer.
IP Configuration Utility (Ipconfig.exe)	Displays all current Transmission Control Protocol/Internet Protocol (TCP/IP) network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and DNS settings.
Name Server Lookup (Nslookup.exe)	Displays information about Domain Name System records for specific IP addresses, host names, or both so that you can troubleshoot DNS problems.
Net services commands (Net.exe)	Performs a broad range of network tasks. Type **net** with no parameters to see a full list of available command-line options.
Netstat (Netstat.exe)	Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, and IPv4/IPv6 statistics.
Network Command Shell (Netsh.exe)	Displays or modifies the network configuration of a local or remote computer that's currently running. This command-line scripting utility has a huge number of options, which are fully detailed in Help.
PathPing (Pathping.exe)	Combines the functions of Traceroute and Ping to identify problems at a router or network link.
TCP/IP NetBIOS Information (Nbtstat.exe)	Displays statistics for the NetBIOS over TCP/IP (NetBT) protocol, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache.
TCP/IP Ping (Ping.exe)	Verifies IP-level connectivity to another internet address by sending Internet Control Message Protocol (ICMP) packets and measuring the response time in milliseconds.
TCP/IP Route (Route.exe)	Displays and modifies entries in the local IP routing table.
TCP/IP Traceroute (Tracert.exe)	Determines the path to an internet address and lists the time required to reach each hop. It's useful for troubleshooting connectivity problems on specific network segments.

Troubleshooting TCP/IP problems

Transmission Control Protocol/Internet Protocol (TCP/IP) is the default communications protocol of the internet; in Windows 10, it's installed and configured automatically and cannot be removed.

Most of the time, your TCP/IP connection should just work, without requiring any manual configuration.

When you encounter problems with TCP/IP-based networks, such as an inability to connect with other computers on the same network or difficulty connecting to external websites, the problems might be TCP/IP related.

You'll need at least a basic understanding of how this protocol works before you can figure out which tool to use to uncover the root of the problem.

Setting IP addresses

Networks that use the TCP/IP protocol rely on IP addresses to route packets of data from point to point.

On a TCP/IP network, every computer has a unique IP address for each protocol (that is, TCP/IPv4 and TCP/IPv6) in use on each network adapter.

An IPv4 address consists of four 8-bit numbers (each one represented in decimal format by a number from 0 through 255) separated by periods.

An IPv6 address consists of eight 16-bit numbers (each one represented in hexadecimal format) separated by colons.

In addition to the IP address, each computer's TCP/IP configuration has the following additional settings:

- A subnet mask, which tells the network how to distinguish between IP addresses that are part of the same network and those that belong to other networks.
- A default gateway, which is a computer that routes packets intended for addresses outside the local network.
- One or more Domain Name System (DNS) servers, which are computers that translate domain names (such as www.microsoft.com) into IP addresses.

Windows provides several methods for assigning IP addresses to networked computers:

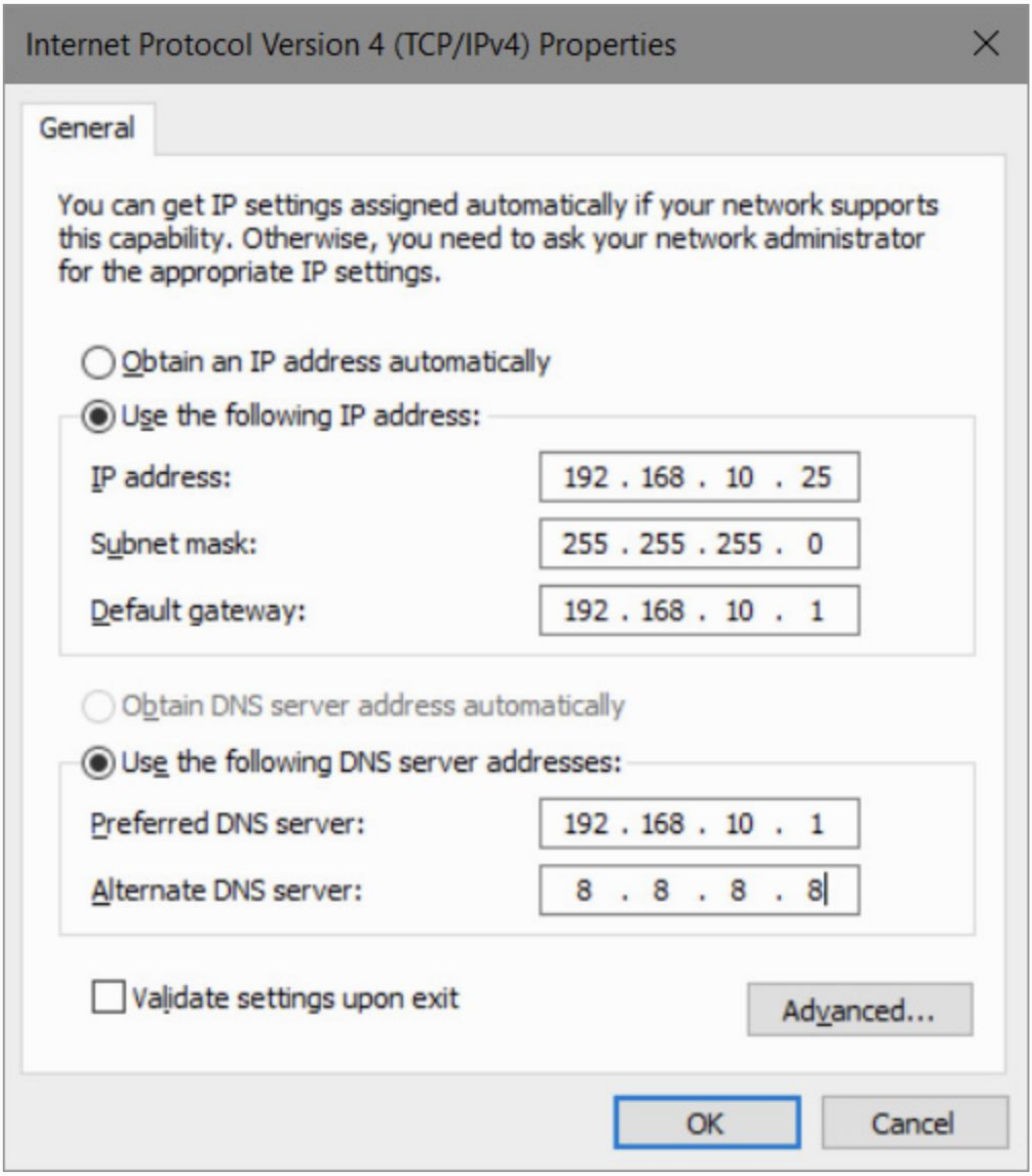
- Dynamic Host Configuration Protocol (DHCP). This is the default configuration for Windows 10. A DHCP server maintains a pool of IP addresses for use by network devices. When you connect to a network, the DHCP server assigns an IP address from this pool and sets subnet masks and other configuration details. Many corporate networks use DHCP to avoid the hassle of managing fixed addresses for constantly changing resources; all versions of Windows Server include this capability. Most routers and residential gateways also incorporate DHCP servers that automatically configure computers connected to those devices.

- Automatic Private IP Addressing (APIPA). When no DHCP server is available, Windows automatically assigns an IP address in a specific private IP range. If all computers on a subnet are using APIPA addresses, they can communicate with one another without requiring any additional configuration. APIPA was introduced with Windows 98 and works the same in all versions of Windows released since that time.
- Static IP Addressing. By entering an IP address, subnet mask, and other TCP/IP details in a dialog box, you can manually configure a Windows workstation so that its address is always the same. This method takes more time and can cause some configuration headaches, but it allows a high degree of control over network addresses. Static IP addresses are useful if you plan to set up a web server, a mail server, a virtual private network (VPN) gateway, or any other computer that needs to be accessible from across the internet. Even inside a local network, behind a router or firewall, static IP addresses can be useful. For instance, you might want to configure the router so that packets entering your network on a specific port get forwarded to a specific computer. If you use DHCP to assign addresses within the local network, you can't predict what the address of that computer will be on any given day. But by assigning that computer a static IP address that's within the range of addresses assigned by the DHCP server, you can ensure the computer always has the same address and is thus always reachable.
- Alternate IP Configuration. Use this feature to specify multiple IPv4 addresses for a single network connection (although only one address can be used at a time). This feature is most useful with portable computers that regularly connect to different networks. You can configure the connection to automatically acquire an IP address from an available DHCP server, and you can then assign a static backup address for use if the first configuration isn't successful.

To set a static IP address, follow these steps:

1. In the Network Connections folder, select the connection whose settings you want to change. On the command bar, click Change Settings Of This Connection. Alternatively, right-click the icon and choose Properties.
2. In the list of installed network items, select Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6), and then click Properties.
3. In the Internet Protocol (TCP/IP) Properties dialog box, select Use The Following IP Address and fill in the blanks. You must supply an IP address, a subnet mask (for IPv6, the length of the subnet prefix, which is usually 64 bits), and a default gateway.

4. Select Use The Following DNS Server Addresses, and then fill in the numeric IP addresses for one or more DNS servers as well. The next picture shows the dialog box with all fields filled in.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 10 . 25

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 10 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 10 . 1

Alternate DNS server: 8 . 8 . 8 . 8

□ Validate settings upon exit

5. Click OK to save your changes.

Public and private IP addresses

Any computer that's directly connected to the internet needs a public IP address—one that can be reached by other computers on the internet—so that information you request (webpages and email, for instance) can be routed back to your computer properly.

When you connect to an internet service provider, you're assigned a public IP address from a block of addresses registered to that ISP.

If you use a dial-up connection, your ISP probably assigns a different IP address to your computer (drawn from its pool of available addresses) each time you connect.

If you have a persistent connection to your ISP via a DSL or cable modem, your IP address might be permanent—or semipermanent if you turn off your computer when you leave your home or office to travel and your assigned IP address is changed when you reconnect on your return.

On a home or small office network, you don't need to have a public IP address for each computer on the network.

In fact, configuring a network with multiple public addresses can increase security risks and often requires an extra fee from your ISP.

A safer, less costly solution is to assign a single public IP address to a router or residential gateway (or a computer that performs that function).

All other computers on the network connect to the internet through that single address.

Each of the computers on the local network has a private IP address that's not directly reachable from the outside world.

To communicate with the internet, the router on the edge of the network uses a technology called Network Address Translation (NAT) to pass packets back and forth between the single public IP address and the multiple private IP addresses on the network.

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IPv4 address space for use on private networks that are not directly connected to the internet:

- 10.0.0.0–10.255.255.255
- 172.16.0.0–172.31.255.255
- 192.168.0.0–192.168.255.255

In addition, the Automatic Private IP Addressing feature in all post-1998 Windows versions uses private IP addresses in the range 169.254.0.0 through 169.254.255.255.

Routers and residential gateways that use NAT almost always assign addresses from these private ranges.

Linksys routers, for instance, typically assign addresses starting with 192.168.1.x.

If you’re setting up a small business or a home network that will not be connected to the internet, or that will be connected through a single proxy server, you can freely use these addresses without concern for conflicts.

Just make sure that all the addresses on the network are in the same subnet.

Checking for connection problems

Any time your network refuses to send and receive data properly, your first troubleshooting step should be to check for problems with the physical connection between the local computer and the rest of the network.

Assuming your network connection uses the TCP/IP protocol, the first tool to reach for is the Ping utility.

When you use the Ping command with no parameters, Windows sends four echo datagrams—small Internet Control Message Protocol (ICMP) packets—to the address you specify.

If the machine at the other end of the connection replies, you know that the network connection between the two points is alive.

To use the Ping command, open a Command Prompt window (Cmd.exe) and type the command ping target_name (where target_name is an IP address or the name of another host machine).

The return output looks something like this:

```
C:\>ping www.example.com

Pinging www.example.com [93.184.216.34] with 32 bytes of data:

Reply from 93.184.216.34: bytes=32 time=54ms TTL=51

Reply from 93.184.216.34: bytes=32 time=40ms TTL=51

Reply from 93.184.216.34: bytes=32 time=41ms TTL=51

Reply from 93.184.216.34: bytes=32 time=54ms TTL=51

Ping statistics for 93.184.216.34:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 40ms, Maximum = 54ms, Average = 47ms
```

If all the packets you send come back and the time values are roughly equal, your TCP/IP connection is fine and you can focus your troubleshooting efforts elsewhere.

If some packets time out, a “Request timed out” message appears, indicating your network connection is working but one or more hops between your computer and the target machine are experiencing problems.

In that case, repeat the Ping test using the –n switch to send a larger number of packets; ping –n 30 192.168.1.1, for example, sends 30 packets to the computer or router at 192.168.1.1.

A high rate of timeouts, also known as packet loss, usually means the problems are elsewhere on the network and not on the local machine.

If every one of your packets returns with the message “Request timed out,” the problem might be the TCP/IP connection on your computer or a glitch with another computer on that network.

To narrow down the problem, follow these steps, in order, stopping at any point where you encounter an error:

1. Ping your own machine by using any of the following commands:

```
ping ::1

ping 127.0.0.1

ping localhost
```

These are standard addresses. The first line is the IPv6 address for your own computer; the second line is the IPv4 address; the third line shows the standard host name. If your local network components are configured correctly, each of these three commands should allow the PC on which the command is run to talk to itself. If you receive an error, TCP/IP is not configured properly on your system.

2. Ping your computer’s IP address.

3. Ping the IP address of another computer on your network.

4. Ping the IP address of your router or the default gateway on your network.

5. Ping the address of each DNS server on your network.

6. Ping a known host outside your network. Well-known, high-traffic websites are ideal for this step, assuming that they respond to ICMP packets.

7. Use the PathPing command to contact the same host you specified in step 6. This command combines the functionality of the Ping command with the Traceroute utility to identify intermediate destinations on the internet between your computer and the specified host or server.

In some cases, pinging an external website results in a string of “Request timed out” messages, even when you have no trouble reaching those sites.

Don’t be misled.

Some popular sites block all ICMP traffic, including Ping packets, as a routine security measure.

Some routers and residential gateways are also configured to block certain types of ICMP traffic.

Try pinging several sites before concluding that your internet connection is broken.

If either of the two final steps in this process fails, your problem might be caused by DNS problems.

To eliminate this possibility, ping the numeric IP address of a computer outside your network instead.

Of course, if you're having DNS problems, you might have a hard time finding an IP address to ping!

If you can reach a website by using its IP address but not by using its name, DNS problems are indicated.

If you suspect that there's a problem on the internet between your computer and a distant host or server, use the Traceroute utility (Tracert.exe) to pinpoint the problem.

Like the Ping command, this utility works from a command line.

You specify the target (a host name or IP address) by using the syntax **tracert target_name**, and the utility sends out a series of packets, measuring the time it takes to reach each hop along the route.

Timeouts or unusually slow performance indicate a connectivity problem.

If the response time from your network to the first hop is much higher than the other hops, you might have a problem with the connection to your internet service provider; in that case, a call to your ISP's support line is in order.

Problems farther along in the traceroute might indicate congestion or hardware problems in distant parts of the internet that are out of your ISP's hands.

These symptoms might disappear when you check another URL that follows a different path through the internet.

If your testing produces inconsistent results, rule out the possibility that a firewall program or NAT device (such as a router or residential gateway) is to blame.

If you're using Windows Firewall or a third-party firewall program, disable it temporarily.

Try bypassing your router and connecting directly to a broadband connection such as a DSL or cable modem.

Use this configuration only for testing and only very briefly because it exposes your computer to various attacks.

If the Ping test works with the firewall or NAT device out of the picture, you can rule out network problems and conclude that the firewall software or router is misconfigured.

After you complete your testing, be sure to enable the firewall and router again!

Diagnosing IP address problems

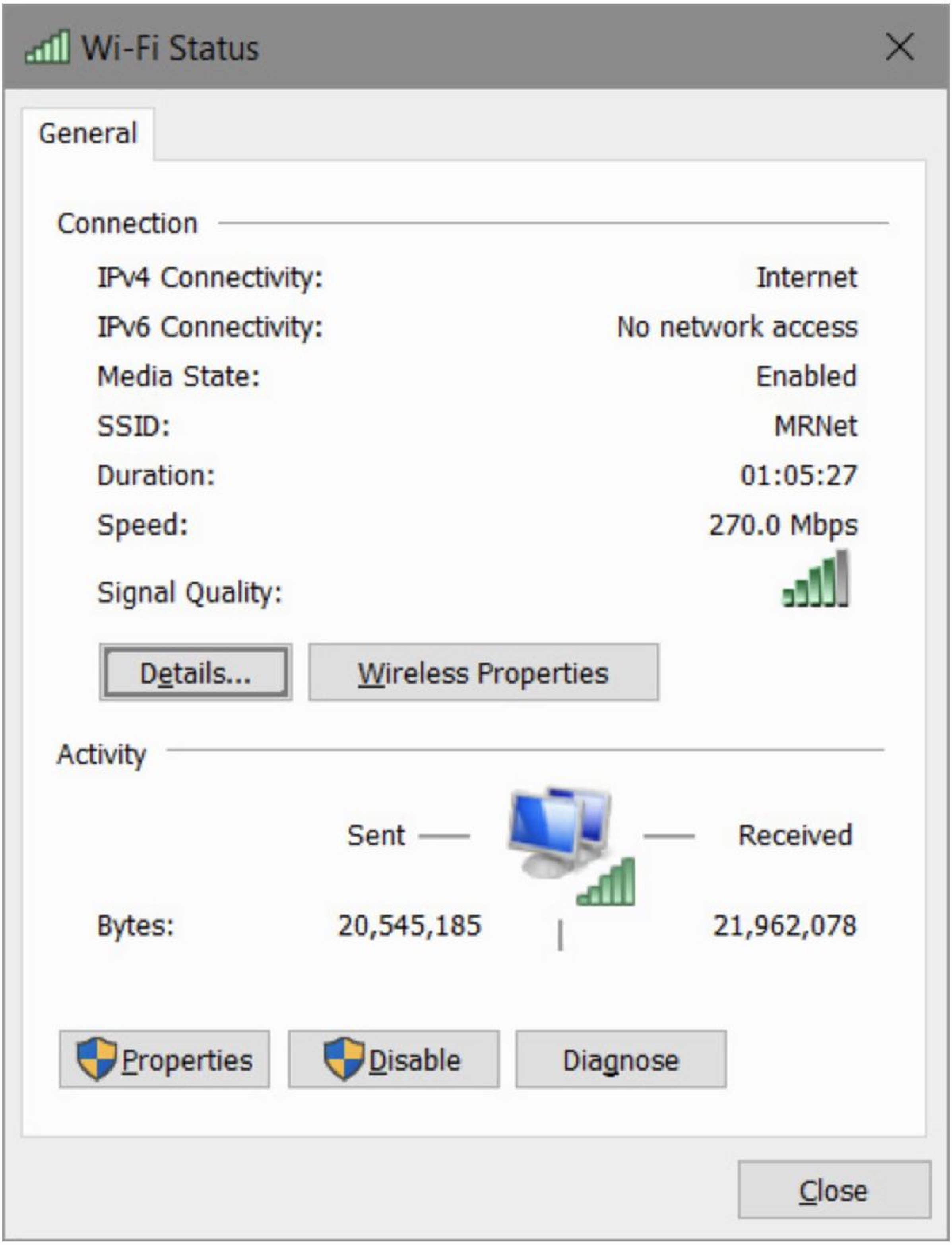
On most networks, IP addresses are assigned automatically by Dynamic Host Configuration Protocol (DHCP) servers; in some cases, you might need (or prefer) to use static IP addresses, which are fixed numeric addresses.

Problems with DHCP servers or clients can cause network connections to stop working, as can incorrectly assigned static IP addresses.

To see details of your current IP configuration, follow these steps:

1. Open Settings > Network & Internet > Change Adapter Options.

2. Double-click the icon for the connection about which you want more information. Alternatively, you can select the icon and click View Status Of This Connection on the command bar.



Wi-Fi Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No network access

Media State: Enabled

SSID: MRNet

Duration: 01:05:27

Speed: 270.0 Mbps

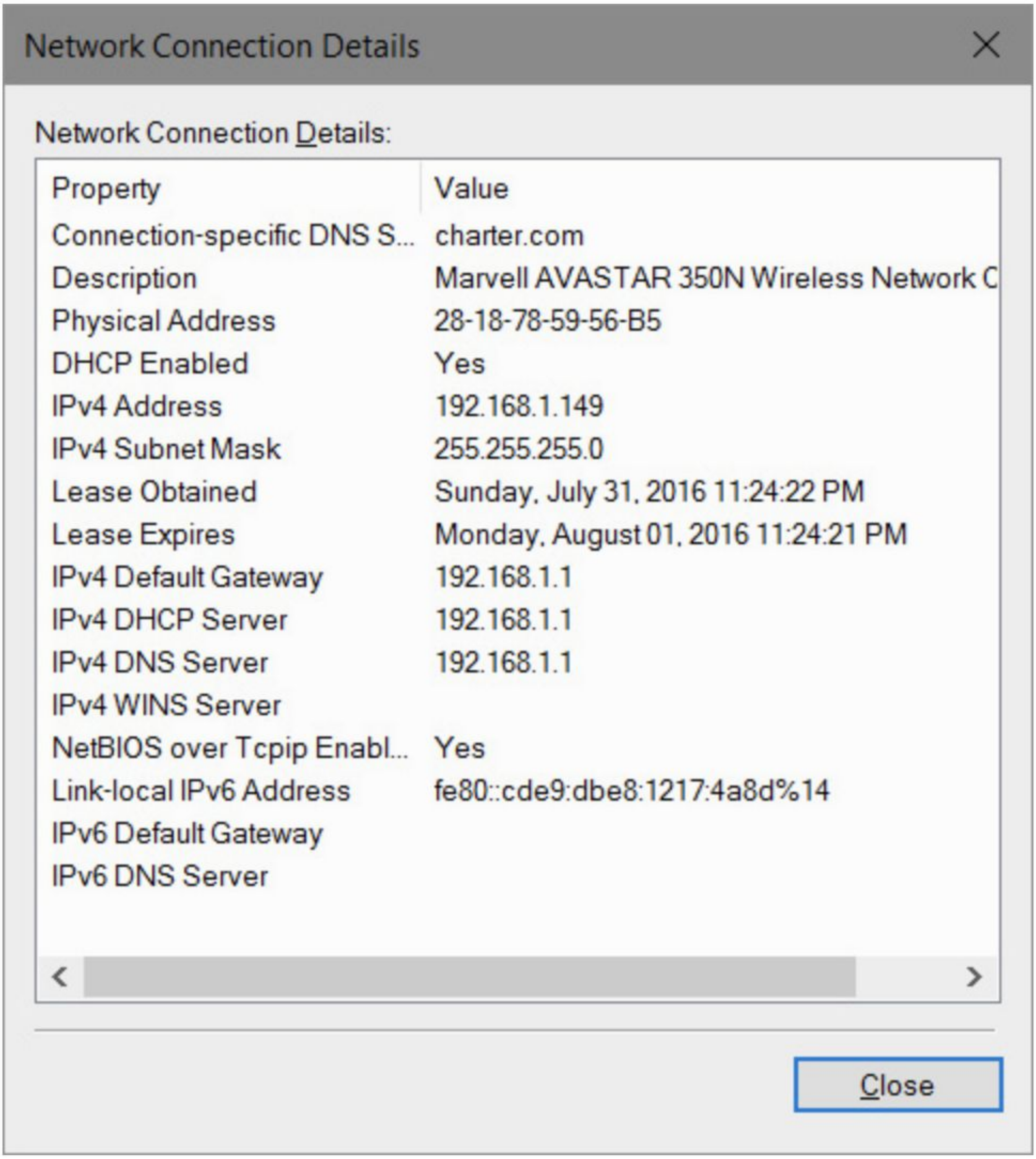
Signal Quality:

Activity

Sent — — Received

Bytes: 20,545,185 21,962,078

3. Click Details to see the currently assigned IP address, subnet mask, and default gateway for this connection. (If you have IPv4 and IPv6 connectivity, the Network Connection Details dialog box shows information for both.) In the following example, you can tell that the IP address was automatically assigned by the DHCP server in a router; details indicate that DHCP is enabled and the DHCP server address matches that of the router:



Network Connection Details:

Property	Value
Connection-specific DNS S...	charter.com
Description	Marvell AVASTAR 350N Wireless Network C
Physical Address	28-18-78-59-56-B5
DHCP Enabled	Yes
IPv4 Address	192.168.1.149
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Sunday, July 31, 2016 11:24:22 PM
Lease Expires	Monday, August 01, 2016 11:24:21 PM
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Server	192.168.1.1
IPv4 WINS Server	
NetBIOS over Tcpip Enabl...	Yes
Link-local IPv6 Address	fe80::cde9:dbe8:1217:4a8d%14
IPv6 Default Gateway	
IPv6 DNS Server	

You can also get useful details of your IP configuration by using the IP Configuration utility, Ipconfig.exe, in a Command Prompt window.

Used without any parameters, typing ipconfig at a command prompt displays the DNS suffix; IPv6 address, IPv4 address, or both; subnet mask; and default gateway for each network connection.

To see exhaustive details about every available network connection, type **ipconfig /all**.

The actual IP address you see might help you solve connection problems:

- If the address is in the format 169.254.x.y, your computer is using Automatic Private IP Addressing (APIPA). This means your computer's DHCP client was unable to reach a DHCP server to be assigned an IP address. Check the connection to your network.

- If the address is in one of the blocks of IP addresses reserved for use on private networks, make sure that a router or residential gateway is routing your internet requests to a properly configured public IP address.
- If the address of your computer appears as 0.0.0.0, the network is either disconnected or the static IP address for the connection duplicates an address that already exists on the network.
- Make sure you're using the correct subnet mask for computers on your local network. Compare IP settings on the machine that's having problems with those on other computers on the network. The default gateway and subnet mask should be identical for all network computers. The first one, two, or three sets of numbers in the IP address for each machine should also be identical, depending on the subnet mask. A subnet mask of 255.255.255.0 means the first three IP address numbers of computers on your network must be identical—192.168.0.83 and 192.168.0.223, for instance, can communicate on a network using this subnet mask, but 192.168.1.101 will not be recognized as belonging to the network. The gateway machine must also be a member of the same subnet. If you use a router, switch, or residential gateway for internet access, the local address on that device must be part of the same subnet as the machines on your network.

Repairing your TCP/IP configuration

If you suspect a problem with your TCP/IP configuration, try either of the following repair options:

- Use the automated repair option. Right-click the connection icon in Network Connections and click Diagnose.
- Release and renew your IP address. Use the **"ipconfig /release"** command to let go of the DHCP-assigned IPv4 address. Then use **"ipconfig /renew"** to obtain a new IP address from the DHCP server. To renew an IPv6 address, use **"ipconfig /release6"** and **"ipconfig /renew6"**.

Translate names to IP addresses and vice versa

The **Nslookup** command is a buried treasure in Windows.

Use this command-line utility to quickly convert a fully qualified domain name to its IP address.

You can tack on a host name to the end of the command line to identify a single address; for instance, you can type **"nslookup ftp.microsoft.com**" to look up the IP address of Microsoft's File Transfer Protocol (FTP) server.

Or type **"nslookup"** to switch into interactive mode.

From this prompt, you can enter any domain name to find its IP address.

If you need more sophisticated lookup tools, you can find them with the help of any search engine.

A good starting point is DNSstuff http://dnsstuff.com/tools , which offers an impressive collection of online tools for looking up domains, IP addresses, and host names.

The site also offers form-based utilities that can translate obfuscated URLs and dotted IP addresses, both of which are widely used by spammers to cover their online tracks.

Resolving DNS issues

The Domain Name System (DNS) is a crucial part of the internet.

DNS servers translate host names (www.microsoft.com, for instance) into numeric IP addresses so that packets can be routed properly over the internet.

If you can use the Ping command to reach a numeric address outside your network but are unable to browse websites by name, the problem is almost certainly related to your DNS configuration.

Here are some questions to ask when you suspect DNS problems:

- Do your TCP/IP settings point to the right DNS servers? Inspect the details of your IP configuration, and compare the DNS servers listed there with those recommended by your internet service provider. You might need to call your ISP to get these details.
- Is your ISP experiencing DNS problems? A misconfigured DNS server (or one that's offline) can wreak havoc with your attempts to use the internet. Try pinging each DNS server to see whether it's available. If your ISP has multiple DNS servers and you encounter problems accessing one server, remove that server from your TCP/IP configuration temporarily and use another one instead.
- Have you installed any "internet accelerator" utilities? Many such programs work by editing the Hosts file on your computer to match IP addresses and host (server) names. When Windows finds a host name in the Hosts file, it uses the IP address listed there and doesn't send the request to a DNS server. If the owner of the server changes its DNS records to point to a new IP address, your Hosts file will lead you to the wrong location.

Temporary DNS problems can also be caused by the DNS cache, which Windows maintains for performance reasons.

If you suddenly have trouble reaching a specific site on the internet and you're convinced there's nothing wrong with the site, type this command to clear the DNS cache: **"ipconfig /flushdns"**.

A more thorough solution is offered by **"ipconfig /registerdns"**, which renews all DHCP leases and reregisters all DNS names.

- Exercises - 1. 4. 3. Advanced networking -

Open the following Google Document that you have created in a previous sub-unit:

"1. 4. Windows 10 for experts and IT pros - Apellidos, Nombre"

being "Apellidos, Nombre" your Last Name and Name.

Inside this Google Document you are going to copy and answer all the "Exercises" of this sub-unit:

1. In your computer and with your Windows user, go to C:\Users\Public and create a new folder named “public-folder”. Check if you can access to that “public-folder” from another computer and with another Windows user.
2. In your computer and with your Windows user, go to C:\ and create a new folder named “shared-folder-1”. Create a new local user named "Luis". Share the folder “shared-folder-1” with the new local user "Luis". Copy the shared link. Check if you can access to that “shared-folder-1” from another computer and with another Windows user. Also check if you can access to that “shared-folder-1” from another computer and with the user "Luis". Note that the user "Luis" is stored in your own computer, not in another computer.
3. Check the NTFS permissions settings of the folders that you have created in the previous exercises.
4. Open File Explorer and click on “Network” on the left pane. Check the computers that you can see on your network. Check for shared resources on those computers and try to access some of those shared resources.
5. Map a network folder of one of your colleagues to a drive letter of your computer.
6. Enable Remote Desktop on your computer and on your friend’s computer. Download the “Remote Desktop” app from the Windows Store. Set up a new remote connection with the PC of your friend. Connect to that new remote connection.
7. Do the same tasks of the last exercise but using the “Remote Desktop Connection” program.
8. What do the following commands make? getmac, hostname, ipconfig /all, nslookup, netstat, ping “IP or Domain”, tracert “IP or Domain”, ipconfig /release, ipconfig /renew, ipconfig /flushdns, ipconfig /registerdns.
9. Open a Command Prompt and execute the commands of the previous exercise.