Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**Module**

**11**

**Managing Enterprise Clients**

* [Chapter Introduction](javascript://)
* **11-1**[Troubleshooting and Managing Enterprise Clients](javascript://)
  + **11-1a**[Remote Desktop](javascript://)
  + **11-1b**[Remote Assistance](javascript://)
  + **11-1c**[Quick Assist](javascript://)
  + **11-1d**[MMC Snap-Ins](javascript://)
  + **11-1e**[Registry Editor](javascript://)
  + **11-1f**[Windows PowerShell Remoting](javascript://)
* **11-2**[Managing Profiles for Roaming Users](javascript://)
  + **11-2a**[Mapped Drive Letters](javascript://)
  + **11-2b**[Folder Redirection](javascript://)
  + **11-2c**[Credential Roaming](javascript://)
  + **11-2d**[User Experience Virtualization](javascript://)
  + **11-2e**[Profile Synchronization with Microsoft Account or Azure AD](javascript://)
* **11-3**[Using a VPN for Remote Access](javascript://)
  + **11-3a**[Configuring VPN Clients](javascript://)
  + **11-3b**[VPN Protocols](javascript://)
  + **11-3c**[Creating a VPN Connection](javascript://)
  + **11-3d**[Automated VPN Deployment](javascript://)
  + **11-3e**[Authentication Protocols](javascript://)
  + **11-3f**[Network Settings](javascript://)
  + **11-3g**[Always On VPN](javascript://)
  + **11-3h**[DirectAccess](javascript://)
* **11-4**[Synchronizing Data for Mobile Clients](javascript://)
  + **11-4a**[OneDrive](javascript://)
  + **11-4b**[Offline Files](javascript://)
  + **11-4c**[Work Folders](javascript://)
* **11-5**[Chapter Review](javascript://)
  + **11-5a**[Summary](javascript://)
  + **11-5b**[Key Terms](javascript://)
  + **11-5c**[Review Questions](javascript://)
  + **11-5d**[Case Projects](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

Chapter Introduction

After reading this module and completing the exercises, you will be able to:

* **1**Troubleshoot and manage enterprise clients
* **2**Manage profiles for roaming users
* **3**Configure clients for virtual private networks
* **4**Describe and configure data synchronization for mobile clients

When you manage clients in an enterprise environment, you need to consider the best ways to scale up your ability to provide support. Small challenges for a few people in a 100-user environment become big issues in an enterprise. In an enterprise, users are more likely to roam among computers, require remote access, and have mobile computers. You need to understand how these services are implemented for Windows 10.

In this module, you learn about methods for remotely managing Windows 10 computers so that you can quickly provide help to users without physically visiting them. You also learn how to centralize profile data to support users that don’t sign in to the same computer each day. For users outside the office, you learn about remote access by using a virtual private network (VPN), including the various protocols that can be used. Finally, you learn about data synchronization options that can be used by mobile computers to provide data access when they are not connected to a network.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# 11-1Troubleshooting and Managing Enterprise Clients

In smaller companies, you can manually go to each computer to perform troubleshooting when a problem arises. It takes you only a few minutes to go from your desk to where the problem is. In larger companies, desktop support staff need to work remotely from the computer where the problem is occurring.

The physical size of large companies makes it impractical to visit each computer to perform troubleshooting. Whether it’s just a physically large building or an organization with multiple physical locations, it takes a lot of time to visit each desktop computer. Desktop support staff are much more efficient when they can work from their own desk. The tools available for remote management are shown in [Table 11.1](javascript://).

**Table 11-1**

### Remote Management Tools

| **Tool** | **Description** |
| --- | --- |
| Remote Desktop | Enables you to remotely sign in to a computer and work with it just as if you were at the console. The main benefit of using Remote Desktop is that it gives you full access to the remote computer and its software; however, you are signed in as your user account and not as the user that needs help. So, if any of the problems are related to configuration information in the user profile, then Remote Desktop won’t help. Also, when you sign in by using Remote Desktop, the user at the console is disconnected. |
| Remote Assistance | Allows you to connect to the console of the remote computer where a user is signed in. The main benefit of remote assistance is that you can see what users are doing when they are experiencing issues. You can ask to remote control the session to perform troubleshooting. Because the remote computer is signed in as the user, you can repair problems caused by settings stored in the user profile. |
| Quick Assist | Allows you to connect to the console of the remote computer where a user is signed in. This is a replacement for Remote Assistance that is included only in Windows 10 and not previous versions of Windows. This tool is easy to use over an Internet connection without any firewall configuration. |
| Microsoft Management Console (MMC) snap-ins | Enables you to connect to a remote computer with an MMC snap-in to manage specific settings on the remote computer. Because MMC snap-ins, such as Event Viewer and Services, are the most common way to manage a local instance of Windows 10, using the same tool to manage remote systems is convenient. More commonly used MMC snap-ins can connect to remote systems. You need to allow remote management of systems to use an MMC snap-in remotely.  Connecting remotely with MMC snap-ins can be done while users are signed in and working. Users are not prompted to accept connections and do not see you performing any actions. |
| Registry Editor (regedit.exe) | Option that lets you connect to the registry of a remote computer and modify registry keys. This performs similarly to MMC snap-ins. When in Registry Editor, select a remote computer to connect to. Be aware that many registry changes don’t take effect until the computer, apps, or services are restarted.  Connecting remotely with Registry Editor can be done while users are signed in and working. Users are not prompted to accept connections and do not see you performing any actions. |
| Windows PowerShell remoting | Enables you to connect to a remote computer with a Windows PowerShell prompt. Then, when connected through PowerShell remoting, you can run Windows PowerShell cmdlets as if you were at a Windows PowerShell prompt on the console of the remote system. This is similar to a system such as Telnet where you remotely control a computer system through a text-based interface.  Connecting remotely with Windows PowerShell can be done while users are signed in and working. Users are not prompted to accept connections and do not see you performing any actions. |
| Group Policy | Option that allows you to configure multiple computers quickly and easily in a domain-based network. Group Policy is useful for standardizing computer configuration quickly. Group Policy is applied to computer objects in Active Directory. When a setting is configured by using Group Policy, users cannot change that setting. |

Enlarge Table

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-1aRemote Desktop

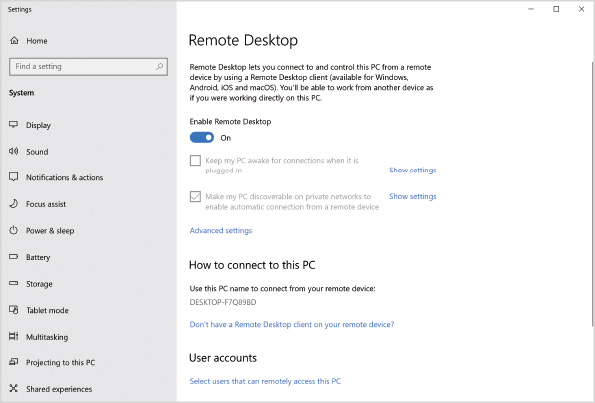
[**Remote Desktop**](javascript://) provides functionality that is similar to an RD Session host, but it does not require additional licensing or servers. It is often used by desktop support staff to connect to a computer running Windows 10 and run troubleshooting tools or perform configuration tasks. When you connect by using Remote Desktop, you sign in as yourself and see your own desktop, as well as the application you are running. You are not able to view what a user is seeing on the desktop. In fact, when you connect to a Windows 10 computer by using Remote Desktop, it disconnects a locally signed in user.

**Note 1**

When you use Remote Desktop to connect to a computer where a user is already signed in, the user is prompted whether to allow you access or not.

You can enable Remote Desktop on a computer running any edition of Windows 10 except Home edition. When Remote Desktop is enabled, as shown in [Figure 11-1](javascript://), local administrators and members of the local Remote Desktop Users group have permission to connect. By default, Remote Desktop Users contain no members. To give standard users access to connect, they must be members of this group.

**Figure 11-1Remote Desktop Settings**



Enlarge Image

Remote Desktop listens on TCP port 3389. When you enable Remote Desktop, Windows Firewall is automatically configured to allow connectivity on port 3389. It is possible to change the port used by Remote Desktop by editing the registry, but this is seldom required. If you change the port for Remote Desktop, you need to manually create a Windows Defender Firewall rule to allow it.

By default, Remote Desktop uses Network Level Authentication. When Network Level Authentication is enabled, Remote Desktop Connection obtains sign-in information from users before connecting to the remote computer. This prevents users from connecting until the connection is authenticated. If Network Level Authentication is not used, you can connect to a computer and see the sign-in screen before you authenticate. This is a security risk because that screen might display the last signed-in user. Also, if the RDP protocol or Remote Desktop contains a flaw, it could be exploited by an unauthenticated user.

**Activity 11-1**

### Enabling Remote Desktop

**Time Required:**5 minutes

**Objective:**Enable Remote Desktop for a computer

**Description:**You want to be able to connect to a Windows 10 computer remotely by using Remote Desktop to perform remote administration. In this activity, you enable Remote Desktop.

**Note 2**

This activity assumes you have access to the desktop of the domain controller that your Windows client is joined to.

1. 1

If necessary, start your Windows 10 computer and sign in as AD\Administrator.

1. 2

Click the **Start** button and then click **Settings**.

1. 3

In the Settings window, click **System**, in the System pane, scroll down if necessary, and select **Remote Desktop**.

1. 4

Click the Enable remote desktop toggle and then click **Confirm** in the Remote Desktop Settings dialog box.

1. 5

In the Settings window, read the information in the How to connect to this PC heading. Take note of the computer name.

1. 6

Click **Advanced settings** and read the information. Notice that Network Level Authentication is required and the Remote Desktop port is 3389.

1. 7

Close the Settings window.

1. 8

On your domain controller, sign in as AD\Administrator.

1. 9

Click the **Start** button, type **remote**, and then click **Remote Desktop Connection**.

1. 10

In the Remote Desktop Connection dialog box, in the Computer box, type the computer name you recorded in [Step 5](javascript://), and then click **Show Options**.

1. 11

Click the **Display** tab and read the options.

1. 12

Click the **Local Resource** tab and read the options.

1. 13

Click the **Experience** tab and read the options.

1. 14

Click the **Advanced** tab, read the options, and then click **Connect**.

1. 15

In the Windows Security window, type the password for AD\Administrator and then click **OK**. You are now connected to the Windows 10 desktop in Remote Desktop Connection.

1. 16

In the Remote Desktop Connection window, on the taskbar, click **Microsoft Edge**.

1. 17

Close the Remote Desktop Connection window and then click **OK** in the dialog box warning about disconnecting from the session.

1. 18

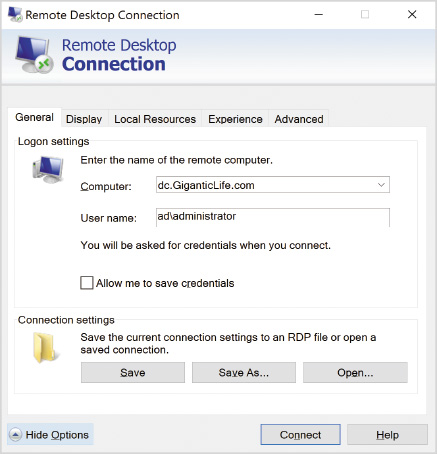
On your Windows 10 computer, sign in as AD\Administrator. Notice that Microsoft Edge remains open from your remote session.

1. 19

Exit Microsoft Edge.

**[Remote Desktop Connection](javascript://)**, shown in [Figure 11-2](javascript://), is the Remote Desktop Protocol (RDP) client that you use to connect to a remote desktop. You can configure many different settings in Remote Desktop Connection, and you might want these settings to be different when connecting to different computers. To simplify using different settings, you can save settings, including the remote computer name, in .rdp files. Then, you can double-click the .rdp file name to initiate the connection.

**Figure 11-2Remote Desktop Connection**



The Display tab in Remote Desktop Connection lets you select the screen resolution and color depth for the remote session. The larger the values are, the more data will be sent back and forth between the two computers. On slow connections, consider reducing the screen resolution and color depth. If you select Use all my monitors for the remote session, you can have a multimonitor connection to the remote computer.

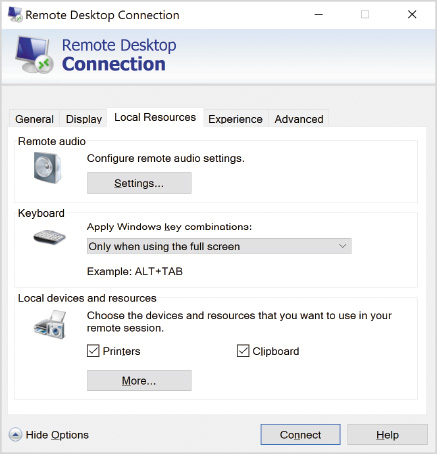
**Tip**

On slow network connections, consider reducing the screen resolution and color depth. A solid color desktop can also reduce data requirements.

The Local Resources tab in Remote Desktop Connection, shown in [Figure 11-3](javascript://), controls which resources in the local computer are available for the session. These settings provide better integration between the local and remote computers to provide a better experience. Some of the things you can configure are:

* Enable playback of sound from the remote computer on the local computer.
* Allow printers from the local computer to be used in the remote session.
* Allow copying of Clipboard data between the local and remote computers.
* Allow hard drives from the local computer to be accessed in the remote session.
* Allow smart cards on the local computer to be used in the remote session.

**Figure 11-3Remote Desktop Connection, Local Resources Tab**

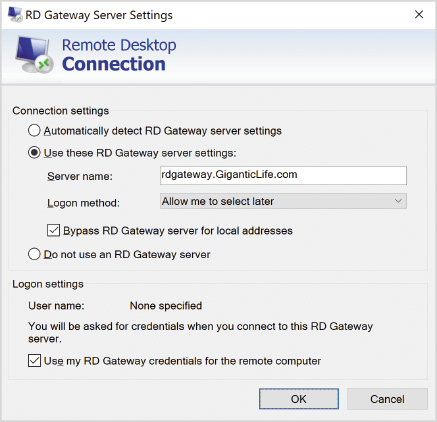


The Experience tab in Remote Desktop Connection allows you to enable and disable various display-related settings that can impact the amount of data sent between the local and remote computers. On slower network connections, you can disable some of these settings to reduce delays in seeing results after you click items or move them around. By default, Remote Desktop Connection detects the connection quality automatically and adjusts the features as necessary. Automatic configuration works well in most cases, but for very slow connections, you might find the experience better if you manually disable most of the features.

On the Advanced tab in Remote Desktop Connection, you can configure server authentication settings and Remote Desktop Gateway (RD Gateway) settings. The server authentication settings control how Remote Desktop Connection behaves when the certificate used by the server does not match the name you use when connecting. By default, a warning is displayed. To increase security, you can prevent mismatched names from being allowed, but this means that you will not be able to connect directly by IP address.

An RD Gateway server is used to secure access to Remote Desktop from public networks, such as the Internet. When Remote Desktop Connection is configured to use an RD Gateway, RDP traffic is tunneled in HTTPS packets to the RD Gateway server. The RD Gateway server sends the RDP packets on to the internal network. Effectively, this is like an SSL VPN that is specifically designed for Remote Desktop and RDS. [Figure 11-4](javascript://) shows the settings for RD Gateway in Remote Desktop Connection.

**Figure 11-4Remote Desktop Connection, RD Gateway Server Settings**



Most of the time, you will start Remote Desktop Connection from the Start button; however, you can start Remote Desktop Connection from a command prompt by running mstsc.exe. You can view all of the options available by running mstsc.exe /?. [Table 11.2](javascript://) lists some configuration options that are available at the command prompt but not in the graphical interface.

**Table 11-2**

### Mstsc.exe Options

| **Option** | **Description** |
| --- | --- |
| /admin | Connects to the console of a remote computer rather than an RDP session. This can be useful in some cases when you are troubleshooting and a typical RDP is not working properly. |
| /public | Prevents Remote Desktop Connection from saving information to the local computer. For example, credentials and the name of the remote computer are not cached for later use. |
| /restrictedAdmin | Prevents the remote computer from accessing your credentials. The session uses the local computer account for permissions instead, which might not allow you to access network resources. This is useful when a remote system may have been compromised. |
| /remoteGuard | Prevents the remote computer from accessing your credentials similarly to /restrictedAdmin. This mode, however, allows connectivity to network resources by routing requests back through Remote Desktop Connection. |
| /shadow | Allows you to connect to an existing session and view what another user is doing. |
| /control | Allows someone else to control your session if that person is viewing it with you. |
| /noConsentPrompt | Allows someone to shadow your session without prompting you for consent. |

**Activity 11-2**

### Customizing Settings for Remote Desktop Connection

**Time Required:**10 minutes

**Objective:**Customize settings for Remote Desktop Connection

**Description:**You want to create a set of customized settings for connecting to a specific remote desktop. In this activity, you configure settings in Remote Desktop Connection and save them as an .rdp file for later use.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, type **mstsc**, and then click **Remote Desktop Connection**.

1. 3

In the Remote Desktop Connection window, in the Computer box, type **w10-45.giganticlife.com** and then click **Show Options**.

1. 4

Click the **Display** tab and in the Display configuration area, select **1024 by 768 pixels**.

1. 5

Click the **Local Resources** tab and then clear the **Printers** check box.

1. 6

Click the **Experience** tab and then in the Choose your connection speed to optimize performance box, select **Low-speed broadband (256 kbps - 2 Mbps)**.

1. 7

Click the **Advanced** tab and then in the Connect from anywhere area, click **Settings**.

1. 8

In the RD Gateway Server Settings dialog box, click **Use these RD Gateway server settings**.

1. 9

In the Server name box, type **RD-Gateway.giganticlife.com** and then click OK.

1. 10

In Remote Desktop Connection, click the **General** tab and then click **Save As**.

1. 11

In the Save As dialog box, in the File name box, type **w10-45** and then click **Save**.

1. 12

Close the Remote Desktop Connection window.

Go to pg.

[**help**](javascript://)

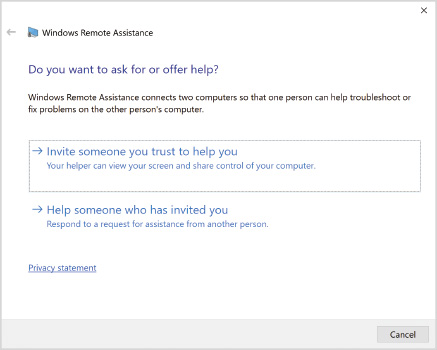
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-1bRemote Assistance

Remote Desktop allows you to connect to a remote computer for troubleshooting. For the best results when troubleshooting, however, it is often useful to have users show you the problem they are experiencing, which is not possible with Remote Desktop. You can use [**Remote Assistance**](javascript://), shown in [Figure 11-5](javascript://), to view what a user is doing and even take control to resolve the issue.

**Figure 11-5Windows Remote Assistance**

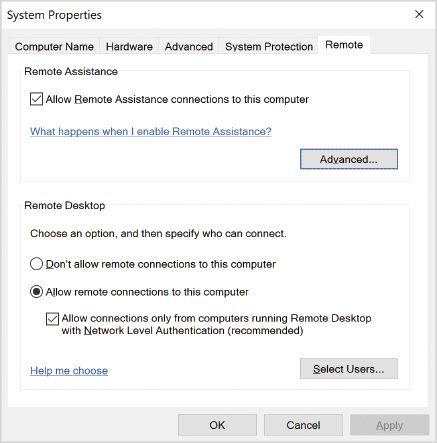


Remote Assistance can be initiated in the following ways:

* Invitation file—Users can create an invitation file that they send to a helper. When the helper opens the file, remote assistance starts. This method does not work over routers that perform Network Address Translation (NAT) because the IP address information in the invitation file is the internal IP address of the computer that is not accessible over the Internet.
* Easy Connect—When users select Easy Connect instead of an invitation, the user is provided with a password that needs to be sent to the helper. The helper enters that password to be connected. This type of connection works over the Internet and through NAT. Easy Connect tunnels IPv6 packets over IPv4 networks and relies on the Teredo Adapter Interface, which is not installed by default.
* Administrator initiated—As a helper, you can offer remote assistance to users if you know the IP address or computer name. After the connection to the computer is established, the user is prompted to allow the connection. This method is used on internal networks and not over the Internet.

After an invitation has been created or Easy Connect has been initiated, the user needs to leave Windows Remote Assistance open. If the Windows Remote Assistance window is closed, the helper cannot connect. On the remote system, you also need to have allowed Remote Assistance, as shown in [Figure 11-6](javascript://).

**Figure 11-6Allow Remote Assistance**



**Tip**

To open Windows Remote Assistance, run msra.exe.

**Activity 11-3**

### Creating a Remote Assistance Request

**Time Required:**5 minutes

**Objective:**Create a Remote Assistance request

**Description:**You want to create a Remote Assistance request so that you can send it to a colleague to work through a problem together on your computer. In this activity, you create a Remote Assistance request.

**Tip**

If there is time, consider working with a partner to test Remote Assistance. The two computers must be able to communicate over the network.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, type **msra**, and then click **msra**.

1. 3

In the Windows Remote Assistance dialog box, click **Invite someone you trust to help you**.

1. 4

On the How do you want to invite your trusted helper screen, click **Save this invitation as a file**.

1. 5

In the Save As dialog box, note the location and file name and then click **Save**.

1. 6

Note the password that is displayed that must also be given to your helper.

1. 7

Close the Windows Remote Assistance window and then click **Yes** when prompted for confirmation.

Go to pg.

[**help**](javascript://)

Application Opened

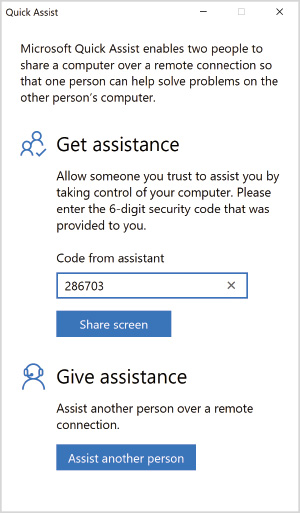
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-1cQuick Assist

[**Quick Assist**](javascript://) is a simplified and improved tool in Windows 10 to remote control another computer. Like Remote Assistance, Quick Assist lets you view what the user is doing, but the connectivity process is simplified and works well over the Internet without the requirement to install or configure any additional software.

Authentication for Quick Assist is based on a security code that is generated by the helper. If you want to assist someone else, you need to sign in by using a Microsoft Account or an Azure AD account. After you are signed in, a security code is displayed, and you need to send the security code to the person you are helping. The person you are helping enters the security code into Quick Assist on their computer to complete the connection, as shown in [Figure 11-7](javascript://). Once connected, you can see their screen. If the user allows it, you can control the mouse and keyboard.

**Figure 11-7Quick Assist**



Computers using Quick Assist do not communicate directly with each other. They each connect to a Microsoft server that mediates the communication. No special firewall configuration is required because Quick Assist connects to port 443 on the Microsoft server just like a browser connecting to a secure website.

**Tip**

Quick Assist is an excellent tool for any environment, but it is very well suited for novice users because of the minimal configuration requirements.

**Activity 11-4**

### Using Quick Assist

**Time Required:**5 minutes

**Objective:**Use Quick Assist for remote control

**Description:**You are working at the help desk and want to provide assistance to a staff member in your company. This person is working at home using a computer running Windows 10. In this activity, you provide remote assistance by using Quick Assist.

**Tip**

If there is time, consider working with a partner to test Quick Assist. The two computers must have access to the Internet.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, type **quick**, and then click **Quick Assist**.

1. 3

In the Quick Assist window, read the information and then click **Assist another person**.

1. 4

Sign in by using your Microsoft Account.

1. 5

When prompted to stay signed in, click **No**.

1. 6

On the Share security code screen, read the information. The security code must be given to the person you are helping.

1. 7

Close the Quick Assist window.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-1dMMC Snap-Ins

Older MMC snap-ins use [**remote procedure calls (RPC)**](javascript://) to connect to computers running Windows 10 over the network. RPC communication is no longer preferred for new snap-ins and apps because it uses randomly selected port numbers that are difficult to regulate using network firewalls. The following general process is used to create an RPC connection:

1. The client connects to the RPC Endpoint Mapper service (TCP port 135) on the remote computer.
2. The RPC Endpoint Mapper service identifies the TCP port for the requested app or service.
3. The RPC Endpoint Mapper service sends the client the TCP port for the requested app or service.
4. The client connects to the app or service on the remote computer using the supplied TCP port.

For RPC communication in Windows 10, the RPC Endpoint Mapper service and the Remote Procedure Call (RPC) service must be running. Both services are set to start automatically in Windows 10.

To allow connectivity for MMC snap-ins, you might need to enable Windows Defender Firewall rules, such as the following:

* Remote Event Log Management (RPC)
* Remote Scheduled Tasks Management (RPC)
* Remote Service Management (RPC)
* Windows Defender Firewall Remote Management (RPC)

**Activity 11-5**

### Viewing Event Logs Remotely by Using RPC

**Time Required:**10 minutes

**Objective:**View event logs remotely by using RPC

**Description:**The Event Viewer MMC snap-in can connect to remote computer systems by using RPC. This allows you to see the contents of event logs on other computers without visiting the desktop. In this activity, you verify RPC connectivity for Event Viewer.

**Note 3**

This activity assumes you have access to the desktop of the domain controller to which your Windows client is joined.

1. 1

Sign in to your domain controller as AD\Administrator.

1. 2

Click the **Start** button, type **event**, and then click **Event Viewer**.

1. 3

In the Event Viewer window, right-click **Event Viewer (Local)** in the left pane and then click **Connect to Another Computer**.

1. 4

In the Select Computer dialog box, click **Browse** and then click **Advanced**.

1. 5

Click **Find Now**, select your Windows 10 computer, and then click **OK** three times.

1. 6

Wait until the connection fails, read the information, and then click **OK**.

1. 7

On your Windows 10 computer, sign in as AD\Administrator.

1. 8

Right-click the **Start** button and then click **Windows PowerShell (Admin)**.

1. 9

At the Windows PowerShell prompt, type **Get-Service rpc\*** and then press **Enter**. Notice that the status for RPC Endpoint Mapper service and the Remote Procedure Call (RPC) service show they are Running.

1. 10

Close the Windows PowerShell prompt window.

1. 11

Click the **Start** button, type **defender**, and then click **Windows Defender Firewall with Advanced Security**.

1. 12

In the Windows Defender Firewall with Advanced Security window, select **Inbound Rules**.

1. 13

In the list of inbound rules, scroll down and click **Remote Event Log Management (RPC)** for the **Domain** profile.

1. 14

In the Actions pane, click **Enable rule**. Notice that a green check mark now appears beside the rule to indicate that it’s enabled.

1. 15

Close the Windows Defender Firewall with Advanced Security window.

1. 16

On the domain controller, in Event Viewer, right-click **Event Viewer (Local)** and then click **Connect to Another Computer**.

1. 17

In the Select Computer dialog box, click **Browse** and then click **Advanced**.

1. 18

Click **Find Now**, select you Windows 10 computer, and then click **OK** three times. Notice that the Windows 10 computer name now appears in the navigation pane.

1. 19

In the navigation pane, expand **Windows Logs**, click **System**, and then double-click an event to open it.

1. 20

In the Event Properties dialog box, read the computer attribute, and verify that the name listed is your Windows 10 computer.

1. 21

Close all open windows.

Newer MMC snap-ins and some other management tools use a web-based protocol for remote management. [**Windows Remote Management (WinRM)**](javascript://) is the Microsoft implementation of the WS-Management protocol for remote management. WS-Management defines how messages are passed between the client and the remote computer.

WinRM is implemented as the Windows Remote Management (WS-Management) service. By default, this service is set for manual startup. Before you can access WinRM on a remote computer, you need to configure it. This process can be done manually, but the simplest method for configuring WinRM is to run one of the following commands:

* winrm quickconfig
* Set-WSManQuickConfig

The quickconfig commands perform the following steps for you:

1. Starts the WinRM service.
2. Configures the WinRM service to start automatically.
3. Creates a listener that accepts requests from any IP address.
4. Enables the firewall rule to allow access to WinRM.

The WinRM service listens on port 5985. You may see some out-of-date documentation that refers to WinRM listening on port 80, but that documentation was relevant only for Windows XP.

WinRM is not configured to use secure sockets layer (SSL) or transport layer security (TLS) to secure communication. Authentication to WinRM is protected by Kerberos, but data sent over the network is unencrypted. If you do decide to enable SSL/TLS for WinRM, the port used is 5986 and you need to create the firewall rule to allow it. You also need to deploy certificates to the computers that will be running WinRM.

**Activity 11-6**

### Enabling WinRM

**Time Required:**5 minutes

**Objective:**Enable WinRM

**Description:**You have purchased a new management tool for Windows 10. This tool uses WinRM to remotely connect to Windows 10. To enable this tool to work, you need to enable WinRM and verify it is listening on the network. In this activity, you enable WinRM and verify which port it is listening on.

1. 1

If necessary, turn on your computer and sign in as AD\Administrator.

1. 2

Right-click the **Start** button and then click **Windows PowerShell (Admin)**.

1. 3

At the Windows PowerShell prompt, type **Set-WSManQuickConfig** and then press **Enter**.

1. 4

Read the information that is displayed, type **Y**, and then press **Enter**.

1. 5

Type **winrm /?** and then press **Enter**. Read the options available with the tool.

1. 6

Type **winrm get winrm/config** and then press Enter.

1. 7

Scroll through the output and read the settings.

1. 8

Close the Windows PowerShell prompt window.

1. 9

Click the **Start** button, type **resource**, and then click **Resource Monitor**.

1. 10

In the Resource Monitor window, click the **Network** tab and then expand **Listening Ports**.

1. 11

Scroll down in the list of ports and verify that the System image for Windows 10 is listening on port 5985.

1. 12

Close the Resource Monitor window.

You can also use Group Policy to enable WinRM. To enable WinRM by using Group Policy, you need to create a Group Policy object that performs the same tasks as the quickconfig option, as follows:

* Set the WinRM service to start automatically
* Configure a WinRM listener
* Enable the Windows Remote Management (HTTP-in) firewall rule

The Group Policy setting for configuring a WinRM listener is Allow remote server management through WinRM located in Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management\WinRM Service\. You need to enable this setting and define a filter for client connections. Using a filter of \* allows connections from any IP address.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-1eRegistry Editor

To use the Registry Editor to edit the registry of a remote computer running Windows 10, you need to enable the Remote Registry service on the remote computer. The Remote Registry service is disabled by default so that you cannot start it accidentally. This also prevents malware from starting the Remote Registry service. The Remote Registry service does not need to be started manually; when you connect to the computer, a trigger starts it automatically.

Connections to the Remote Registry service are on TCP port 445. You typically do not need to configure the firewall to allow access to this port because it is already allowed for file sharing. The rule is File and Printer Sharing (SMB-In).

**Activity 11-7**

### Enabling Remote Registry Editing

**Time Required:**10 minutes

**Objective:**Enable remote registry editing

**Description:**To simplify troubleshooting with users in your organization, you want to view and modify registry settings remotely. You want to use the Registry Editor because it is easier than running scripts while you are investigating. In this activity, you enable the Remote Registry service and test the capability to view the registry remotely.

**Note 4**

This activity assumes you have access to the desktop of the domain controller to which your Windows client is joined.

1. 1

If necessary, turn on your computer and sign in as AD\Administrator.

1. 2

Right-click the **Start** button and then click **Computer Management**.

1. 3

In the Computer Management window, expand **Services and Applications** and then click **Services**.

1. 4

Scroll down in the list of services and then click **Remote Registry**. Notice that this service is disabled.

1. 5

Right-click **Remote Registry** and then click **Properties**.

1. 6

In the Remote Registry Properties dialog box, in the Startup type box, select **Automatic** and then click **OK**.

1. 7

Close the Computer Management window.

1. 8

Click the **Start** button, type **defender**, and then click **Windows Defender Firewall with Advanced Security**.

1. 9

In the Windows Defender Firewall with Advanced Security window, select **Inbound Rules**.

1. 10

In the list of inbound rules, scroll down and then click **File and Printer Sharing (SMB-In)** for the **Domain** profile.

1. 11

If the rule is disabled, in the Actions pane, click **Enable rule**. Notice that a green check mark now appears beside the rule to indicate that it’s enabled.

1. 12

Close the Windows Defender Firewall with Advanced Security window.

1. 13

On your domain controller, sign in as AD\Administrator.

1. 14

Click the **Start** button, type **regedit**, and then click **Registry Editor**.

1. 15

In the Registry Editor window, click **File** and then click **Connect Network Registry**.

1. 16

In the Select Computer dialog box, click **Advanced** and then click **Find Now**.

1. 17

Select your Windows 10 computer and then click **OK** twice. Your Windows 10 computer name appears.

1. 18

Under your Windows 10 computer name, expand **HKEY\_LOCAL\_MACHINE.**

1. 19

Close the Registry Editor window.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-1fWindows PowerShell Remoting

You can use [**Windows PowerShell remoting**](javascript://) to run Windows PowerShell cmdlets and scripts on remote computer systems. For any tasks that you can use Windows PowerShell at the desktop, you can perform that same task remotely over the network by using Windows PowerShell remoting. By default, Windows PowerShell remoting is disabled in Windows 10.

To enable Windows PowerShell remoting, you need to run the Enable-PSRemoting cmdlet. This command performs all the following tasks:

1. Enables WinRM if not already configured (same as quickconfig).
2. Registers Windows PowerShell with WinRM.
3. Restarts the WinRM service to force settings to take effect.

To remotely access a computer by using PowerShell Remoting, run the Enter-PSSession -ComputerName RemoteComputer command. In a domain-based network, no further configuration is required because Kerberos authentication is successful. Your current credentials are used to authenticate to the remote computer. In a workgroup-based network you need to perform these two extra steps:

* Configure TrustedHosts on the client.
* Provide credentials when connecting.

By default, WinRM only allows Kerberos authentication using HTTP. In a workgroup-based network this is not possible. To allow authentication, you can either enable HTTPS for WinRM or configure TrustedHosts. The client will transmit unencrypted credentials to the remote computer only if the remote computer has been added to TrustedHosts. To add a trusted host, use the following PowerShell command:

* Set-Item WSMAN:\localhost\Client\TrustedHosts -Value “IPAddress”

Or add a trusted host at a command prompt, as follows:

* wsman set winrm/config/client @{TrustedHosts=“IPAddress”}

To be prompted for credentials when connecting, use this modified command to connect to the remote host:

* Enter-PSSession -ComputerName RemoteComputer -Credential (Get-Credential)

**Activity 11-8**

### Enabling Windows PowerShell Remoting

**Time Required:**10 minutes

**Objective:**Enable Windows PowerShell remoting

**Description:**Your organization has hundreds of desktop computers, and you want to use Windows PowerShell remoting to help perform troubleshooting on those computers. Before you use Group Policy to enable Windows PowerShell remoting on all the computers, you want to enable Windows PowerShell remoting manually and try it out. In this activity, you enable Windows PowerShell remoting on Windows 10 and test the functionality.

**Note 5**

This activity assumes you have access to the desktop of the domain controller to which your Windows client is joined.

1. 1

If necessary, turn on your computer and sign in as AD\Administrator.

1. 2

Right-click the **Start** button and then click **Windows PowerShell (Admin)**.

1. 3

At the Windows PowerShell prompt, type **Enable-PSRemoting** and then press **Enter**. Notice that WinRM is already configured from a previous Activity.

1. 4

Close the Windows PowerShell prompt window.

1. 5

On your domain controller, sign in as AD\Administrator.

1. 6

Right-click the **Start** button and then click **Windows PowerShell (Admin)**.

1. 7

At the Windows PowerShell prompt, type **Enter-PSSession -ComputerName <Win10Computer>**, where <Win10Computer> is the name of your Windows 10 computer, and then press **Enter**.

1. 8

Read the text at the prompt. Notice that the computer name is now displayed to indicate that you are connected to a remote session.

1. 9

Type **Get-ComputerInfo** and then press **Enter**.

1. 10

Scroll through the displayed computer information and verify that the operating system is Windows 10 and the computer name matches the name of your Windows 10 computer.

1. 11

Type **Exit-PSSession** and then press **Enter**.

1. 12

Close the Windows PowerShell prompt window.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**11-2**Managing Profiles for Roaming Users

A roaming user is a person who does not use the same computer each day. This has long been common in businesses such as call centers, but you can now see this in open office environments also. An important concern for roaming users is consistent computer configuration. Users strongly prefer a consistent work environment, including files and settings.

Windows has long supported roaming user profiles that are stored on a file server, but roaming users profiles have never worked well. They are prone to corruption, which requires intervention by an administrator. If a large amount of data is stored in a roaming profile, the sign-in and sign-out process can be very slow.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-2aMapped Drive Letters

Even though roaming user profiles don’t work well, the concept of centrally storing data so that it’s accessible from multiple locations is a sound one. One of the first measures that any organization should implement is centralized file shares for data storage. Computers can be configured with mapped drive letters that connect to the file shares so that files are accessible from any computer. All users in a department will have access to the same files for collaboration.

**Tip**

Cloud storage services are quite popular, but large organizations still keep many files on premises in shares.

For personal data, users can be given a private home drive on a file server. Again, this would be available from any computer when the user signs in.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-2bFolder Redirection

You can use [**folder redirection**](javascript://) to store some profile information on a file server so that it’s accessible from any computer. This is better than a roaming profile because the data is used directly from the network location and isn’t synchronized locally. You typically configure folder redirection by using Group Policy.

Some of the folders you can synchronize include:

* AppData\Roaming
* Documents
* Desktop
* Downloads
* Favorites

**Tip**

Redirecting the Documents folder to a network share makes it easy for users to store documents in a central location.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-2cCredential Roaming

Some organizations issue certificates to users for authentication to resources. In Windows 10, user certificates are stored in the user profile but are not part of any folder that can be redirected. You can implement credential roaming to allow certificates to synchronize to the profile on multiple computers when roaming users profiles are not implemented.

When you implement Credential Roaming, the user certificates are stored in Active Directory. Then, during sign in, certificates are synchronized with the local user profile. You enable Credential Roaming by using Group Policy.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-2dUser Experience Virtualization

[**User Experience Virtualization (UE-V)**](javascript://) provides user state virtualization similar to roaming profiles. When users sign in to different domain-joined computers, their settings follow them from computer to computer; however, UE-V provides more advanced functionality that is not provided by roaming profiles, such as:

* Synchronization is based on templates for fine-grained control of specific application settings.
* Synchronization can be performed between multiple operating systems where user profiles would not be compatible.
* Settings are synchronized while the user is signed in rather than at sign-in or sign-out.

The UE-V agent is included with Windows 10 Enterprise and Education. To enable UE-V, you configure Group Policy settings to configure the client. Two important settings are as follows:

* Setting storage location—This location is a file share where the settings for users are stored by the agent.
* Settings template catalog location—This location is a file share where settings location templates that describe how to synchronize settings for specific applications are stored. The agent reads the settings location templates.

You do not need to create settings location templates for all apps for which you want to synchronize settings. UE-V includes the ability to synchronize settings for Microsoft Office and many Windows settings. Settings location templates typically need to be created for custom apps and non-Microsoft apps.

**Note 6**

For detailed information about UE-V, see User Experience Virtualization (UE-V) for Windows 10 overview at [https://docs.microsoft.com/en-us/windows/configuration/ue-v/uev-for-windows](https://docs.microsoft.com/en-us/windows/configuration/ue-v/uev-for-windows" \t "_blank).

Go to pg.

[**help**](javascript://)

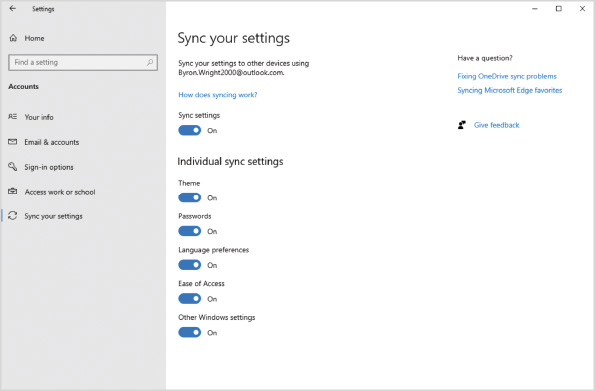
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-2eProfile Synchronization with Microsoft Account or Azure AD

You can use a Microsoft Account or an Azure AD account to synchronize profile settings to multiple computers. The profile settings are stored online as part of the Microsoft Account or Azure AD account. When you use the cloud-based account to sign in to another computer, the settings are downloaded and used in the local copy of the profile, as shown in [Figure 11-8](javascript://).

**Figure 11-8Sync Settings with Microsoft Account**



Enlarge Image

If a computer is Azure AD joined, you can’t manually enable the Sync your settings option. On an Azure AD-joined device, an administrator needs to enable Enterprise State Roaming in Azure AD.

Go to pg.

[**help**](javascript://)

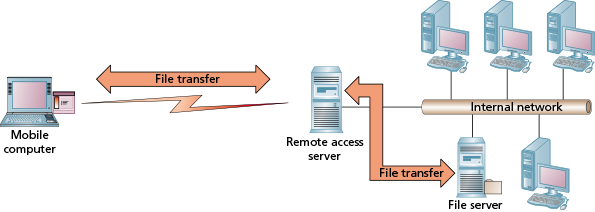
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**11-3**Using a VPN for Remote Access

Remote access consists of a dedicated computer acting as a remote access server and clients connecting to that server. After clients are connected to the remote access server, the clients have access to resources on the network where the remote access server is located. For example, remote access clients can open and save files on a file server back in the main office, as shown in [Figure 11-9](javascript://). In fact, the client gets an IP address for the organizational network.

**Figure 11-9Remote Access**



Enlarge Image

The oldest technology for remote access is dial-up networking. Dial-up networking clients have a modem and connect to the remote access server over telephone lines. This technology is seldom used now because it is very slow when compared with Internet connectivity. Dial-up connectivity is limited to approximately 56 KBps (kilobits per second). A 4G data plan on most mobile phones is over 1000 times faster.

**Note 7**

For a detailed list of Windows 10 settings that can be synced, see Windows 10 roaming settings reference at [https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-reference](https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-windows-settings-reference" \t "_blank).

It is much more common for remote access to be done over a [**virtual private network (VPN)**](javascript://). A VPN creates an encrypted connection between the VPN clients and the remote access server over a public network, such as the Internet. Because the connection is encrypted, anyone between the VPN client and the remote access server is prevented from viewing the data in transit.

A VPN is much faster than dial-up because it operates at almost the same speed as the Internet connection; however, latency is still much higher over a VPN than on a local area network (LAN). Therefore, even with a fast connection, accessing data is slower over a VPN than it is locally. Opening and saving files, such as Word documents, is a noticeably slower process over a VPN, but users might find it tolerable. For many apps that use a central database for data storage, a VPN is not practical because the app running on the client generates many small requests, and each request has high latency, which delays processing in the app.

Go to pg.

[**help**](javascript://)

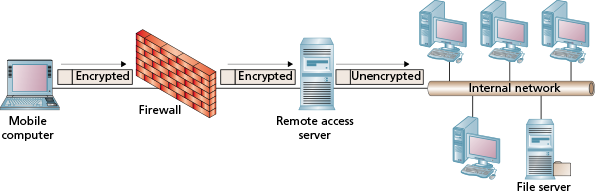
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-3aConfiguring VPN Clients

One of the main concerns when you allow remote access to resources is security. A VPN encrypts communication between the VPN clients and the remote access server, as shown in [Figure 11-10](javascript://). On the internal network, the remote access server sends the data as unencrypted cleartext just as if the client were located on the internal network. When you evaluate VPN security, you need to be aware of the different protocols and authentication methods that can be used.

**Figure 11-10Windows Remote Assistance**



Enlarge Image

Windows Server 2019 can be configured as a remote access server by installing the Remote Access server role. When you use Windows Server as a remote access server, the required protocols for connectivity with Windows 10 are included in Windows 10. It’s not necessary to deploy additional software on the clients.

Many organizations use a non-Microsoft solution for their VPN. Often, these solutions are provided by network equipment vendors, such as Cisco, Juniper, Palo Alto, SonicWALL, Fortinet, and WatchGuard. Most of the non-Microsoft solutions require you to install a VPN client that is specific to their solution.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-3bVPN Protocols

The VPN protocols that are supported by Windows 10 are the protocols supported when you use Windows Server as a remote access server. When you are planning a VPN deployment, you decide which protocols will be offered based on your analysis of how secure they are and how easy they are to use. When you configure the VPN clients, you need to select a protocol that is already configured on the server.

### PPTP

[**Point-to-Point Tunneling Protocol (PPTP)**](javascript://) is one of the easiest protocols to use for a VPN. Authentication for PPTP is typically based on a user name and password, which is easy for users to work with. It is possible to configure certificate-based authentication, which is more secure, but this is seldom done.

Most remote locations, such as hotels, allow PPTP packets to pass through their firewalls. PPTP is widely supported because it is an older protocol that has been available since the 1990s; however, it is also one of the most insecure protocols. A determined hacker who has captured authentication traffic for PPTP can easily determine the user name and password. Despite the security concerns, PPTP is still used for some networks with low security requirements.

The PPTP protocol is initiated by the VPN client communicating with the remote access server on TCP port 1723. At this point, a Generic Routing Encapsulation (GRE) tunnel is created. The GRE packets are IP protocol type 47 and need to be allowed through any firewalls. The GRE packets have a source and destination IP address, but they are not TCP (6) or UDP (17) packets. This is why they require special consideration.

### L2TP

[**Layer 2 Tunneling Protocol (L2TP)**](javascript://) is only an authentication protocol. When you create an L2TP VPN connection, IPSec is used with L2TP to provide data encryption. The authentication provided by L2TP is based on user credentials. IPSec includes authentication for the VPN client and remote access server. The combination of the two authentication levels increases security, but it also makes it more difficult to manage L2TP VPN connections. As a consequence, the Microsoft implementation of L2TP has never become very popular.

The authentication for IPSec can be based on:

* Pre-shared key—This is a password that needs to be configured on both the VPN client and the remote access server. A pre-shared key is relatively easy to implement, but, because a single password is shared by all clients and the remote access server, this is not very secure.
* Certificates—If the VPN client and the remote access server have both been configured with certificates that are trusted, certificate authentication can be used. This is more secure than a pre-shared key, but it can be awkward to deploy certificates to all the VPN clients.
* Kerberos—Windows-based networks use Kerberos to authenticate users and computers. This same protocol can be used by IPSec. Using IPSec is possible only if the VPN client computer and the remote access server are members of the same Active Directory forest.

To allow L2TP connectivity through a firewall, you need to allow UDP port 500, UDP port 4500, and IP protocol type 50. IP protocol type 50 is Encapsulating Security Payload (ESP) that is used by IPSec.

### SSTP

To simplify firewall configuration and ensure the best compatibility with remote locations, many VPNs are now based on Secure Sockets Layer (SSL). An SSL VPN uses TCP port 443, which is also used by secure websites. All public networks allow connectivity using TCP port 443. Microsoft has implemented [**Secure Socket Tunneling Protocol (SSTP)**](javascript://) as an SSL VPN.

**Tip**

SSL is an obsolete protocol for network encryption. SSL VPNs have been updated to use the new Transport Layer Security (TLS) protocol for network encryption, but retain SSL in the name.

An SSTP connection is authenticated by a user name and password to make it easier for users. In addition, the remote access server is authenticated because the certificate installed on the remote access server for encryption must be trusted.

### IKEv2 Tunneling Protocol

[**Internet Key Exchange v2 Tunneling Protocol (IKEv2)**](javascript://) is a newer VPN protocol that allows IPSec to be used for data encryption. Unlike L2TP, authentication for an IKEv2 VPN connection does not require that IPSec authentication be configured separately. You can use authentication based only on a user name and password.

The main benefit of IKEv2 is better support for unreliable network connections. Microsoft refers to this feature as [**VPN Reconnect**](javascript://). Unlike a typical VPN connection, which may lose connectivity when a network interruption occurs, IKEv2 can reconnect automatically when network connectivity is restored. In some cases, users might not notice that the VPN was ever disconnected.

Firewall configuration for IKEv2 is the same as for L2TP. You need to allow UDP port 500, UDP port 4500, and IP protocol type 50.

Go to pg.

[**help**](javascript://)

Application Opened

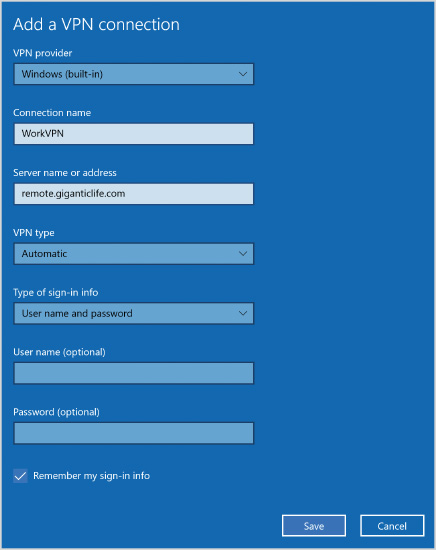
[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-3cCreating a VPN Connection

In most cases, a typical user will have only one VPN connection back to the main office to access data; however, a support technician with multiple clients may have a VPN connection for each client. Your specific scenario determines which method for creating VPN connections will work best for you.

Individual Windows 10 users can create a VPN connection from Settings, as shown in [Figure 11-11](javascript://). You can also create a new connection from Network and Sharing Center by selecting Set up a new connection or network. When users configure a VPN connection manually, you will need to provide instructions on how to create the VPN connection, including any settings that are necessary. Even with instructions, the process tends to be error-prone because users make mistakes in the configuration.

**Figure 11-11Creating a VPN Connection in Settings**



Enlarge Image

When you configure a VPN from Settings, you need to provide the following information:

* VPN provider—The VPN provider is the software that creates and controls the VPN connection. Windows 10 includes the Windows VPN provider, but other vendors can make providers available to support their specific type of VPN. Other VPN providers need to be installed as additional software because they are not included in Windows 10.
* Connection name—Each VPN connection needs a name to identify it. This should be given a name that relates to its purpose.
* Server name or address—This is the FQDN or IP address of the remote access server that the VPN client connects to.
* VPN type—The default value for VPN type is Automatic, which attempts to detect the type of VPN automatically. This avoids the need for the user to know the specific VPN type. If the type of VPN is not detected properly, you can select a specific VPN type, such as PPTP or SSTP, as defined on the remote access server.
* Type of sign-in info—Many organizations allow users to sign in by using a user name and password; however, you can enhance sign-in security by using smart cards, one-time passwords, or certificates.

An option to enter and save credentials (user name and password) is provided when you create the VPN connection. If you save the credentials, any user who gains access to your computer could remotely access over the VPN. This is less of a risk if BitLocker is being used to protect the hard drive.

**Activity 11-9**

### Creating a VPN Connection

**Time Required:**5 minutes

**Objective:**Create a VPN connection that connects to a remote access server

**Description:**You want to connect to the remote access server at your office to access files securely over the Internet. In this activity, you configure a VPN connection.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button and then click **Settings**.

1. 3

In the Settings window, click **Network & Internet** and then click **VPN**.

1. 4

Below the VPN heading, click **Add a VPN connection**.

1. 5

In the Add a VPN connection window, in the VPN provider box, select **Windows (built-in)**.

1. 6

In the Connection name box, type **WorkVPN**.

1. 7

In the Server name or IP address box, type **vpnserver.giganticlife.com**.

1. 8

In the VPN type box, select **Automatic**.

1. 9

In the Type of sign-in info box, select **User name and password** and then click **Save**.

1. 10

In the Settings window, click **WorkVPN** and then click **Advanced options**.

1. 11

Review the list of options and close all open windows.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-3dAutomated VPN Deployment

Many organizations provide users with a list of instructions to create VPN connections manually on their computers. If you want to simplify VPN deployment for your users and reduce the chance of configuration errors, you can automate VPN deployment.

Several methods are available for deploying VPN connections automatically. These methods are listed in [Table 11.3](javascript://).

**Table 11-3**

### Methods to Deploy VPN Connections

| **Deployment Method** | **Description** |
| --- | --- |
| Group Policy Preferences | You can distribute VPN connections by using Group Policy Preferences. For domain-joined computers, this is the simplest way to configure VPN connections automatically. This method cannot be used for computers that are not domain joined. |
| Connection Manager Administration Kit (CMAK) | Connection Manager Administration Kit (CMAK) is a feature that can be installed on Windows 10 or Windows Server. You use CMAK to create VPN connections that are packaged as an executable file. Users can run the executable file to create VPN connections on their computer. Computers do not need to be domain joined. |
| Windows PowerShell | Although it is possible to create and manage VPN connections by using Windows PowerShell cmdlets, it is beyond the scope of this book to identify the cmdlet details for occasional use. You could, however, create a script that creates VPN connections as an alternative to distributing an executable created with CMAK. Computers do not need to be domain joined, but users need to be knowledgeable enough to run the Windows PowerShell script. |
| Windows Configuration Designer | You can use Windows Configuration Designer to create VPN connectivity profiles that are deployed to client computers as provisioning packages. Provisioning packages can be distributed to clients as a file that needs to be installed, via Microsoft Intune or via Microsoft Endpoint Configuration Manager. |

**Activity 11-10**

### Using CMAK

**Time Required:**15 minutes

**Objective:**Use CMAK to create a deployment package for a VPN connection

**Description:**You would like to create a deployment package for a VPN connection that can be used by Windows 10 computers that are domain joined or not domain joined. In this activity, you install CMAK and create a deployment package for a VPN connection.

1. 1

If necessary, start your computer and sign in as AD\Administrator.

1. 2

Click the **Start** button and then click **Settings**.

1. 3

In the Settings window, click **Apps**, click **Apps & features**, and then click **Optional features**.

1. 4

On the Optional features screen, click **Add a feature**.

1. 5

In the Add an optional feature window, select the **RAS Connection Manager Administration Kit (CMAK)** check box and then click **Install (1)**.

1. 6

When installation is complete, close the Settings window.

1. 7

Click the **Start** button, type **cmak**, and then click **Connection Manager Administration Kit**.

1. 8

In the Connection Manager Administration Kit Wizard window, click **Next**.

1. 9

On the Select the Target Operating System screen, click **Windows Vista or above** and then click **Next**.

1. 10

On the Create or Modify a Connection Manager profile screen, click **New profile** and then click **Next**.

1. 11

On the Specify the Service Name and the File Name screen, in the Service name text box, type **GiganticLifeVPN**.

1. 12

In the File name text box, type **GLvpn** and then click **Next**.

1. 13

On the Specify a Realm Name screen, click **Do not add a realm name to the user name** and then click **Next**.

1. 14

On the Merge Information from Other Profiles screen, click **Next**.

1. 15

On the Add Support for VPN Connections screen, select the **Phone book from this profile** check box.

1. 16

In the VPN server name or IP address area, click **Always use the same VPN server**, type **remote.giganticlife.com** in the text box, and then click **Next**.

1. 17

On the Create or Modify a VPN Entry screen, click **GiganticLifeVPN Tunnel <Default>** and then click **Edit**.

1. 18

In the Edit VPN Entry window, click the **Security** tab.

1. 19

In the VPN Strategy box, select **Try Secure Socket Tunneling Protocol First**.

1. 20

In the Logon security area, click **Use Extensible Authentication Protocol (EAP)**, select **Microsoft: Protected EAP (PEAP) (encryption enabled)**, and then click **OK**.

1. 21

On the Create or Modify a VPN Entry screen, click **Next**.

1. 22

On the Add a Custom Phone Book screen, clear the **Automatically download phone book updates** check box and then click **Next**.

1. 23

On the Configure Dial-up Networking Entries screen, click **Next**.

1. 24

On the Specify Routing Table Updates screen, click **Next**.

1. 25

On the Configure Proxy Settings for Internet Explorer screen, click **Next**.

1. 26

On the Add Custom Actions screen, click **Next**.

1. 27

On the Display a Custom Logon Bitmap screen, click **Next**.

1. 28

On the Display a Custom Phone Book Bitmap screen, click **Next**.

1. 29

On the Display Custom Icons screen, click **Next**.

1. 30

On the Include a Custom Help File screen, click **Next**.

1. 31

On the Display Custom Support Information screen, click **Next**.

1. 32

On the Display a Custom License Agreement screen, click **Next**.

1. 33

On the Install Additional Files with the Connection Manager profile screen, click **Next**.

1. 34

On the Build the Connection Manager Profile and Its Installation Program screen, click **Next**.

1. 35

On the Your Connection Manager Profile is Complete and Ready to Distribute screen, verify the location of the .exe file and then click **Finish**.

**Activity 11-11**

### Using Windows PowerShell to View VPN Connections

**Time Required:**5 minutes

**Objective:**Use Windows PowerShell to view the VPN connections on a computer

**Description:**As an administrator, you want a quick way to see the VPN connections that have been created on a computer. In this activity, you use Windows PowerShell to view the VPN connections on a computer.

1. 1

If necessary, start your computer and sign in as AD\Administrator.

1. 2

Right-click the **Start** button and then click **Windows PowerShell (Admin)**.

1. 3

At the Windows PowerShell prompt, type **Get-Command \*vpn\*** and then press Enter.

1. 4

Type **Get-VpnConnection -AllUserConnection** and then press **Enter**.

1. 5

Close all open windows.

Go to pg.

[**help**](javascript://)

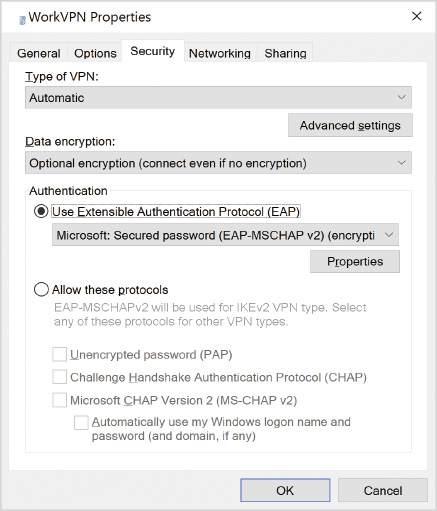
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-3eAuthentication Protocols

When you create a VPN connection in Settings, you are required to specify the type of sign-in information. This setting defines the options that are used for authentication, which are shown in [Figure 11-12](javascript://). These advanced security settings can be edited from the properties of the VPN adapter. In most cases, you should configure the type of sign-in info through Settings rather than modifying the authentication settings directly.

**Figure 11-12VPN Security Settings**



For the purpose of understanding documentation and using other tools, such as Windows PowerShell, for VPN management, it is useful to understand the authentication protocols.

**[Extensible Authentication Protocol (EAP)](javascript://)** is a framework that allows multiple authentication methods to be integrated with the sign-in process. Multiple authentication methods are included with Windows 10, and more can be added by vendors. EAP can be used by the newer VPN protocols. IKEv2 requires the use of EAP.

Windows 10 includes Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP). Both of these protocols should be used only if there is no other choice. PAP transmits unencrypted credentials during authentication and CHAP has serious security flaws that make it easy to obtain the credentials. Microsoft CHAP version 2 (MS-CHAP v2) provides significantly better security than PAP and CHAP, but it is also known to be vulnerable to hacking with minimal effort and should be avoided whenever possible.

PAP, CHAP, and MS-CHAP v2 are used with PPTP VPNs. A preferred alternative is to use another VPN type for better security. If that is not possible, evaluate the possibility of using PEAP-MS-CHAP v2 with PPTP. This authentication method uses MS-CHAP v2 within [**Protected EAP**](javascript://). Protected EAP uses TLS to protect the authentication process and make it secure.

Go to pg.

[**help**](javascript://)

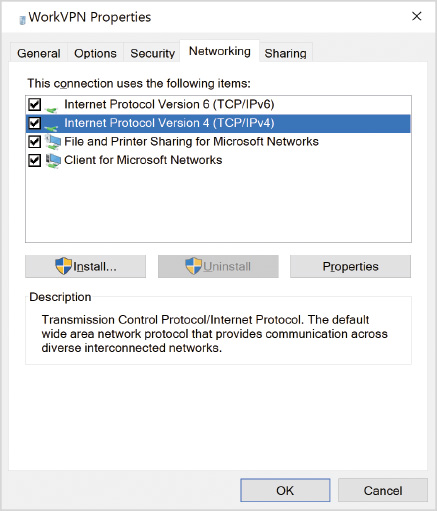
Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-3fNetwork Settings

A VPN connection has network settings just like an Ethernet or Wi-Fi connection, as shown in [Figure 11-13](javascript://). The Client for Microsoft Networks and File and Printer Sharing for Microsoft Networks can be disabled, but there are no configuration settings. IPv4 and IPv6 have configuration options similar to a standard network adapter.

**Figure 11-13VPN Network Settings**



By default, IPv4 is configured to obtain an IP address from DHCP automatically. In most cases, this is the preferred configuration; however, if you need to, you can configure a static address for the VPN connection. One setting that can be useful to change in the Advanced TCP/IP Settings is for the default gateway, as shown in the next activity.

The setting Use default gateway on remote network is selected by default. When this setting is enabled, all network access is done through the VPN. This is on by default to ensure that VPN clients can access resources on remote networks where the remote access server is located; however, this also means that all Internet access goes through the VPN, which might make Internet access slow. The remote access server can be configured to provide static routes to the VPN clients for internal resources and then allow VPN clients to continue using their normal default gateway.

**Note 8**

Configuring a VPN client to route some traffic through the VPN and some through the local default gateways is known as split tunneling.

**Activity 11-12**

### Disabling the VPN as Default Gateway

**Time Required:**5 minutes

**Objective:**Disable a VPN from being used as a default gateway

**Description:**You want to optimize Internet connectivity for a VPN client. The VPN server provides static routes for all of the internal networks, and the VPN clients use the local Internet connection as a default gateway. In this activity, you disable the use of the VPN as a default gateway.

1. 1

If necessary, start your computer and sign in as AD\Administrator.

1. 2

Click the **Start** button and then click **Settings**.

1. 3

In the Settings window, click **Network & Internet**, click **VPN**, and then click **Change Adapter options**.

1. 4

In the Network Connections window, right-click **WorkVPN** and then click **Properties**.

1. 5

In the WorkVPN Properties dialog box, click the **Networking** tab, click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.

1. 6

In the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box, click **Advanced**.

1. 7

In the Advanced TCP/IP Settings dialog box, on the IP Settings tab, clear the **Use default gateway on remote network** check box and then click **OK**.

1. 8

In the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box, click **OK**.

1. 9

In the WorkVPN Properties dialog box, click **OK**.

1. 10

Close all open windows.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-3gAlways On VPN

[**Always On VPN**](javascript://) is a VPN configuration that is available only for Windows 10 clients. When you configure Always On VPN, client computers can automatically connect to the VPN whenever connectivity is available. Benefits of this configuration are:

* Easier for users—Users do not need to do anything for Always On VPN to work. Access to all resources can be maintained with the only difference being slower access.
* Clients are manageable—Because the VPN is always on, the clients are manageable even when they are on the road. Group Policy Objects (GPOs) can still be applied and software deployment technologies still work. Generally, with a VPN, clients are not considered to be manageable.

You can implement device tunnel as part of Always On VPN. Device tunnel allows the VPN to connect and authenticate before users sign in. This means that user authentication is directly to the domain controller rather than using cached credentials. In this state, the help desk can reset user passwords and have them take effect immediately.

**Caution**

To implement device tunnel, you need to be using Windows 10 Enterprise or Education and the computers must be domain joined.

If you are using Windows 10 Pro, then only user tunnel is available for Always On VPN. User tunnel authenticates automatically after the user signs in to Windows 10. This still provides an excellent user experience but does not provide some of the management options available with device tunnel.

Always On VPN uses the IKEv2 protocol whenever possible, but will fallback and use SSTP when IKEv2 cannot be used. IKEv2 is preferred due to the VPN Reconnect functionality. Authentication is based on certificates issued to users and computers by an internal certification authority configured on a Windows Server.

**Caution**

The server configuration for Always On VPN is complex and should be carefully planned before you attempt to deploy.

To configure Always On VPN for Windows 10 computers, you need to create an XML configuration file with the settings for your deployment. Then, you run a Windows PowerShell script (typically VPN\_Profile.ps1) that uses the settings in the XML file to create the Always On VPN profile. To automate this process, you can use a logon script or Microsoft Endpoint Configuration Manager. There is no support to deploy Always On VPN by using Group Policy.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-3hDirectAccess

[**DirectAccess**](javascript://) is a technology similar to Always On VPN that is based on using a device tunnel. Authentication is performed automatically in the background whenever there is connectivity between the roaming client and the DirectAccess server. The initial release of DirectAccess for Windows 7 required certificates to be issued for authentication, but Windows 10 does not require certificates. Instead, a Kerberos proxy can be used for Windows 10 if some advanced features, such as high availability, are not required.

The client connectivity for DirectAccess is based on IPv6. Because most DirectAccess clients do not have IPv6 connectivity directly to the DirectAccess server, the IPv6 packets are tunneled in IPv4 packets over the Internet. On the internal network, there is no requirement for servers accessed by clients to have IPv6 configured.

Windows 10 is configured for DirectAccess by using GPOs. The GPOs are created on the server side during the DirectAccess configuration process. So, no manual configuration is required on the Windows 10 clients. In most cases, after DirectAccess is properly configured on the server, there is nothing to do on the client side.

The GPOs for DirectAccess are applied to a specific Active Directory group that is selected during configuration. For DirectAccess GPOs to apply to computers, the computer accounts need to be added to that group.

**Caution**

It is strongly recommended to implement Always On VPN instead of DirectAccess because it does not require the Enterprise or Education edition of Windows 10. If you need to support Windows 8.1, then DirectAccess is required.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

**11-4**Synchronizing Data for Mobile Clients

When you are in a location without network connectivity or with poor network quality, you cannot use a VPN or other forms of remote access. Sometimes locations do not provide guest Wi-Fi access, and hotels are notorious for having poor quality Wi-Fi.

When there is either no connectivity or poor connectivity, [**data synchronization**](javascript://) can be a solution. Data synchronization copies files locally to mobile computers. Then, users can work with the files whether they are connected to a network or not. At some point, the changed files are copied back (uploaded) to the server. The timing of the synchronization varies depending on the technology used for data synchronization.

One key consideration for data synchronization is shared application data. Users cannot access shared app data by using data synchronization unless the app performs its own offline data synchronization process. So, generally, data synchronization is good for personal files but not as useful for shared data.

**Note 9**

For more information about Always On VPN, see Remote Access Always On VPN at [https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/](https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/" \t "_blank).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-4aOneDrive

OneDrive is an example of how file synchronization can be used. Multiple computers can access the same OneDrive account, and all the computers can synchronize the files locally. For example, you can use the same OneDrive account on your desktop computer at the office, a laptop, and a desktop computer at home.

By default, OneDrive uses File On-Demand, which does not synchronize files locally until you open them. If you are on a mobile device and expect to be without network connectivity, you should force the files to sync locally. When you choose the Always keep on this device option for a file or folder, changes are automatically synced locally as soon as possible. This is important to be aware of when you are using multiple devices.

When you edit files, it is from a local copy, which is faster than accessing the file remotely. When you modify a file, the changes are synchronized back up to OneDrive. If you are offline when you modify a file, the changes are synchronized the next time you have an Internet connection.

In addition to the consumer version of OneDrive, OneDrive for Business also is included as part of Microsoft 365 and Office 365 cloud services. OneDrive for Business has approximately the same functionality as the consumer version, but it is part of SharePoint Online. You can also synchronize files from libraries in SharePoint Online. The default storage limit in OneDrive for Business is 1 terabyte (TB).

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-4bOffline Files

[**Offline files**](javascript://) is a Windows 10 feature that synchronizes files from a shared folder to a Windows 10 computer. Synchronization happens when the computer has connectivity to the server sharing the files. So, files are typically synchronized while in the office, used and modified offline while on the road, and then synchronized again when the computer is back in the office.

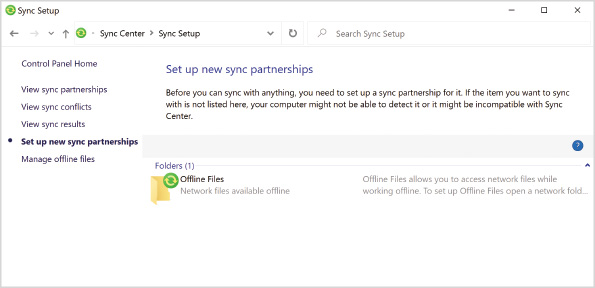
Offline files need to be enabled on both the Windows 10 computer and on the file share. If offline files are enabled in both locations, the default behavior is for the user to manually select any files or folders that will be cached (available offline). It is possible to configure a share to automatically make files available offline, but that is not recommended, so as to avoid synchronization errors on clients.

After files have been cached, they are available even when not connected to a network. Users access offline files using the exact same path as was used when the files were cached. If a user enables a folder on a mapped drive letter, such as H:\Important, to be offline, the files are accessible through H:\Important when disconnected from the network.

Typically, the offline files feature is not used for shared data, only personal data (such as a home folder). This minimizes the risk of conflicts where a cached copy of the file has been modified and the original source also has been modified. No automated mechanism exists to resolve such conflicts; the user needs to look at both files and merge the changes together if necessary. Some apps provide functionality to merge changes between two files, but sometimes it must be done manually.

To review any synchronization errors, you can use Sync Center, as shown in [Figure 11-14](javascript://). Sync Center shows any replication conflicts. Sync Center lists the locations being synchronized.

**Figure 11-14Sync Center**



Enlarge Image

**Activity 11-13**

### Enabling Offline Files

**Time Required:**5 minutes

**Objective:**Enable offline files

**Description:**You want to use offline files to store the contents of your home folder on your laptop. In this activity, you enable offline files on your computer.

1. 1

If necessary, start your computer and sign in.

1. 2

Click the **Start** button, type **Control**, and then click **Control Panel**.

1. 3

In the Control Panel window, in the **Search Control Panel** box, type **sync** and then click **Sync Center**.

1. 4

In Sync Center, click **Manage offline files**.

1. 5

In the Offline Files dialog box, click **Enable offline files** and then click **OK**.

1. 6

Click **Yes** to restart your computer.

1. 7

Close all open windows.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

## 11-4cWork Folders

When you implement [**Work Folders**](javascript://), each user is given a unique folder for file storage that can be synchronized across multiple devices. The folder for each user is stored on a file server. So, it is possible to access the folder through a file share and also to synchronize the folder contents by using the Work Folders client. The Work Folders client is available for Windows 7 and newer client operating systems. You can also obtain a Work Folders client for iOS and Android devices.

**Tip**

Work Folders is similar to running a private version of OneDrive.

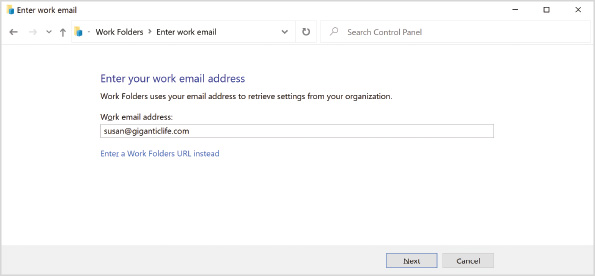
When Work Folders is configured on the server(s), a URL is identified for accessing Work Folders. Clients need to be configured to use that URL. Several methods can be used to configure the clients, but automatic discovery is preferred because it supports devices that are not domain joined.

Automatic discovery of the Work Folders URL is based on the email address of the user. If the user’s email address is [susan@giganticlife.com](mailto:susan@giganticlife.com), the Work Folders client attempts to connect to [https://workfolders.giganticlife.com](https://workfolders.giganticlife.com/" \t "_blank). In a single-server deployment of Work Folders, this directs all users directly to the server hosting their Work Folder.

If multiple Work Folder servers exist, you can still use automatic discovery, but you also need to configure each user object in Active Directory with the appropriate Work Folders URL. When [susan@giganticlife.com](mailto:susan@giganticlife.com) contacts [https://workfolders.giganticlife.com](https://workfolders.giganticlife.com/" \t "_blank), she is redirected to the Work Folders URL configured in her user object. The URL is stored in the msDS-SyncServerUrl attribute of the user object.

Another simple method that works when devices are not domain joined is manually entering the Work Folders URL. This is provided as an option in the Work Folders configuration screen, as shown in [Figure 11-15](javascript://). When allowing users to enter the URL, there is always a risk of the URL being incorrectly entered.

**Figure 11-15Work Folders Configuration**



Enlarge Image

For domain-joined computers, you can use Group Policy to configure the Work Folders URL. You can also use Group Policy to force the Work Folders client to be enabled instead of waiting for the user to start configuration.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 11-5a**Summary**

* In enterprise environments you need to use remote connectivity to manage and troubleshoot Windows 10 clients. You can use Remote Desktop, Remote Assistance, and Quick Assist to remote control clients. You can use MMC snap-ins, the registry editor, and Windows PowerShell remoting to remotely configure clients.
* To provide a consistent user environment for roaming users, you can use tools that store data in a central location. Mapped drive letters and folder redirection can be used to centralize data storage. Credential roaming, UE-V, and profile synchronization can be used to store settings centrally.
* VPNs provide secure remote access to network resources over the Internet. A VPN connection can use various protocols such as PPTP, L2TP, SSTP, or IKEv2. Always On VPN and DirectAccess provide automatic connectivity for remote users.
* Data synchronization is an important consideration for mobile clients to retain access to data when they don’t have network connectivity. OneDrive can synchronize data between a client and a cloud service. Offline files and Work Folders can synchronize data with a file server.

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 11-5b**Key Terms**

* [**Always On VPN**](javascript://)
* [**data synchronization**](javascript://)
* [**DirectAccess**](javascript://)
* [**Extensible Authentication Protocol (EAP)**](javascript://)
* [**folder redirection**](javascript://)
* [**Internet Key Exchange v2 Tunneling Protocol (IKEv2)**](javascript://)
* [**Layer 2 Tunneling Protocol (L2TP)**](javascript://)
* [**offline files**](javascript://)
* [**Point-to-Point Tunneling Protocol (PPTP)**](javascript://)
* [**Protected EAP**](javascript://)
* [**Quick Assist**](javascript://)
* [**Remote Assistance**](javascript://)
* [**Remote Desktop**](javascript://)
* [**Remote Desktop Connection**](javascript://)
* [**remote procedure calls (RPC)**](javascript://)
* [**Secure Socket Tunneling Protocol (SSTP)**](javascript://)
* [**User Experience Virtualization (UE-V)**](javascript://)
* [**virtual private network (VPN)**](javascript://)
* [**VPN Reconnect**](javascript://)
* [**Windows PowerShell remoting**](javascript://)
* [**Windows Remote Management (WinRM)**](javascript://)
* [**Work Folders**](javascript://)

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 11-5c**Review Questions**

1. You want to connect to a user desktop to review Windows 10 configuration settings when the user is not present. Which technology should you use?
   1. VPN
   2. Remote Desktop
   3. Windows PowerShell remoting
   4. Remote Assistance
   5. Quick Assist
2. Which of the following technologies allows you to access files from a Windows 10 computer that is not currently connected to a network (wired or wireless)? (Choose all that apply.)
   1. VPN
   2. Work Folders
   3. OneDrive
   4. Remote Desktop
   5. offline files
3. PPTP is the preferred VPN protocol. True or False?
4. Which of the following are authentication methods that can be used by IPSec? (Choose all that apply.)
   1. pre-shared key
   2. hash value
   3. certificates
   4. Kerberos
   5. NTLM
5. Which port numbers and packet types are relevant for allowing L2TP/IPSec through a firewall? (Choose all that apply.)
   1. TCP port 1723
   2. UDP port 4500
   3. TCP port 443
   4. IP protocol type 47 (GRE)
   5. IP protocol type 50 (ESP)
6. Which port numbers and packet types are relevant for allowing SSTP through a firewall?
   1. TCP port 1723
   2. UDP port 4500
   3. TCP port 443
   4. IP protocol type 47 (GRE)
   5. IP protocol type 50 (ESP)
7. Which VPN protocol supports the VPN Reconnect feature?
   1. PPTP
   2. L2TP/IPSec
   3. SSTP
   4. IKEv2
   5. DirectAccess
8. Which remote connectivity type automatically connects clients to the main office when they are roaming? (Choose all that apply.)
   1. PPTP
   2. Always On VPN
   3. SSTP
   4. IKEv2
   5. DirectAccess
9. Selecting a VPN type of Automatic is suitable for most VPN deployments. True or False?
10. Which automated method for VPN connection deployment would work best in combination with Microsoft Intune or Microsoft Endpoint Configuration Manager?
    1. CMAK
    2. Group Policy Preferences
    3. Windows Configuration Designer
    4. Windows PowerShell
11. EAP is a framework for implementing authentication protocols rather than an actual authentication protocol. True or False?

True

False

1. Which VPN authentication protocol uses SSL?
   1. PAP
   2. CHAP
   3. MS-CHAP v2
   4. EAP
   5. Protected EAP
2. When you configure a VPN connection, the VPN must be used as the default gateway. True or False?
3. Which technology, based on templates, allows you to synchronize application settings across multiple computers for domain users?
   1. mapped drive letters
   2. folder redirection
   3. credential roaming
   4. UE-V
   5. profile synchronization by using a Microsoft account
4. Which option for mstsc.exe prevents connection information from being cached on the local computer?
   1. /admin
   2. /shadow
   3. /restrictedAdmin
   4. /remoteGuard
   5. /public
5. Remote Desktop in Windows 10 allows multiple users to connect to one computer at the same time. True or False?
6. Which technology allows you to store user profile data, including documents, on a central file server instead of on the local disk?
   1. mapped drive letters
   2. folder redirection
   3. credential roaming
   4. UE-V
   5. profile synchronization by using a Microsoft account
7. Automatic configuration for Work Folders is based on the email address of the user. True or False?
8. Which command can you use to configure Windows PowerShell remoting on a computer running Windows 10?
   1. winrm quickconfig
   2. Enter-PSSession
   3. Set-WSManQuickConfig
   4. VPN\_Profile.ps1
   5. Enable-PSRemoting
9. You want to connect to a user desktop and have the user demonstrate a problem that they are having. Which technology should you use?
   1. VPN
   2. Remote Desktop
   3. Windows PowerShell remoting
   4. Remote Assistance
   5. Quick Assist

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)

# Chapter Review

## 11-5d**Case Projects**

**Case Project 11-1**

### Data for Traveling Users

Hyperactive Media Sales needs to provide a remote access solution for its traveling salespeople. They have a server running Windows Server 2019 that can be configured as a remote access server for VPN connectivity. You have been reviewing the VPN protocols that are available and need to decide on the best protocol. The traveling salespeople often stay in hotels, so firewall compatibility is a serious concern. Which VPN protocol has the best compatibility with firewalls

**Case Project 11-2**

### Managing Mobile Computers

Big Bob’s Construction has many construction sites where computers running Windows 10 Pro are located. At the remote sites, Internet connectivity can be of poor quality and intermittent. Because the computers are onsite and have poor connectivity to the main office, they are not currently domain joined, although they could be if required.

You want to be able to manage the computers at the construction sites. Which technology can allow you to do this and not force users to reconnect constantly?

**Case Project 11-3**

### Managing Enterprise Clients

Gigantic Life Insurance has a centralized help desk that supports users in multiple physical locations. The computers in company-owned buildings are domain joined and are running Windows 10. Sales agents are also in independent offices with computers running Windows 10 that are not domain joined. The independent offices don’t have direct connectivity to the Gigantic Life Insurance network.

When users call in to the help desk with problems, they often have trouble describing the issue accurately. You need the ability to view the user desktop as the user demonstrates the problem. You’d like to standardize on a single tool for this purpose. Which tool should you select, and why?

Go to pg.

[**help**](javascript://)

Application Opened

[Main content](https://ng.cengage.com/static/nbreader/ui/apps/nbreader/fullbook.html?#header)