Application Opened

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

**Module**

**10**

**Enterprise Computing**

* Chapter Introduction
* **10-1**Active Directory
	+ **10-1a**Active Directory Structure
	+ **10-1b**Active Directory Partitions
	+ **10-1c**Active Directory Sites and Replication
	+ **10-1d**Active Directory and DNS
	+ **10-1e**Joining a Domain
	+ **10-1f**Time Synchronization
	+ **10-1g**Offline Domain Join
* **10-2**Group Policy
	+ **10-2a**Group Policy Inheritance
	+ **10-2b**Group Policy Preferences
	+ **10-2c**Multiple Local Policies
	+ **10-2d**Controlling Device Installation
* **10-3**Enterprise Management Tools
	+ **10-3a**Windows Server Update Services
	+ **10-3b**Microsoft Endpoint Configuration Manager
	+ **10-3c**Microsoft BitLocker Administration and Monitoring
* **10-4**Enterprise File Services
	+ **10-4a**Distributed File System
	+ **10-4b**BranchCache
* **10-5**Microsoft Cloud Services
	+ **10-5a**Azure AD
	+ **10-5b**Azure AD Join
	+ **10-5c**Microsoft Intune
* **10-6**Chapter Review
	+ **10-6a**Summary
	+ **10-6b**Key Terms
	+ **10-6c**Review Questions
	+ **10-6d**Case Projects

Go to pg.

**help**

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**Understand Active Directory
* **2**Use Group Policy to control Windows 10
* **3**Describe enterprise management tools for Windows 10
* **4**Configure enterprise file services for Windows 10
* **5**Describe Microsoft cloud services

In the computer industry, the term enterprise is used to describe large companies with needs that are different from smaller companies. Enterprise products typically have much better features for manageability than those used by smaller companies. Enterprise deployments of Windows 10 have unique challenges that need to be addressed.

In this module, you learn how Active Directory and Group Policy can be used to manage hundreds or thousands of Windows 10 computers. Enterprise management tools for Windows 10 can also be used to deploy software and configure Windows 10 computers in large environments. You’ll also learn how enterprise file services differ from simple file sharing. Finally, Microsoft cloud services and how they are used by enterprises is described.

Go to pg.

**help**

Application Opened

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

**10-1**Active Directory

Microsoft includes Active Directory as a centralized directory service that can be used to control a network of Windows computers. When you implement a domain-based network by using Active Directory, you enable centralized management that is much more scalable than a workgroup-based network. To allow for centralized management, computers running Windows 10 are joined to the domain, and a computer account is created in the domain. User accounts are also managed centrally in the domain, rather than on each computer.

A **domain controller** is a server that holds a copy of Active Directory information. Domain controllers are responsible for authenticating users when they sign in to a workstation. After users are authenticated, they can access network resources. Domain controllers also respond to requests for other domain information, such as printer information or application configuration.

**Note 1**

Microsoft rebranded several services under the Active Directory name and uses the term Active Directory Domain Services (AD DS) to refer to what was previously known as Active Directory. The term Active Directory is still commonly used by IT professionals and is used throughout this book.

Go to pg.

**help**

Application Opened

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

## 10-1aActive Directory Structure

The key feature of Active Directory is a **domain**. A domain has a central security database that is used by all computers that are members of the domain. This central database means that user accounts can be created once in the domain and then used to sign in at any workstation in the domain. No matter which workstation the user signs in at, the user gains access to all the appropriate network resources. There are no concerns about synchronizing passwords because only one central account is used.

In addition to user account information, domains also store information about computers. Each computer that is a member of the domain has an account in Active Directory. Information about applications and printers is also found in Active Directory. DNS information is often stored in Active Directory, too.

Active Directory uses the same naming convention for domains and objects contained in these domains as DNS. For example, an Active Directory domain can be named [GiganticLife.com](http://giganticlife.com/%22%20%5Ct%20%22_blank). Active Directory domains and DNS domains, however, contain very different content. Many organizations use the same DNS domain name for Active Directory and the Internet email, but it is not required.

### Organizational Units

Each domain can be subdivided into **organizational units (OUs)**. Using OUs allows you to organize the objects in a domain. For example, you can organize the users in a domain by department by creating an OU for each department. This makes it easier to find the user accounts that you are looking for. Figure 10-1 shows how OUs are displayed when using the Active Directory Users and Computers administrative tool on the server.

**Figure 10-1Active Directory Users and Computers**





OUs can also be used for delegating management permissions. For example, you can delegate the capability of creating and managing objects in the Marketing OU to an administrator assigned to the Marketing department. That administrator will not be able to create and manage objects in the OUs of other departments.

Finally, OUs are used to apply group policies. Group policies can be applied to a specific OU, which applies Group Policy settings to the user accounts or computer accounts in the OU. For example, you could create a group policy with marketing-specific settings and apply it to the Marketing OU.

### Trees and Forests

In most cases, a single domain subdivided into OUs is sufficient to manage a network; however, you can create more complex Active Directory structures by combining multiple domains into a tree and multiple trees into a **forest**. Figure 10-2 shows a single Active Directory forest with two trees. The domains using [ad.GiganticLife.com](http://ad.giganticlife.com/%22%20%5Ct%20%22_blank) are one tree and the domains in [EnormousLife.com](http://enormouslife.com/%22%20%5Ct%20%22_blank) are another tree. Europe.ad.GiganticLife and Asia.ad.GiganticLife are subdomains of [ad.GiganticLife.com](http://ad.giganticlife.com/%22%20%5Ct%20%22_blank).

**Figure 10-2Domains, Trees, and Trusts**





When multiple domains exist in a forest, trust relationships are automatically generated among the domains. This allows administrators to give users in one domain access to resources in another domain.

### Server Roles

Within Active Directory, Windows servers can be either member servers or domain controllers. Member servers are integrated into Active Directory and can participate in the domain by sharing files and printers with domain users. Windows 10 computers integrate into Active Directory in the same way as member servers. Windows 10, however, is a desktop operating system and is not able to function as either a member server or a domain controller.

**Activity 10-1**

### Installing a Domain Controller

**Time Required:**1.5 hours

**Objective:**Install a Windows Server 2019 domain controller

**Description:**To create a single centralized security database, you must have a computer running Windows Server configured as a domain controller. In this activity, you install Windows Server 2019 and configure the server as a domain controller.

**Note 2**

The preferred method for implementing this activity is for students to have their own virtual machines in an isolated environment. Client Hyper-V can be used for the server installed in this activity; however, you can use a single server shared by multiple students. In such a case, you need to modify the activities slightly to ensure that each student is not affecting other students. Some parts, such as this activity, must be demonstrated.

1. 1

Place the Windows Server 2019 DVD in the computer and start it.

1. 2

Press a key to boot from the DVD when prompted.

1. 3

In the Windows Setup window, click **Next** to accept the default language, time, and keyboard settings.

1. 4

Click **Install now**.

1. 5

If necessary, on the Activate Windows screen, click **I don’t have a product key**. This screen does not appear when you install the evaluation version of Windows Server 2019.

1. 6

On the Select the operating system you want to install screen, click **Windows Server 2019 Standard Evaluation (Desktop Experience)** and click **Next**. This name will not include the word Evaluation if you are using volume license media.

1. 7

On the Applicable notices and license terms screen, select the **I accept the license terms** check box and then click **Next**.

1. 8

On the Which type of installation do you want screen, click **Custom: Install Windows only (advanced)**.

1. 9

On the Where do you want to install Windows screen, if any preexisting partitions exist, delete them all, click **Drive 0 Unallocated Space**, and then click **Next**. The install proceeds and will reboot.

1. 10

In the Customize settings window, in the Password and Reenter password boxes, type **Passw0rd** (0 is zero) and then click **Finish**.

1. 11

Sign in to your server as **Administrator** with a password of **Passw0rd**.

1. 12

In the Networks area, click **Yes** to make the server discoverable and then wait for Server Manager to start.

1. 13

In the Server Manager dialog box, select the **Don’t show this message again** check box and then close the dialog box.

1. 14

In Server Manager, in the navigation pane, click **Local Server**.

1. 15

Next to Ethernet, click **IPv4 address assigned by DHCP, IPv6 enabled**.

1. 16

Right-click **Ethernet** and then click **Properties**.

1. 17

In the Ethernet Properties window, click **Internet Protocol Version 4 (TCP/IPv4)** and then click **Properties**.

1. 18

In the Internet Protocol Version 4 (TCP/IPv4) Properties window, click **Use the following IP address** and then enter an IP address, subnet mask, and default gateway assigned by your instructor. This server needs to be on the same IP network as the client you will be connecting to it.

1. 19

In the Preferred DNS server box, type **127.0.0.1** and then click **OK**. This server will be configured as a DNS server.

1. 20

In the Ethernet Properties window, click **Close**.

1. 21

Close the Network Connections window.

1. 22

Next to Computer name, click the computer name.

1. 23

In the System Properties window, on the Computer Name tab, click **Change**.

1. 24

In the Computer Name/Domain Changes window, in the Computer name box, type **DC** and then click **OK**. If your environment is coexisting with other students, obtain a unique name from your instructor.

1. 25

In the Computer Name/Domain Changes dialog box, click **OK**.

1. 26

In the System Properties window, click **Close**.

1. 27

In the Microsoft Windows dialog box, click **Restart Now**.

1. 28

Sign in to your server as **Administrator** with the password of **Passw0rd**.

1. 29

In Server Manager, click **Manage** and then click **Add Roles and Features**.

1. 30

In the Add Roles and Features Wizard, click **Next**.

1. 31

On the Select installation type screen, click **Role-based or feature-based installation** and then click **Next**.

1. 32

On the Select destination server screen, click **DC** and then click **Next**.

1. 33

On the Select server roles screen, select the **Active Directory Domain Services** check box.

1. 34

In the Add Roles and Features Wizard dialog box, click **Add Features**.

1. 35

On the Select server roles screen, click **Next**.

1. 36

On the Select features screen, click **Next**.

1. 37

On the Active Directory Domain Services screen, read the information and then click **Next**.

1. 38

On the Confirm installation selections screen, click **Install**.

1. 39

Wait a few minutes for installation to complete and then click **Close**.

1. 40

In Server Manager, click **Notifications** and then click **Promote this server to a domain controller**.

1. 41

In the Active Directory Domain Services Configuration Wizard, on the Deployment Configuration screen, click **Add a new forest**.

1. 42

In the Root domain name, type **ad.GiganticLife.com** and click **Next**. If your environment is coexisting with other students, obtain a unique name from your instructor.

1. 43

On the Domain Controller Options screen, in the Password and Confirm password boxes, type **Passw0rd** and then click **Next**.

1. 44

On the DNS Options screen, click **Next**.

1. 45

On the Additional Options screen, click **Next**. If your environment is coexisting with other students, obtain a unique name from your instructor.

1. 46

On the Paths screen, click **Next**.

1. 47

On the Review Options screen, read the information and then click **Next**.

1. 48

Wait for the prerequisite check to complete and then click **Install**.

1. 49

In the You’re about to be signed out dialog box, click **OK**.

1. 50

After the reboot, sign in as **AD\Administrator** with a password of **Passw0rd**. The first startup might take a few minutes.

**Caution**

This domain controller is suitable for use by a single student. If the domain controller is being shared by multiple students, you can enable the server as an RD Session Host to allow multiple students to connect simultaneously. Alternatively, you can have students install the Remote Server Admin Tools (RSAT) to perform Active Directory management tasks from Windows 10.

Go to pg.

**help**

Application Opened

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

## 10-1bActive Directory Partitions

Active Directory is not a single monolithic database with all the information about the network. To make Active Directory more manageable, it is divided into the domain partition, configuration partition, and schema partition:

* The **domain partition** holds the user accounts, computer accounts, and other domain-specific information. This partition is replicated only to domain controllers in the same domain.
* The **configuration partition** holds general information about the Active Directory forest. Also, applications, such as Exchange Server, use the configuration partition to store application-specific information. This partition is replicated to all domain controllers in the Active Directory forest.
* The **schema partition** holds the definitions of all objects and object attributes for the forest. This partition is replicated to all domain controllers in the Active Directory forest.

**Note 3**

Active Directory also contains application partitions, but they are outside the scope of this course.

One special case for replication of information in the domain partition is global catalog servers. A **global catalog server** is a domain controller that holds a subset of the information in all domain partitions. For example, a global catalog has information about all users in the entire Active Directory forest, but only some of the information that is available about the users in each domain. Global catalog servers are used to hold the membership of universal groups and by applications, such as Microsoft Exchange Server. Exchange Server uses global catalog servers to perform address book lookups and locate user mailboxes.

Go to pg.

**help**

Application Opened

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

## 10-1cActive Directory Sites and Replication

Active Directory uses multimaster replication. This means that Active Directory information can be changed on any domain controller and those changes will be replicated to other domain controllers. This process ensures that all domain controllers have the same information. Replication, however, is not immediate, and the amount of time required to replicate data depends on whether domain controllers are in the same site or different sites.

An **Active Directory site** represents a physical location in your network; however, Active Directory is not aware of physical locations, and sites are defined by IP subnets. As administrator, you create sites and define the IP subnets in each site. In most cases, you should create an Active Directory site for each physical location in your network. If you have fast (10 Mbps) and reliable WAN links, however, you can consider making separate physical locations part of the same site.

Within a site, Active Directory replication is uncontrolled. The replication process is completely automatic. When a change is made to an Active Directory object, the change replicates to all domain controllers in the site after five seconds.

Between sites, Active Directory replication is controlled by site links. By default, all replication is controlled by a single site link that allows replication to occur every 180 minutes, but this can be shortened to 15 minutes.

Go to pg.

**help**

Application Opened

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

## 10-1dActive Directory and DNS

One of the more common configuration problems in Active Directory networks is incorrect DNS configuration on servers and workstations. Proper configuration of DNS is essential for using Active Directory. Active Directory stores information about domain controllers and other services in DNS. Workstations use the information in DNS to find domain controllers in their local site and sign in.

Incorrect DNS configuration can result in:

* Slow user sign-ins
* Inability to apply group policies
* Failed replication among domain controllers

All domain-joined workstations and servers should be configured to use an internal DNS server. This ensures that all domain controllers register their information in the correct location and that all workstations have access to domain controller information. The internal DNS server can resolve Internet DNS records on behalf of clients, as well. An external DNS server that is provided by an Internet service provider is typically unable to accept dynamic registration of DNS records, which is required for Active Directory.

**Activity 10-2**

### Viewing Active Directory DNS Records

**Time Required:**10 minutes

**Objective:**View the DNS records for Active Directory

**Description:**Active Directory DNS records are used by Windows 10 to locate domain controllers and other domain services. In this activity, you use the DNS management tool console to view the DNS records registered by a domain controller.

**Caution**

If you are using a shared server, use Remote Desktop Connection to sign in to the domain controller from your Windows 10 computer or the DNS RSAT tool.

1. 1

Sign in to the DC as **AD\Administrator** with a password of **Passw0rd**.

1. 2

If necessary, click the **Start** button and then click **Server Manager**.

1. 3

In Server Manager, click **Tools** and then click **DNS**.

1. 4

In the left pane, expand **DC**, expand **Forward Lookup Zones**, and then click **\_msdcs.ad.GiganticLife.com**. This is the DNS domain that holds DNS records for Active Directory.

1. 5

Expand **\_msdcs.ad.GiganticLife.com**, expand **dc**, and then click **\_tcp**. Notice that [DC.ad.GiganticLife.com](http://dc.ad.giganticlife.com/%22%20%5Ct%20%22_blank) is listed for the \_kerberos and \_ldap services. These records are used by clients to find a domain controller for sign-in.

1. 6

Expand **Sites**, expand **Default-First-Site-Name**, and then click **\_tcp**. Notice that [DC.ad.GiganticLife.com](http://dc.ad.giganticlife.com/%22%20%5Ct%20%22_blank) is listed for the \_kerberos and \_ldap services in this Active Directory site.

1. 7

Close all open windows.

Go to pg.

**help**

Application Opened

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

## 10-1eJoining a Domain

When a workstation joins a domain, it is integrated into the security structure for the domain. Administration of the workstation can be performed centrally by using Group Policy. Also, domain administrators are automatically given the ability to manage the workstation.

The following security changes occur when a workstation joins a domain:

* The Domain Admins group becomes a member of the local Administrators group.
* The Domain Users group becomes a member of the local Users group.
* The Domain Guests group becomes a member of the local Guests group.

The process of joining a workstation to a domain creates a computer account. It is this computer account that allows the workstation to integrate with Active Directory. If the computer account is removed, the workstation can no longer be used to access domain resources by users with domain-based accounts.

By default, all domain users can create 10 computer accounts in Active Directory. To increase security, many organizations change this limit to zero and prevent standard users from joining computers to the domain. If your organization makes this change, then only users that are assigned the appropriate permissions can create computer accounts. A standard user can still join a computer to the domain if an administrator creates the computer account in Active Directory before the computer is joined to the domain. The pre-staged computer account needs to have the same name as the computer running Windows 10.

By default, a computer account changes its password in the domain every 30 days. This happens in the background automatically. If the computer operating system is restored, the password that is restored might be an old password, which prevents the computer from authenticating. At this point, Windows 10 might present a message indicating that the trust relationship with the domain has been lost. One way to fix this is to put the computer back in a workgroup and rejoin the domain.

You can also use the Test-ComputerSecureChannel PowerShell cmdlet. The Test-ComputerSecureChannel cmdlet reports the status of the trust relationship with the domain. If the trust relationship is broken, you can use the -Repair parameter to fix it.

**Activity 10-3**

### Joining a Domain

**Time Required:**15 minutes

**Objective:**Join Windows 10 to an Active Directory domain

**Description:**Joining a domain integrates Windows 10 into the security system for Active Directory. In this activity, you join a Windows 10 workstation to an Active Directory domain and view the security changes.

**Caution**

This activity can be performed with a physical computer or a virtual machine with Windows 10 installed. The computer must be on the same IPv4 network as the domain controller and must be using the domain controller for the DNS server. Make these changes before beginning the activity.

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 **Accounts** and then click **Access work or school**.

1. 4

On the Access work or school screen, click **Connect**.

1. 5

In the Microsoft account window, click **Join this device to a local Active Directory domain**.

1. 6

In the Join a domain window, in the Domain name box, type **ad.GiganticLife.com** and then click **Next**.

1. 7

Sign in as **Administrator** with a password of **Passw0rd**.

1. 8

On the Add an account screen, click **Skip**. This screen provides you the opportunity to give a domain user account administrator permissions if required.

1. 9

Click **Restart now**.

1. 10

Sign in to your computer as **AD\Administrator** with a password of **Passw0rd.** Be sure to include the domain name to ensure you don’t attempt to sign in as the local Administrator account.

1. 11

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

1. 12

In the Computer Management window, expand **Local Users and Groups**, click **Groups**, and then double-click **Administrators**.

1. 13

In the Administrator Properties window, verify that AD\Domain Admins has been added to the Administrators group and click **OK**.

1. 14

Double-click **Users**, verify that AD\Domain Users has been added to the Users group, and then click **OK**.

1. 15

Close the Computer Management window.

1. 16

Right-click the **Start** button and click **Windows PowerShell (Admin)**. You are not prompted by UAC because you are signed in as the domain administrator account.

1. 17

At the Windows PowerShell prompt, type **Test-ComputerSecureChannel** and then press **Enter**. The status True indicates that the trust relationship with the domain is working properly.

1. 18

Close the Windows PowerShell prompt window.

Go to pg.

**help**

Application Opened

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

## 10-1fTime Synchronization

Time synchronization is a critical part of Active Directory authentication. If the clock on a computer running Windows 10 is more than five minutes different from the domain controller, authentication to Active Directory fails. To ensure that time settings don’t prevent authentication, domain-joined computers synchronize their time with domain controllers. Time is synchronized at startup and periodically afterwards. The time synchronization is based on network time protocol (NTP).

Before a Windows 10 computer is domain-joined, it synchronizes time with [time.windows.com](http://time.windows.com/%22%20%5Ct%20%22_blank). This is a time server provided by Microsoft and available on the Internet. If the domain time and the time provided by [time.windows.com](http://time.windows.com/%22%20%5Ct%20%22_blank) are not within 5 minutes, you might need to manually set the time on the computer to match the domain to successfully join the domain. As a best practice, your domain should synchronize time with a time server on the Internet. This avoids potential time mismatches when joining a domain.

Time synchronization in Windows 10 is performed by the Windows Time service. This service is configured by setting registry key values, but you can view and modify the configuration by using w32tm.exe. If you need to force Windows 10 to resync time, the simplest method is restarting the Windows Time service.

**Tip**

To complete reset time synchronizations settings, run w32tm /unregister and then w32tm /register.

**Activity 10-4**

### View Time Synchronization Settings

**Time Required:**5 minutes

**Objective:**View time synchronization settings for Windows 10

**Description:**Accurate time synchronization is a critical part of Active Directory authentication. In this activity, you verify the configuration of time synchronization on a domain-joined Windows 10 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-Service W32Time** and then press **Enter**. Verify that the Windows Time service is running.

1. 4

To view help information for w32tm.exe, type **w32tm** and then press **Enter**. Scroll up and down to read the help information for w32tm.exe.

1. 5

To view the configuration of time synchronization, type **w32tm /query /configuration** and then press **Enter**. Verify that below [TimeProviders] the Type is set to NT5DS. The type NT5DS means that time is being obtained from a domain controller.

1. 6

To force Windows Time service to read new configuration settings, type **w32tm /resync /rediscover** and then press **Enter**.

1. 7

Close the Windows PowerShell prompt window.

Go to pg.

**help**

Application Opened

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

## 10-1gOffline Domain Join

In enterprise environments, sometimes a need arises to automate the domain join process and have it occur very quickly. The offline domain join process allows a Windows 10 computer to be joined to an Active Directory without ever directly communicating with the domain controller. This can also be required in high security environments where only domain-joined computers can connect to the local network.

**Note 4**

To see examples of using djoin.exe, see the Djoin page at [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/ff793312(v=ws.11)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/ff793312%28v%3Dws.11%29%22%20%5Ct%20%22_blank).

The high level steps to perform an offline domain join are as follows:

1. 1

Run djoin.exe on Windows Server with the /provision option to create a computer account and a blob file. The blob file contains authentication information for the Windows 10 computer.

1. 2

Copy the blob file to the Windows computer.

1. 3

Run djoin.exe on the Windows 10 computer with the /requestodj option to import the blob file.

1. 4

Reboot to apply the changes.

**Caution**

You can use only local users for authentication until a domain controller is reachable.

Go to pg.

**help**

Application Opened

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

# 10-2Group Policy

**Group Policy** is a feature integrated with Active Directory that can be used to centrally manage the configuration of a Windows 10 computer. You can use thousands of Group Policy settings to control almost any aspect of Windows 10, so many, in fact, that you shouldn’t browse through them to find something useful. Instead, you configure specific settings based on documentation that instructs you how to accomplish a task. Or, you might browse a specific category of Group Policy settings to see if anything can help you to accomplish a specific task.

**Note 5**

If you want to browse a list of Windows 10 Group Policy settings, download the Group Policy Reference Spreadsheet at [https://www.microsoft.com/en-us/download/101451](https://www.microsoft.com/en-us/download/101451%22%20%5Ct%20%22_blank).

The Group Policy settings used by Windows 10 are contained in a **Group Policy object (GPO)**. A GPO is a collection of registry settings applied to the Windows 10 computer. To apply GPO settings, the GPO is linked to an OU, Active Directory site, or domain. A GPO can also be applied locally to a single computer. Configuration of Group Policy Objects is performed with the Group Policy Management Console, as shown in Figure 10-3.

**Figure 10-3Group Policy Management**





The settings in a GPO are divided into user settings and computer settings. The user settings are applied to any user accounts in the OU to which the GPO is linked. Computer settings in the GPO are applied to any computer accounts in the OU to which the GPO is linked. In Figure 10-4, if Bob signs in to WS1, the user settings from the GPO linked to the Marketing OU and the computer settings from the GPO linked to the Head Office OU are applied.

**Figure 10-4Group Policy Application**



Windows workstations and member servers download Group Policy settings during startup and approximately every 90 minutes thereafter. If you are testing GPO settings, you can use the gpupdate utility to trigger faster Group Policy Object downloads and application. Domain controllers download Group Policy settings every 5 minutes.

**Activity 10-5**

### Creating a GPO

**Time Required:**15 minutes

**Objective:**Create and apply a Group Policy Object (GPO)

**Description:**You can create GPOs to control users and their workstations. In this activity, you create an OU, link a GPO to the OU, and verify that it is applied to your Windows 10 computer.

1. 1

If necessary, start DC and sign in as **AD\Administrator** with a password of **Passw0rd**.

1. 2

If necessary, start **Server Manager**.

1. 3

In Server Manager, click **Tools** and then click **Active Directory Users and Computers**.

1. 4

In the Active Directory Users and Computers window, expand **ad.GiganticLife.com** and then click **ad.GiganticLife.com**.

1. 5

Right-click **ad.GiganticLife.com**, point to **New**, and then click **Organizational Unit**.

1. 6

In the New Object - Organizational Unit dialog box, in the Name box, type **MyOU** and then click **OK**. If you are sharing the domain with other students, get a unique name for your OU from your instructor.

1. 7

Right-click **MyOU**, point to **New**, and then click **User**.

1. 8

In the New Object - User dialog box, in the First name box, type **Samantha**.

1. 9

In the Last name box, type **Lopez**.

1. 10

In the User logon name box, type **SLopez** and then click **Next**. If you are sharing the domain with other students, get a unique sign-in name from your instructor.

1. 11

In the Password and Confirm password boxes, type **Passw0rd**.

1. 12

Deselect the **User must change password at next logon** check box and then click **Next**.

1. 13

Click **Finish** and then close the Active Directory Users and Computers window.

1. 14

In Server Manager, click **Tools** and then click **Group Policy Management**.

1. 15

In the Group Policy Management window, expand **Forest:** **ad.GiganticLife.com**, expand **Domains**, expand **ad.GiganticLife.com**, and then click **MyOU**.

1. 16

Right-click **MyOU** and then click **Create GPO in this domain, and Link it here**.

1. 17

In the New GPO dialog box, in the Name box, type **MyOU-Policy** and then click **OK**. If you are sharing the domain with other students, get a unique GPO name from your instructor.

1. 18

In the Group Policy Management window, expand **MyOU**, right-click **MyOU-Policy** and then click **Edit**.

1. 19

In the Group Policy Management Editor window, browse to **\User Configuration\Policies\Administrative Templates\System\Ctrl+Alt+Del Options.**

1. 20

Double-click **Remove Task Manager**, click **Enabled**, and then click **OK**.

1. 21

Close all open windows.

1. 22

On your Windows 10 computer, sign in as **AD\Administrator** with a password of **Passw0rd**.

1. 23

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

1. 24

At the Windows PowerShell prompt, type **gpupdate** and then press **Enter**.

1. 25

Sign out and sign in as **AD\SLopez** with a password of **Passw0rd**.

1. 26

After the profile is ready, press **Ctrl+Alt+Delete**.

1. 27

Verify that Task Manager is not available and then sign out.

1. 28

Sign in as **AD\Administrator** with a password of **Passw0rd**.

1. 29

Press **Ctrl+Alt+Delete**, verify that Task Manager is an option, and then click **Cancel**.

Go to pg.

**help**

Application Opened

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

## 10-2aGroup Policy Inheritance

Group Policy Objects can be linked to the Active Directory domains, OUs, and Active Directory sites. In addition, each Windows 10 computer can have local Group Policy Objects. It is essential to understand the precedence given to each of these policies. For example, when a local policy configures the home page for Microsoft Edge as [http://www.microsoft.com](http://www.microsoft.com/%22%20%5Ct%20%22_blank) and a domain policy configures the home page for Microsoft Edge as [http://intranet](http://intranet/%22%20%5Ct%20%22_blank), which one is effective? The precedence determines what settings apply when there are conflicting settings between policies.

When a Windows computer starts, GPOs are applied in the following order:

1. Local computer
2. Site
3. Domain
4. Parent OU
5. Child OU

All the individual GPO settings are inherited by default. For example, a Group Policy setting on a parent OU is also applied to child OUs and to all users and computers in the child OUs. One computer or user can process many policies during startup and sign-in.

At each level, more than one GPO can be applied to a user or computer. If more than one GPO per container exists, the policies are applied in the order specified by the administrator. The following steps are used to determine which policy settings to apply:

1. 1

If no conflict exists, the settings for all policies are applied.

1. 2

If a conflict does exist, later settings overwrite earlier settings. For example, the setting from a domain policy overrides the setting from a local policy. This means that a child OU would be applied last and have the greatest priority by default.

1. 3

If the settings in a computer policy and user policy conflict, the settings from the computer policy are applied.

When you are troubleshooting Group Policy application, it can be difficult to track down which policies are being applied. You can generate an HTML report to identify which Group Policy Objects are being applied. Use gpresult /h report.html to generate the report.

**Activity 10-6**

### Generating a Report for GPO Troubleshooting

**Time Required:**5 minutes

**Objective:**Generate and view a report for GPO troubleshooting

**Description:**When Group Policy settings are not being applied as you think they should be, it can be difficult to identify why. The gpresult.exe command can be used to generate a report that shows which GPOs and specific settings are being applied. In this activity, you use gpresult.exe to generate a report and then view the contents of the report.

1. 1

Sign in to your Windows 10 computer as **AD\SLopez** with a password of **Passw0rd**.

1. 2

Right-click the **Start** button and then click **Windows Powershell**.

1. 3

At the Windows PowerShell prompt, type **gpresult /h report.html** and then press **Enter**.

1. 4

Type **.\report.html** and then press **Enter**. In Windows PowerShell you need to use .\ to refer to the current directory when attempting to run an app.

1. 5

Review the contents of the report. Notice that MyOU-Policy is an applied GPO. Also notice that no computer settings are reported because SLopez is not a local administrator and does not have the necessary permissions to view information about the computer.

1. 6

Close all open windows.

Go to pg.

**help**

Application Opened

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

## 10-2bGroup Policy Preferences

A typical Group Policy setting is applied to a computer and cannot be changed by the user, even if the user has full administrative privileges to the computer. **Group Policy Preferences** are pushed down to the computer as part of the same process as Group Policy settings; however, a Group Policy Preference can be changed by the user. For example, you can use Group Policy Preferences to configure power options, such as configuring the computer to sleep after 10 minutes of inactivity. The user can manually change this; however, the next time the computer is restarted, the Group Policy Preference is reapplied.

Group Policy Preferences provide a way to configure many Windows 10 features that might have been done with scripting in the past. Many organizations have replaced logon scripts with Group Policy Preferences. Some of the things you can configure with Group Policy Preferences include:

* ODBC data sources
* Enable and disable devices
* Printers
* Drive mappings
* Scheduled tasks
* Service configuration
* VPN and dial-up connections
* Registry keys

One of the unique features of Group Policy Preferences is the ability to target them. By using targeting, you can have a single Group Policy Object that provides different settings for different users. For example, you can configure a drive mapping that is applied only if you are a member of the Sales group.

**Activity 10-7**

### Configuring Group Policy Preferences

**Time Required:**15 minutes

**Objective:**Configure and test Group Policy Preferences

**Description:**One of the common tasks performed by sign-in scripts is creating drive mappings. Management of drive mappings can be simplified by using Group Policy Preferences to apply the drive mappings. In this activity, you create a file share and then create a drive mapping to that file share that is distributed by using Group Policy Preferences.

1. 1

If necessary, sign in to DC as **AD\Administrator** with a password of **Passw0rd**.

1. 2

If necessary, open **Server Manager**.

1. 3

In Server Manager, click **Tools** and then click **Computer Management**.

1. 4

In Computer Management, expand **Shared Folders** and then click **Shares**.

1. 5

Right-click **Shares** and then click **New Share**.

1. 6

In the Create A Shared Folder Wizard, click **Next**.

1. 7

In the Folder path box, type **C:\MyFolder** and then click **Next**. If you are sharing the domain with other students, obtain a unique folder name from your instructor.

1. 8

Click **Yes** in the dialog box to create the folder.

1. 9

On the Name, Description, and Settings screen, click **Next** to accept the default settings. Notice the Share path.

1. 10

On the Shared Folder Permissions screen, click **Customize permissions** and then click **Custom**.

1. 11

In the Customize Permissions window, with **Everyone** selected, select the **Allow Change** check box and then click **OK**.

1. 12

Click **Finish** and then click **Finish** again.

1. 13

On the taskbar, click **File Explorer** and browse to **C:\**.

1. 14

Right-click **MyFolder** and then click **Properties**.

1. 15

In the MyFolder Properties dialog box, click the **Security** tab and then click **Edit**.

1. 16

In the Permissions for MyFolder dialog box, click **Users (AD\Users)**, select the **Allow Modify** check box, and then click **OK** twice.

1. 17

Close the File Explorer window.

1. 18

In Server Manager, click **Tools** and then click **Group Policy Management**.

1. 19

In the Group Policy Management window, click **Group Policy Objects**, right-click **MyOU-Policy**, and then click **Edit**.

1. 20

In the Group Policy Management Editor window, below **User Configuration**, expand **Preferences**, expand **Windows Settings**, and then click **Drive Maps**.

1. 21

Right-click **Drive Maps**, point to **New**, and then click **Mapped Drive**.

1. 22

In the New Drive Properties dialog box, in the Location box, type **\\DC\MyFolder**.

1. 23

In the Drive Letter area, click **Use** and then select **S** in the drop-down list.

1. 24

Click the **Common** tab and review the options. Item-level targeting is the option used to apply preferences to specific groups of users.

1. 25

Click **OK**.

1. 26

Close all open windows.

1. 27

On your Windows 10 computer, sign in as **AD\SLopez** with a password of **Passw0rd**.

1. 28

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

1. 29

At the Windows PowerShell prompt, type **gpupdate** and then press **Enter**.

1. 30

After the Group Policy update is complete, close the Windows PowerShell prompt window.

1. 31

On the taskbar, click **File Explorer** and then click **This PC**. Notice that the S: drive is listed. If the S: drive is not listed, sign out and sign in again.

1. 32

Close the File Explorer window.

Go to pg.

**help**

Application Opened

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

## 10-2cMultiple Local Policies

In a nondomain environment, it can be useful to have different Group Policy settings applied to administrative and nonadministrative users. Typically, this functionality is useful when you are trying to set up a public computer that is locked down when signed in with a public account, but unlocked when signed in with an administrative user.

You can create a local GPO for any local group or local user. You cannot create a local GPO directly for domain users; however, a domain user can be a member of a local group, which has a local GPO. You select who a local GPO applies to in the Microsoft Management Console (MMC) when you are adding the Group Policy Object Editor snap-in, as shown in Figure 10-5. Creating a local GPO is typically done for special-purpose computers that are not connected to a domain.

**Figure 10-5Selecting a Local Group Policy Object**





Go to pg.

**help**

Application Opened

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

## 10-2dControlling Device Installation

In a security-conscious organization, there are often concerns about users having the ability to remove organizational data by using a USB drive. One of the ways you can mitigate that risk is by controlling device installation. You can use Group Policy to define specific device types that are allowed or not allowed on the computer.

**Note 6**

By default, restrictions on device installation do not apply to users with local administrator permissions.

### Identifying Devices

When a new device is installed in a Windows 10 computer, the operating system uses a device identification string and device setup class to properly install the new device. The **device identification string** is used to find an appropriate driver for the device. The **device setup class** controls how the device driver software is installed. Both the device identification string and the device setup class can be used when controlling the installation of devices.

A device often reports multiple device identification strings when queried by the operating system. A hardware ID is the most specific device identification string. When multiple hardware IDs are reported, there is typically one very specific hardware ID that includes make, model, and revision, then other less-specific hardware IDs, such as make and model. Figure 10-6 shows the hardware IDs for a disk drive.

**Figure 10-6Hardware IDs for a Disk Drive**



Including multiple hardware IDs in a device allows the best available driver to be installed from those that are available. From a device installation control perspective, you can use the more generic hardware IDs to control installation rather than the very specific ones.

Device setup classes are used during the installation process for a new device to describe how the installation should be performed. The device setup class identifies a generic type of device rather than a specific make or model. Each device setup class is identified by a globally unique identifier (GUID).

Some devices have multiple GUIDs defined if they are multifunction devices, such as scanner/fax/printer devices. The parent device (overall device) has one GUID, and other functions (scanner, fax, printer) each have their own GUID.

### Device Installation Group Policy Settings

Windows 10 includes Group Policy settings specifically to control device installation, as shown in Figure 10-7. They control which devices can and cannot be installed. Also, you can define a default option for whether users are allowed to install new devices. All of these settings are located in Computer Configuration\Policy\Administrative Templates\System\Device Installation\Device Installation Restrictions.

**Figure 10-7Device Installation Group Policy Settings**





### Removable Storage Group Policy Settings

Because access to removable storage is a concern for many organizations, there are additional Group Policy settings, as shown in Figure 10-8, which can be used to control access to different types of removable storage, rather than preventing installation. With these policy settings, you can deny read or write access to specific removable storage types. All of these settings are located in Computer Configuration\Policies\Administrative Templates\System\Removable Storage Access and User Configuration\Policy\Administrative Templates\System\Removable Storage Access.

**Figure 10-8Removable Storage Group Policy Settings**





In some cases, a reboot is required to enforce removable storage Group Policy settings. This is normally a problem only when a device is in use. In such a case, you can define how long the system waits to apply the changes before rebooting the system. Rebooting the system allows the policy changes to be applied.

**Activity 10-8**

### Controlling Device Installation

**Time Required:**15 minutes

**Objective:**Use Group Policy settings to control device installation

**Description:**Windows 10 includes a number of Group Policy settings to control the installation of devices and access to removable storage. In this activity, you use Group Policy settings to prevent the installation of any new disks, including portable storage devices, such as USB drives.

1. 1

On your Windows 10 computer, sign in as **AD\Administrator** with a password of **Passw0rd**.

1. 2

Right-click the **Start** button and then click **Device Manager**.

1. 3

In the Device Manager window, expand **Disk drives**, right-click a disk installed in your system, and then click **Properties**.

1. 4

In the disk Properties dialog box, click the **Details** tab, and in the Property box, select **Hardware Ids**. This displays the hardware IDs reported by your disk. Notice that the lowest value in the list is GenDisk. This is the least specific reference to your disk.

1. 5

Close all open windows.

1. 6

On DC, sign in as **AD\Administrator** with a password of **Passw0rd**.

1. 7

If necessary, open Server Manager.

1. 8

In Server Manager, click **Tools** and then click **Group Policy Management**.

1. 9

In Group Policy Management, right-click **MyOU-Policy** and then click **Edit**.

1. 10

In the Group Policy Management Editor, browse to Computer Configuration\Policies\Administrative Templates\System\Device Installation\Device Installation Restrictions.

1. 11

Select each Group Policy setting and read the description.

1. 12

Double-click **Prevent installation of devices using drivers that match these device setup classes**.

1. 13

In the Prevent installation of devices using drivers that match these device setup classes window, click **Enabled** and then click **Show**.

1. 14

In the Value box, type **GenDisk** and then click **OK**.

1. 15

In the Prevent installation of devices using drivers that match these device setup classes dialog box, click **OK**.

1. 16

Close all open windows.

Go to pg.

**help**

Application Opened

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

**10-3**Enterprise Management Tools

Larger organizations need automated tools to simplify management of their desktop computers. Group Policy is a useful tool for many tasks, but it doesn’t meet all the needs of large organizations. Three areas that often require additional tools are applying updates, deploying software, and managing BitLocker.

Go to pg.

**help**

Application Opened

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

## 10-3aWindows Server Update Services

**Windows Server Update Services (WSUS)** is a role included in Windows Server to manage the deployment of Windows updates to desktop computers and servers. WSUS downloads updates from Microsoft Update and stores them in a local datastore, rather than each client computer downloading updates individually. This is very efficient for network utilization because each update is downloaded only once and stored on the WSUS server.

Client computers are configured to contact a WSUS server for updates rather than contacting the Microsoft update service directly. This can be configured by editing the registry or by using a Group Policy object.

WSUS is significantly more flexible than automatic updates downloaded directly from Microsoft. You can organize computers into groups to control the update process and generate reports to view which computers have been updated and which have not. The ability to test updates before they are generally applied to workstations significantly reduces the risk of an update causing system downtime. You can also use WSUS to remove updates that have already been installed. The WSUS update process is shown in Figure 10-9.

**Figure 10-9WSUS Update Process**



The WSUS update process still relies on the client computers to trigger the installation of updates. After updates are approved for a specific computer, the update is downloaded by that computer from the WSUS server the next time Automatic Updates is triggered.

You can configure rules on the WSUS server to automatically approve some updates for specific computers. For example, you might want to automatically approve all updates for your test computers to reduce administrative work.

The updates downloaded automatically from Microsoft can be controlled by product, product family, update classification, and language. For example, you can choose to download only English updates or only critical updates. You can manually specify to download an update that is not configured to download automatically.

**Activity 10-9**

### Configuring Clients for WSUS

**Time Required:**10 minutes

**Objective:**Use Group Policy settings to configure clients to use WSUS

**Description:**After installing and configuring a WSUS server, you need to configure clients to use the WSUS server. In this activity, you use Group Policy settings to configure clients to use a WSUS server.

**Note 7**

This Activity performs only the steps required to configure the WSUS client, because configuring a WSUS server is outside the scope of the course.

1. 1

On DC, sign in as **AD\Administrator** with a password of **Passw0rd**.

1. 2

If necessary, open Server Manager.

1. 3

In Server Manager, click **Tools** and then click **Group Policy Management**.

1. 4

In the Group Policy Management window, right-click **MyOU-Policy** and then click **Edit**.

1. 5

In the Group Policy Management Editor, browse to **Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update**.

1. 6

Select each of the Group Policy settings and read the description.

1. 7

Double-click **Specify intranet Microsoft update service location**.

1. 8

In the Specify intranet Microsoft update service location dialog box, click **Enabled**.

1. 9

In the Set the intranet update service for detecting updates and Set the intranet statistics server text boxes, type **http://wsus.ad.GiganticLife.com** and then click **OK**. This step assumes that you have a Windows server with WSUS installed with the name [wsus.ad.GiganticLife.com](http://wsus.ad.giganticlife.com/%22%20%5Ct%20%22_blank).

1. 10

Close all open windows.

Go to pg.

**help**

Application Opened

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

## 10-3bMicrosoft Endpoint Configuration Manager

Many large organizations use **Microsoft Endpoint Configuration Manager** to help manage on-premises desktop computers that are domain-joined. In small organizations, it’s possible to configure computers manually or have a single standardized configuration. In large organizations, many different variations are required to support the needs of different user groups. Configuration Manager provides management flexibility for groups of users and computers.

**Tip**

Microsoft Endpoint Configuration Manager is part of Microsoft Endpoint Manager. This product was formerly known as System Center Configuration Manager.

You can use Configuration Manager to help with the following tasks:

* Desktop analytics, which includes hardware and software inventory
* Deploy updates for Windows operating systems and non-Microsoft apps
* App deployment with greater flexibility than Group Policy, including APPX and MSIX apps
* Operating system deployment with task sequences to perform complex configuration, including app deployment
* Manage BitLocker deployment

**Note 8**

For more information on Microsoft Endpoint Configuration Manager, see the product documentation at [https://docs.microsoft.com/en-us/mem/configmgr/](https://docs.microsoft.com/en-us/mem/configmgr/%22%20%5Ct%20%22_blank).

Go to pg.

**help**

Application Opened

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

## 10-3cMicrosoft BitLocker Administration and Monitoring

**Microsoft BitLocker Administration and Monitoring (MBAM)** is used to simplify the deployment and management of BitLocker. By default, BitLocker is enabled individually on each computer. There is no centralized management of BitLocker except for storage of recovery passwords in Active Directory. When you implement MBAM, you enable centralized deployment and monitoring of BitLocker.

To enable centralized management of BitLocker, you need to install the MBAM agent on each computer. After this is done, Group Policy settings are read and applied by the MBAM agent. The Group Policy settings are part of an .admx template that is part of MBAM. The .admx template allows you to configure the new Group Policy settings in a GPO.

To simplify recovery of encrypted drives, MBAM includes a self-service web portal to look up recovery keys. In some cases, this means that users will be able to perform their own recovery without needing to call support.

MBAM is part of the Microsoft Desktop Optimization Pack that is included with subscriptions to Windows 10 Education and Windows 10 Enterprise. This product has ceased development and is slated for retirement in 2026. For new deployments, you should use the BitLocker functionality in Configuration Manager.

**Tip**

The BitLocker management functionality in Configuration Manager can manage Windows 10 Pro. MBAM cannot manage Windows 10 Pro.

Go to pg.

**help**

Application Opened

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

**10-4**Enterprise File Services

The file-sharing functionality in Windows provides a high level of control for security but can be difficult to use in a large organization with multiple locations. In particular, if locations are connected by slow WAN links, opening files over those links is very slow. Distributed File System (DFS) and BranchCache help to mitigate this issue.

Go to pg.

**help**

Application Opened

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

## 10-4aDistributed File System

**Distributed File System (DFS)** is composed of DFS replication and DFS namespaces. DFS replication is used to synchronize data among file shares. DFS namespaces are used to virtualize access to shared folders and hide the true location of the shared folder. When you implement DFS, you can have multiple replicated copies of data and provide highly available access to that data. Figure 10-10 shows how DFS replication and DFS namespaces work together. The namespace \\[ad.GiganticLife.com](http://ad.giganticlife.com/%22%20%5Ct%20%22_blank)\Shares\Marketing points to two file shares with data replicated between them.

**Figure 10-10DFS folder with Multiple Targets**



Some scenarios for using DFS are:

* High availability in a single location—In this scenario, file shares are replicated between two servers in the same site. The namespaces point at both servers. If one server goes down, clients continue using the other server.
* Close data access among locations—In this scenario, file shares are replicated between two servers in different locations. The namespaces point at both servers. When users roam between the two sites, they automatically use the file share in the local location.
* Data backup off-site—In this scenario, file shares are replicated between two locations. The namespaces point at both servers. The file shares for remote users are backed up in the central location.

DFS replication is very efficient between locations. When a file is changed, only the changes to that file are replicated between the two servers.

Windows 10 includes DFS client software for accessing DFS namespaces. A DFS namespace appears to be a single, large file structure, but it can really be composed of shared folders on multiple servers. This allows administrators to change the location of file shares without impacting client computers. When the DFS namespace is updated, clients automatically begin using the new location.

You can customize the connection process, but by default, when a DFS namespace refers to multiple file shares (targets), the client is directed to a file share in the local Active Directory site. If multiple file shares are in the local Active Directory site, one file share is randomly selected. If connectivity to the first file share fails, the client connects to another available file share identified by the namespace.

The list of targets provided by a DFS namespace is known as a referral list. The order of targets in the referral list determines the order in which the client attempts to access the targets. If the target being used by a client becomes unavailable, the client switches over to another target almost immediately.

When changes are made to the list of targets, clients are not updated immediately. By default, clients cache the folder referral list for 30 minutes before refreshing it. If you remove a target from a folder, clients continue to use it until the cache for that folder is updated. Similarly, if you add a new target for a folder, the clients might not be informed for up to 30 minutes. You can change the cache time in the properties of a folder, but it is seldom required because changes to DFS namespaces are typically well planned and can be implemented over the span of a few hours or days. Figure 10-11 shows the properties of a folder in DFS Management.

**Figure 10-11DFS Folder Properties, Referrals Tab**



If Windows 10 connects to a nonoptimal target in a remote site due to a short-term error, Windows 10 remains connected to the nonoptimal target unless the Clients fail back to preferred targets option has been enabled on the folder. If this option is enabled, Windows 10 fails back to the preferred target at the next refresh. If the option is not enabled, you can cause clients to fail back by restarting, sleeping, or hibernating. As part of the Windows 10 startup process, the cache is cleared.

**Tip**

No interface for managing the DFS client in Windows 10 exists. The folder settings are retrieved from Active Directory.

Go to pg.

**help**

Application Opened

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

## 10-4bBranchCache

**BranchCache** is a file-caching technology for domain-joined computers in remote locations with slow WAN links. Files are stored in a file share in a central location but are cached at the remote site to make it faster to open the files. In addition to files in file shares, BranchCache can also cache data from web servers and application servers using Background Intelligent Transfer Service (BITS).

BranchCache has these two modes:

* Distributed cache mode—In this mode, each computer running Windows 10 maintains a cache and the computers in a single site share cache data. If a computer with cached data is turned off, other clients obtain the data from the file share over the slow WAN link.
* Hosted cache mode—In this mode, a Windows server is used as a central cache by all computers in the remote site. This maximizes the availability of cached data because the server will always be on.

When you open a file that has been cached, BranchCache verifies with the server hosting the file share that the file has not been modified since it has been cached. If the file has not been modified, it is opened from the cache. If the file has been modified, it is opened from the file share over the WAN link. This process ensures that an out-of-date file is never used, but it also means that if the WAN link is down, cached data cannot be accessed. Saving a file is always done back to the file share and the cache.

In most cases, you enable BranchCache on clients by using a GPO. It is possible, however, to manually enable BranchCache and view BranchCache configuration by using the netsh command and Windows PowerShell cmdlets. To view the Windows PowerShell cmdlets available for managing BranchCache, run Get-Command \*-BC\*.

**Caution**

BranchCache is available only in the Enterprise and Education editions of Windows 10.

**Activity 10-10**

### Configuring Clients for BranchCache

**Time Required:**10 minutes

**Objective:**Use Group Policy settings to configure clients to use BranchCache

**Description:**To use BranchCache, it needs to be enabled on the client and the server hosting the data. To enable clients to use BranchCache, you use Group Policy settings. In this activity, you enable clients to use BranchCache in distributed cache mode.

**Note 9**

This activity does not configure the server hosting data for BranchCache because it is outside the scope of this course.

1. 1

On DC, sign in as **AD\Administrator** with a password of **Passw0rd**.

1. 2

If necessary, open Server Manager.

1. 3

In Server Manager, click **Tools** and then click **Group Policy Management**.

1. 4

In Group Policy Management, right-click **MyOU-Policy** and then click **Edit**.

1. 5

In the Group Policy Management Editor, browse to **Computer Configuration\Policies\Administrative Templates\Network\BranchCache**.

1. 6

Click each setting and read the description.

1. 7

Double-click **Turn on BranchCache**, click **Enabled**, and then click **OK**.

1. 8

Double-click **Set BranchCache Distributed Cache mode**, click **Enabled**, and then click **OK**.

1. 9

Close all open windows.

Go to pg.

**help**

Application Opened

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

# 10-5Microsoft Cloud Services

Many organizations are starting to use cloud-based applications and services, including device management. **Cloud services** are available over the Internet using infrastructure provided by the vendor. In general, using cloud services is simpler to manage than deploying the same service on-premises. To deploy a new service on-premises, you need to purchase and maintain hardware, install operating systems, install apps, and maintain apps. When you use cloud-based services, all those tasks are the responsibility of the vendor.

Another key benefit of cloud services is availability over the Internet. To allow access to on-premises apps from the Internet requires complex security configurations in an on-premises data center. A cloud service is available over the Internet automatically with no additional configuration.

Microsoft is a large vendor in the cloud services space. Some of the cloud services available from Microsoft are listed in Table 10-1 below.

**Table 10-1**

### Microsoft Cloud Services

| **Service** | **Description** |
| --- | --- |
| Microsoft Azure | Provides online hosting of virtual machines and services for applications, such as storage and databases. Services and virtual machines hosted in Azure can be securely integrated with on-premises networks. |
| Office 365 Enterprise | This is a suite of cloud-hosted services that includes email (Exchange Online), file storage (SharePoint Online and OneDrive for Business), collaboration (Microsoft Teams), and online versions of Office apps. Some licensing plans also include the desktop version of Microsoft Office Suite (Microsoft 365 Apps). |
| Microsoft 365 Business | This suite of cloud-hosted services includes similar functionality to Office 365 Enterprise, but it is focused on small organizations of up to 300 users. Some plans include the desktop version of Microsoft Office Suite. These plans do not include Windows 10 Enterprise. |
| Microsoft 365 Enterprise | This suite of cloud-hosted services includes all the features in Office 365, along with additional security features and Windows 10 Enterprise. |

For smaller organizations, using cloud services is an easy way to get complex services for a minimal cost. For example, a small business can buy five licenses for Microsoft 365 Business and start using all the features right away without ever hiring IT staff or purchasing servers. Then, if the organization grows, they can easily purchase additional licenses as required.

Even larger organizations benefit from cloud services. They can increase capacity without expanding their data center. They also have the option to cut costs by reducing the number of licenses that they purchase for the month. This means that a seasonal business can expand capacity in the busy season and then reduce capacity in the slower season.

Go to pg.

**help**

Application Opened

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

## 10-5aAzure AD

Azure AD is the online directory service used for Microsoft cloud services. To give a user access to Office 365 or Microsoft 365, you create a user account in Azure AD and then assign the appropriate license. Similar to Active Directory on-premises, you can also create groups to organize users.

Small organizations often have cloud-only user accounts in Azure AD. These are user accounts that exist only in Azure AD and are not synchronized with on-premises Active Directory. This is suitable for very small organizations that don’t have on-premises Active Directory or don’t want the complexity of synchronizing user accounts from Active Directory to Azure AD.

Larger organizations synchronize user accounts from Active Directory into Azure AD. This simplifies the logon process for users because they have the same user name and password for the cloud services as they use on-premises with Active Directory. Administrators install Azure AD Connect on a Windows server to perform directory synchronization.

Go to pg.

**help**

Application Opened

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

## 10-5bAzure AD Join

In the same way that you can join a computer to Active Directory, you can join a computer to Azure AD. After a device is Azure AD-joined, it can be managed by using services integrated with Azure AD. The most common tool for management is Microsoft Intune.

In small organizations, users might join their device to Azure AD manually based on instructions provided by the IT department or Microsoft. Larger organizations can automate the process during initial system setup or by using a provisioning package.

Azure AD join is designed for devices that are not joined to Active Directory. This can be used by small organizations for centralized management. Azure AD join is also useful for larger organizations that have devices that seldom connect to the corporate network, for example, sales staff that are outside the office. Users sign into an Azure AD-joined device by using an Azure AD account.

**Note 10**

For more information about Azure AD join, see Azure AD-joined devices at [https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join](https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join%22%20%5Ct%20%22_blank).

If your organization has services that rely on Active Directory, but you also want to introduce cloud-based management, you can configure Windows 10 as hybrid Azure AD-joined. In this configuration, the computer running Windows 10 is joined to Active Directory and Azure AD.

**Tip**

If your Azure AD-joined computer has BitLocker enabled, the BitLocker recovery key is automatically backed up to Azure AD.

Go to pg.

**help**

Application Opened

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

## 10-5cMicrosoft Intune

**Microsoft Intune** is a cloud-based management solution that is integrated with Azure AD. This service is included as part of Microsoft Endpoint Manager to manage mobile devices while Configuration Manager is used to manage on-premises devices. Microsoft Intune is also available as a stand-alone service. In many ways, Microsoft Intune is a cloud-based version of Configuration Manager but can manage Android and iOS devices in addition to Windows 10 devices.

The tasks that you perform with Windows 10 devices by using Microsoft Intune include:

* Deploy and update apps
* Manage Windows updates
* Deploy profiles for VPN, certificates, email, and Wi-Fi
* Enforce policies, like those provided by Group Policy
* Enable and disabled device features
* Reset or wipe devices
* Monitor and manage anti-malware status (including Windows Defender)

**Note 11**

To see what the management portal for Windows Intune looks like, see Tutorial: Walkthrough of Microsoft Intune in the Azure portal at [https://docs.microsoft.com/en-CA/mem/intune/fundamentals/tutorial-walkthrough-intune-portal](https://docs.microsoft.com/en-CA/mem/intune/fundamentals/tutorial-walkthrough-intune-portal%22%20%5Ct%20%22_blank).

To support communication between Windows 10 and Microsoft Intune, you need to install the client software for Microsoft Intune. Administrators can download the client from the administration portal and provide it to users, but it’s typically more convenient for users to install it from the Microsoft Store. In the Microsoft Store, the app is called Company Portal.

**Note 12**

For a video that shows the Company Portal installation process, see Enroll your Windows 10 Device in Microsoft Intune at [https://youtu.be/TKQxEckBHiE](https://youtu.be/TKQxEckBHiE%22%20%5Ct%20%22_blank).

Go to pg.

**help**

Application Opened

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

# Chapter Review

## 10-6a**Summary**

* Active Directory is a database of network information about users, computers, and applications. A network based on Active Directory is far more scalable than workgroup-based networks. The components of Active Directory are domains, OUs, trees, and forests.
* Servers in an Active Directory domain can be either domain members or domain controllers. A domain member is integrated into the security structure of the domain. A domain controller holds a copy of the Active Directory information for the domain.
* Active Directory is composed of a domain partition, configuration partition, and schema partition. The replication of the information in each partition is controlled by Active Directory sites.
* Clients use DNS to locate domain controllers. If DNS is not configured properly, client performance suffers and group policies may not be applied.
* Group Policy is used to configure and control workstations. Group Policy settings are stored in Group Policy Objects. The order of application for Group Policy Objects is: local, site, domain, parent OU, and child OU. If a conflict occurs, the last applied policy has the highest priority. Multiple local policies can be created.
* You can use Group Policy settings to control device installation and the use of removable storage devices. Both of these enhance the ability of organizations to control data leaving the organization.
* Enterprise environments need additional tools to help manage Windows 10 computers. Commonly used management tools include WSUS, Configuration Manager, and MBAM.
* Enterprise environments often use advanced file services functionality. DFS is used to replicate file shares and virtualize access to the file shares with namespaces. BranchCache is used to speed up file access in remote locations.
* Microsoft provides cloud services that are used by small organizations and large enterprises. Azure AD stores user and computer identities. Microsoft Intune is used to manage devices.

Go to pg.

**help**

Application Opened

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

# Chapter Review

## 10-6b**Key Terms**

* **Active Directory site**
* **BranchCache**
* **cloud services**
* **configuration partition**
* **device identification string**
* **device setup class**
* **Distributed File System (DFS)**
* **domain**
* **domain controller**
* **domain partition**
* **forest**
* **global catalog server**
* **Group Policy**
* **Group Policy object (GPO)**
* **Group Policy Preferences**
* **Microsoft BitLocker Administration and Monitoring (MBAM)**
* **Microsoft Endpoint Configuration Manager**
* **Microsoft Intune**
* **organizational units (OUs)**
* **schema partition**
* **Windows Server Update Services (WSUS)**

Go to pg.

**help**

Application Opened

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

# Chapter Review

## 10-6c**Review Questions**

1. Which type of server is used to sign in clients that are joined to an Active Directory domain?
	1. domain controller
	2. member server
	3. global catalog server
	4. Azure AD server
2. Which type of server holds some of the domain information for all domains in the forest?
	1. domain controller
	2. member server
	3. global catalog server
	4. Azure AD server
3. Which Active Directory partitions are replicated to all domain controllers in the Active Directory forest? (Choose all that apply.)
	1. domain partition
	2. configuration partition
	3. schema partition
	4. global catalog partition
4. The  partition contains the definition of the objects and their attributes that can exist in Active Directory.
5. Which network service is used by workstations to find domain controllers?
	1. Active Directory
	2. DHCP
	3. DNS
	4. NetBIOS
6. Group Policy can be used to distribute software to a Windows 10 computer. True or False?
7. Approximately how often does a Windows 10 computer download Group Policy Objects?
	1. every 5 minutes
	2. every 90 minutes
	3. only at shutdown
	4. only at startup
8. Which Group Policy setting location has the lowest priority and will always be overridden by other GPOs when there is a conflict?
	1. Local
	2. Site
	3. Domain
	4. Parent OU
	5. Child OU
9. Which Windows technology requires an agent to be installed?
	1. DFS
	2. BitLocker
	3. MBAM
	4. BranchCache
10. A DFS folder can have a maximum of two targets. True or False?
11. Group Policy Preferences can be overridden by users. True or False?
12. By default, how long do DFS clients cache the referral list for a folder?
	1. 30 seconds
	2. 5 minutes
	3. 15 minutes
	4. 30 minutes
	5. 90 minutes
13. Which methods can you use to fix a Windows 10 computer that has a broken trust relationship with the domain? (Choose all that apply.)
	1. Move the workstation to a workgroup and then rejoin the domain.
	2. Run Repair-ComputerTrust.
	3. Run dism /rejoin.
	4. Synchronize the time with the domain controller.
	5. Run Test-ComputerSecureChannel -Repair.
14. After a computer has been joined to a domain, all domain users can sign in to that computer. True or False?
15. Which tool or command can you use to view time synchronization settings in Windows 10?
	1. Computer Management
	2. WinTime.exe
	3. w32tm.exe
	4. Get-TimeConfig
	5. Event Viewer
16. Which management tools can you use to approve the deployment of Windows Updates to computers? (Choose two.)
	1. WSUS
	2. BranchCache
	3. Configuration Manager
	4. Group Policy
	5. DFS
17. Which enterprise file system allows you to create duplicate copies of files for high availability?
	1. WSUS
	2. BranchCache
	3. Configuration Manager
	4. Group Policy
	5. DFS
18. Which cloud service can you use to deploy software to Windows 10 computers?
	1. Microsoft Intune
	2. Configuration Manager
	3. Azure AD
	4. Microsoft 365
	5. Group Policy
19. Companies can synchronize users from Active Directory into Azure AD. True or False?
20. Which tool or utility can you use to perform an offline domain join?
	1. dism.exe
	2. djoin.exe
	3. Group Policy
	4. w32tm.exe
	5. Azure AD

Go to pg.

**help**