- 1. 4. 4. Managing Windows 10 in business -

Using a domain-based network

In this unit we have described setup, configuration, and usage of peer-to-peer (or workgroup) networks.

This is the type of network most commonly found in homes and small businesses, and it does not require a server; each computer on the network is an equally empowered peer.

Windows 10 Pro, Enterprise, and Education editions can also be configured in an Active Directory domain.

The traditional Active Directory domain-based network requires at least one computer running a version of Windows Server.

This is sometimes called on-premises Active Directory to differentiate it from a newer, cloud-based alternative called Azure Active Directory (Azure AD).

Both variants of Active Directory provide identity and access services, allowing users to sign on to any cloud or on-premises web application using a wide variety of devices, and to sign on to domain-joined devices.

All computers and user accounts on the network can be centrally managed through the server or through a web-based Azure AD dashboard.

An on-premises domain controller offers full, policy-based management capabilities.

Azure AD, in its current incarnation, provides a more limited set of management tools.

When you have more than a handful of computers in a network, they become much easier to manage when configured as a domain.

If you use a business-focused Microsoft cloud service such as Office 365 or Microsoft Dynamics CRM (among others), your subscription already includes Azure AD.

Managing computers with Group Policy

Group Policy lets administrators configure computers throughout sites, domains, or organizational units.

In addition to setting standard desktop configurations and restricting what settings users are allowed to change, administrators can use Group Policy to centrally manage software installation, configuration, updates, and removal; specify scripts to run at startup, shutdown, sign in, and sign out; and redirect users' profile folders (such as Documents) to network server drives.

Administrators can customize all these settings for different computers, users, or groups.

In a domain environment, Group Policy enables an administrator to apply policy settings and restrictions to users and computers (and groups of each) in one fell swoop.

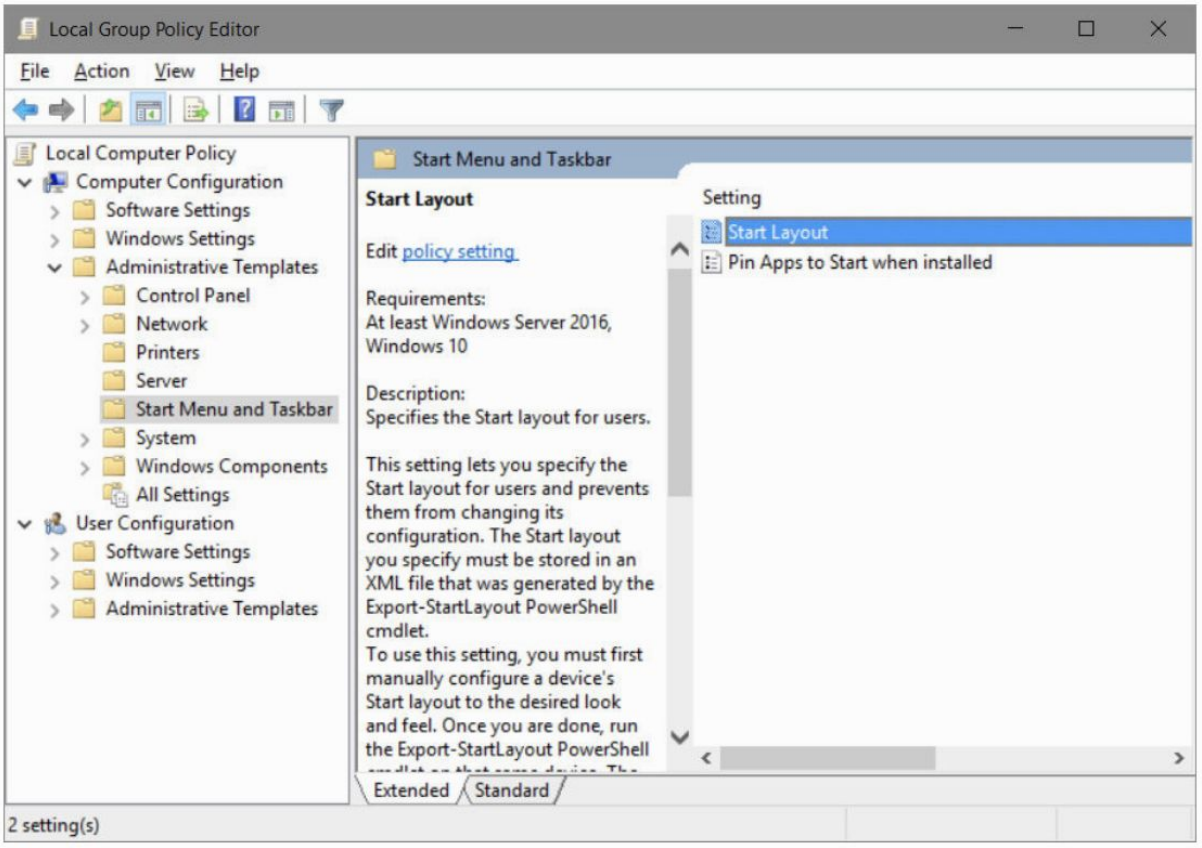
With a workgroup, you must make similar Group Policy settings on each computer where you want such restrictions imposed.

Nonetheless, Group Policy can be a useful tool for managing computers on a small network or even for managing a single computer.

Using Local Group Policy Editor

To begin exploring Group Policy, in the Start search box type **"group policy"** and then tap or click **"Edit Group Policy"**.

As shown in the next image, Local Group Policy Editor appears in the familiar Microsoft Management Console format.



The Computer Configuration branch of Group Policy includes various computer-related settings, and the User Configuration branch includes various user-related settings.

The line between computer settings and user settings is often blurred, however.

Your best bet for discovering the policies you need is to scan them all.

You'll find a treasure trove of useful settings, including many that can't be made any other way short of manually editing the registry.

In the Administrative Templates folders, you'll find several hundred computer settings and even more user settings, which makes this sound like a daunting task—but you'll find that you can quickly skim the folder names in Local Group Policy Editor, ignoring most of them, and then scan the policies in each folder of interest.

To learn more about each policy, simply select it in Local Group Policy Editor.

If you select the Extended tab at the bottom of the window, a description of the selected policy appears in the center pane.

The policy setting shown in the previous figure controls one aspect of Start.

Many more policies—most of them located in User Configuration > Administrative Templates > Start Menu And Taskbar—manage all manner of Start details, such as the appearance of suggestions and most-used apps in the app list on Start.

You can download a comprehensive list of all policy settings from the Administrative Templates folder, in Microsoft Excel format, by visiting https://bit.ly/group-policy-settings .

The list is huge—thousands of entries—but you can use Excel to sort, filter, or search the list to find policy settings of interest.

The list also provides other details about each setting, such as the scope of the setting (machine or user), the registry value it controls, and whether a setting change requires a sign-off or reboot to take effect.

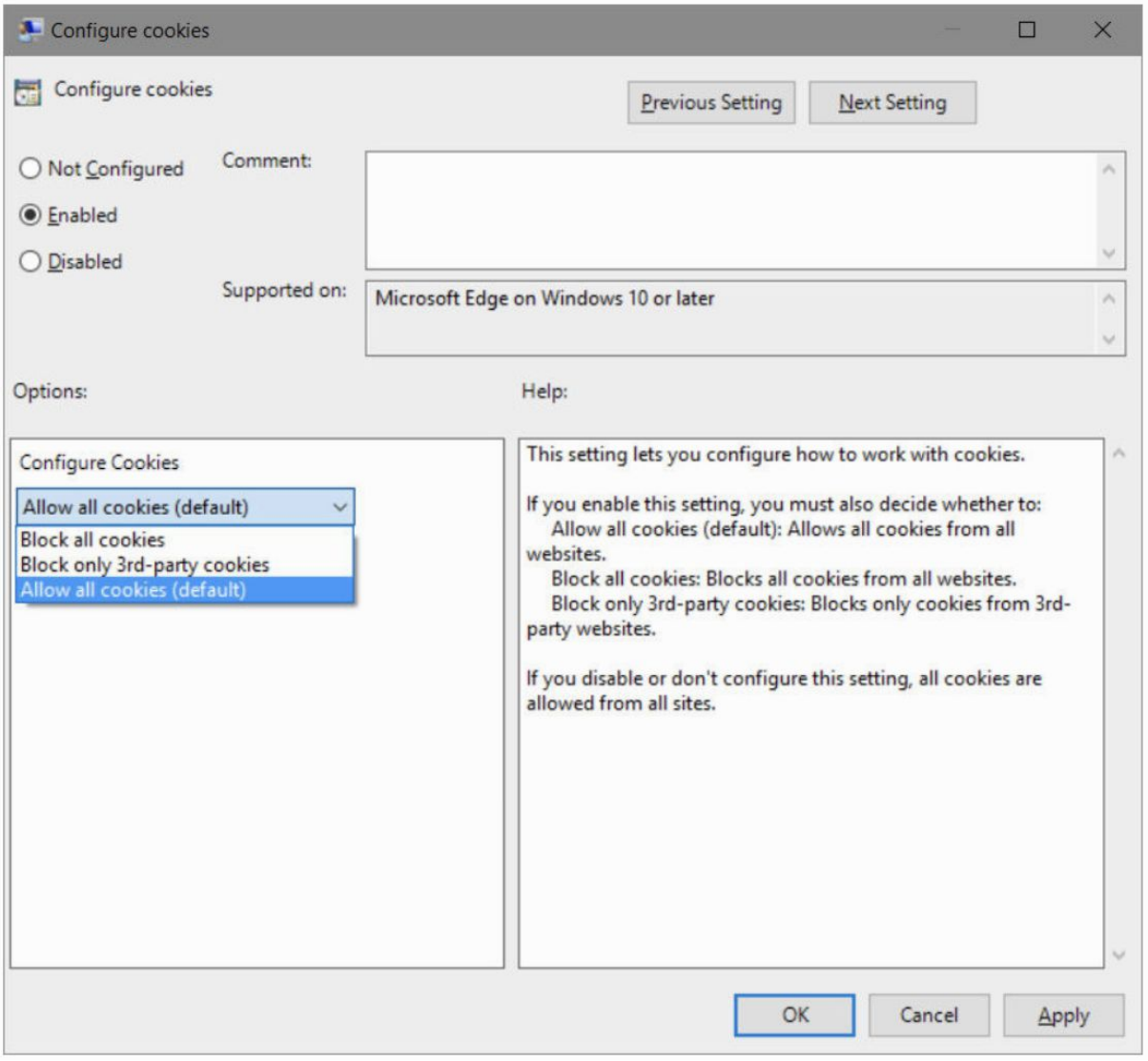
Changing policy settings

Each policy setting in the Administrative Templates folders has one of three settings: Not Configured, Enabled, or Disabled.

By default, all policy settings in the local Group Policy objects are initially set to Not Configured.

To change a policy setting, in Local Group Policy Editor, simply double-click the name of the policy setting you want to change or click the Policy Setting link that appears in the center pane of the Extended tab.

A dialog box then appears:



Beside the settings option buttons is a large area where you can write a comment.

The Help pane below this Comment area includes detailed information about the policy setting (the same information that appears in the center pane of the Extended tab).

The pane to the left of the Help pane offers options relevant to the current policy.

Previous Setting and Next Setting buttons make it convenient to go through an entire folder without opening and closing individual dialog boxes.

Managing updates

In earlier versions of Windows, updates, fixes, and feature improvements were offered as an ever-growing collection of individual updates.

This approach meant you could pick and choose which updates to install.

But it also meant you were sometimes faced with installing scores of updates (and performing multiple reboots), especially when updating a machine that hadn't been used for a few months.

Servicing options for Windows

That all changes with Windows 10, which receives so-called quality updates, to fix security and reliability issues, in cumulative packages.

When you install the latest cumulative update, it retrieves all the updates you need and applies them en masse.

If you use Windows 10 Home edition, that's pretty much the end of the story: security and reliability updates, as well as major upgrades (called feature updates) such as version 1607 (Anniversary Update), are installed automatically at the first opportunity.

With other Windows editions, you might have the ability to choose among these servicing options:

- The first option is available for those who want to be ahead of the curve. The Windows Insider Program delivers updates before they're distributed to the masses. Insider Preview builds allow you to get an early look at new features, test them, and provide feedback to Microsoft—but it also means you install software that hasn't been as widely tested and might cause severe problems. If you want to be a guinea pig, go to Settings > Update & Security > Windows Insider Program.
- Current Branch (CB). With CB, security updates and feature upgrades are pushed to your computer automatically. This is the default setting for all retail Windows editions.
- Current Branch for Business (CBB). Under CBB, only definition updates are installed immediately. Security, reliability, and driver updates can be postponed for up to 30 days to allow time for testing before deployment throughout your organization. Feature updates are not even offered to CBB clients until they've been road tested by CB clients for a period of time—at least four months. Even then, installation of feature updates can be deferred for up to eight months. Because CBB allows for controlled rollout of both quality and feature updates over a longer period of time, it's often the best option for the majority of users in an organization. CBB is available only on Pro, Enterprise, and Education editions of Windows 10. Deferring updates for CBB is most easily done with Windows Update for Business, which we describe in the next section.
- Long Term Servicing Branch (LTSB). Each LTSB release includes the usual monthly security and reliability updates, but no new features are added for up to 10 years. LTSB is not intended for general-purpose workstations; rather, it's targeted at specialized devices (such as manufacturing control systems or point-of-sale systems) that run mission-critical applications and where high reliability is the primary goal. For this reason, LTSB editions lack several

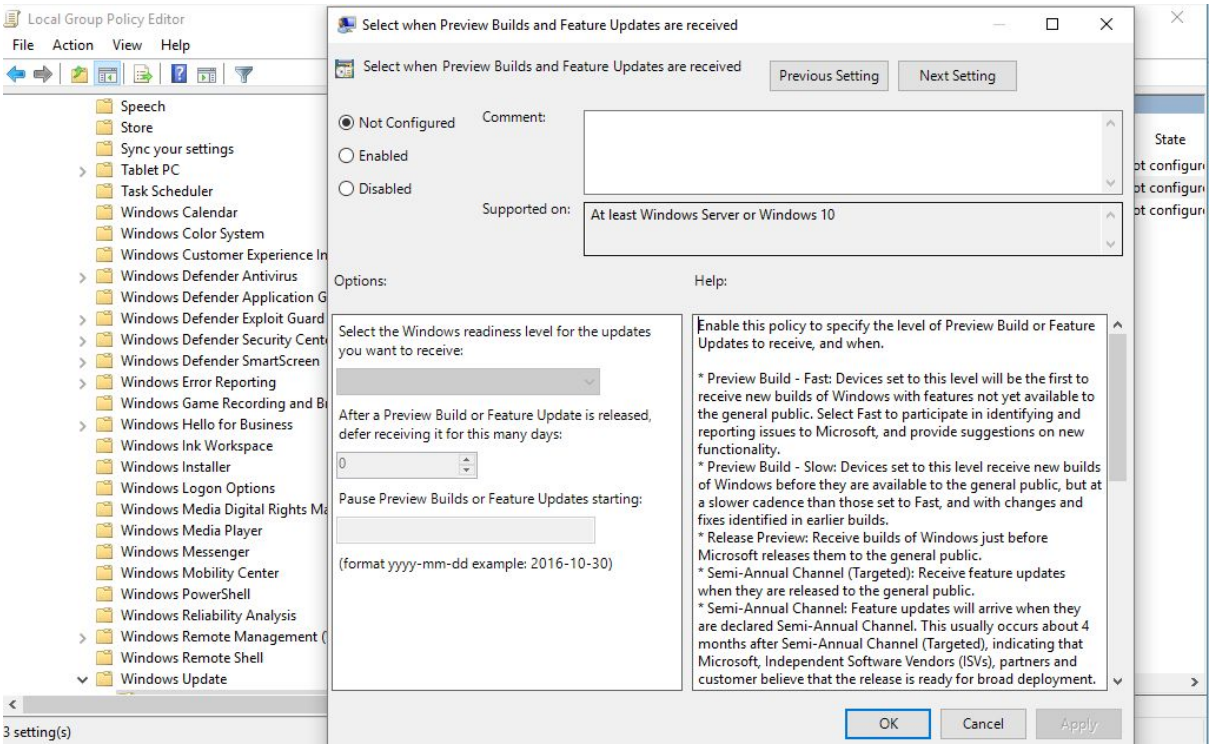
Windows components that are included in other editions, including Windows Store, Microsoft Edge, Cortana, and the built-in universal apps such as Mail, Weather, Photos, Alarms & Clock, and Groove Music. LTSB is a licensing option for Windows 10 Enterprise and is available only for customers with a Volume License agreement. Because you don't get feature updates with LTSB, the only way to get a new Windows version is to pay for a new license (unless you have Software Assurance) and upgrade to a newer LTSB release when it's available.

Using Windows Update for Business

Windows Update for Business is a set of configuration options for the free Windows Update service that allows users of Windows 10 Pro, Enterprise, and Education editions to defer most updates and upgrades.

You configure Windows Update for Business through Group Policy.

In Windows 10, you'll find the policy settings in Computer Configuration > Administrative Templates > Windows Components > Windows Update > Windows Update for Business.



You have 3 entries:

- Manage preview builds: this is for enabling or disabling the possibility of using the Windows Insider Program, in order to get Windows updates before the general public.

- Select when Preview Builds and Feature Updates are received: this is for selecting if you want to be part of the Windows Insider Program (to get Windows updates before the general public), or if you want to use the Current Branch for Business (to defer Windows updates). You can modify the time when you will get Preview Builds and Feature Updates, depending on the option you choose.
- Select when Quality Updates are received: with this option you can defer Quality Updates for up to 30 days.

- Vocabulary -

- to defer: retrasar en el tiempo.

- Exercises - 1. 4. 4. Managing Windows 10 in business -

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

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

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

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

1. Download a list with all the Group Policy settings and check it out.
2. Go to the Windows search box, type “gpedit.msc” and open the “Local Group Policy Editor”. Check this console and navigate through the different sections.
3. Which are the 4 servicing options for managing Windows updates?
4. In the”Local Group Policy Editor”, go to Computer Configuration -> Administrative Templates -> Windows Components -> Windows Update -> Defer Windows Updates. Here you can choose to defer Windows Updates. Deferments can be indicated using days. Or you can select the checkbox labeled “Pause feature (or quality) updates”, which will turn them off until the next big update rolls around.