

I'm not a bot



























At times, you need administrator privileges to make some changes on your computer, but you don't know if you have admin rights. Here is how to check if you have administrator privileges using 4 different but easy methods. Try this free data recovery software to rescue files under any circumstances: MiniTool Power Data Recovery is specially designed to recover files from HDDs, SSDs, USB flash drives, memory cards, SD cards, etc. If you want to recover your lost, deleted, or formatted files, you can try this software. Even if your computer is unbootable, you can use this software to recover your files and then fix the system. MiniTool Power Data Recovery FreeClick to Download100%Clean & SafeHow to Check if You Have Admin Rights on Windows 11/10?Many operations on a Windows computer require you to have administrator privileges. For example, you need to have local admin rights to install Office or you need administrator permissions to delete a file or folder. You need to log into your PC using the administrator account if you want to have admin rights. However, you may be not sure if you have admin rights. In this post, MiniTool Software will introduce some easy ways to tell you how to check if you are an administrator and what to do if you don't have administrator privileges to make changes on your PC. Way 1: Check If You Are an Administrator Using Control PanelStep 1: Click the search icon in the taskbar and search for Control Panel, then select Control Panel from the search results to open it. Step 2: Go to User Accounts > User Accounts. Step 3: Check if you are an administrator from the right section. Way 2: Check If You Have Administrator Privileges in SettingsOn Windows 10Step 1: Press Windows + I to open Settings. Step 2: Go to Accounts > Your info and check if you are an administrator under the user profile image. On Windows 11Step 1: Press Windows + I to open Settings. Step 2: Click the User profile image or click Accounts from the left menu. Step 3: Check if you are logged in as an administrator. Way 3: Check if You Have Admin Rights Using Command PromptStep 1: Press Windows + R to open Run. Step 2: Type cmd into the Run dialog and press Enter. This will open Command Prompt. Step 3: Type net user username into Command Prompt and press Enter. You need to replace username with your username in the command. Then, you can see if you are an administrator in the line of Command Prompt. Local Group Memberships. If your account belongs to the Administrator group, it should have administrator privileges. Way 4: Check if You Have Admin Rights in Computer ManagementStep 1: Right-click Start and select Computer Management. Step 2: Go to Computer Management > Local Users and Groups > Users. Step 3: Double-click the user name and you will see the Properties interface. Step 4: Switch to the Member of tab and see if you are a member of administrators. If yes, it means you have administrator privileges. Want to know if you are an administrator on Windows? You can use one of these 4 ways in this post to check. Besides, if you encounter issues when using MiniTool software like MiniTool Power Data Recovery, you can contact us via [email protected]. MiniTool Power Data Recovery FreeClick to Download100%Clean & Safe Don't know if you have admin rights in Windows? You can find it easily. Here's how to check if your user account has admin rights. You can create two types of user accounts in Windows, i.e., a Standard and Administrator user account. As the name implies, the administrator user account will have administrative privileges, whereas the regular user account will not. Generally, while setting up Windows for the first time, the first user account you create is an administrator account. After that, Windows will automatically default to a Standard user account, i.e., any subsequent user accounts you create will have Standard user rights. A system administrator can manually assign admin rights to a Standard user account when necessary. You must use an administrator account to perform specific actions like installing applications, changing system settings, installing updates, etc. If you are unsure whether you have administrative rights in Windows, you may quickly check. So, without further ado, let me share with you ways to check if you have admin rights in Windows. The steps below work the same in Windows 10 and 11. Table of contents:As you might have expected, you can check if you have admin rights from the Settings app. Here's how to do it. Open the Settings app. Click "Accounts" on the sidebar. Go to the "Your info" page. You will see the account type at the top, right under the user account name. If it says "Administrator," then you have admin rights. Steps with more details: Use the "Windows key + I" keyboard shortcut to open the Settings app. You can also search for the same in the Start menu. After opening the Settings app, click "Accounts" on the sidebar and go to the "Your info" page. As the name suggests, this page shows all the information regarding your user account. You will see your user account type at the top, right under the user name. If it says "Administrator," the user account has admin rights. We can use the net user command to get the user account details, i.e., know if your user account has administrative privileges. Here is how to use the command. Right-click the Start menu. Choose "Windows Terminal (Admin)." Execute the net user command. Take a look at the "Local group memberships" line. If it says "Administrators," then you have admin rights. Exit the terminal application. Steps with more details: First, we must open the terminal application. Right-click the Start menu and choose the "Windows Terminal (Admin)" option. On Windows 10, you can select the "Windows PowerShell (Admin)" option. In the terminal window, execute the below command. Replace with the actual username of the account. net user The terminal window lists the details of the user. Take a look at the "Local group memberships" line. If it says "Administrators," your user account has admin rights. —That is all. It is that simple to check if you have admin rights in Windows 10 and 11. I hope this simple and easy Windows how-to guide helped you. If you are stuck or need some help, send an email, and I will try to help as much as possible. If you're wondering how to check if you have admin rights on Windows 11, it's a straightforward process. You'll need to access the User Accounts settings through the Control Panel or Settings menu. This article will walk you through each step, ensuring that you can determine your administrative status quickly and easily. In this section, we're going to guide you through the steps to check if you have admin rights on Windows 11. By following these steps, you'll be able to confirm whether your user account has the necessary permissions to make system changes. Click on the Start button in the lower-left corner of your screen. Accessing the Start Menu is your gateway to all the settings and applications on your Windows 11 device. This step is crucial because it allows you to navigate to the necessary settings. Type "Settings" into the search bar and click on the app when it appears. The Settings application is where you'll find various options to manage your Windows 11 device. It's a centralized hub for your system preferences. Within the Settings app, click on the "Accounts" option. Accounts is the section where you can manage all user accounts on your device. It contains information about each user's role, including admin rights. Under Accounts, select "Your info" to see details about your user account. This step is essential because "Your info" provides a summary of your account type and rights. It's like looking at a snapshot of your profile on the system. Check if it mentions "Administrator" under your account name. If "Administrator" is listed, you have admin rights. If not, you're likely using a standard user account with limited permissions. Once you've completed these steps, you'll know if you have admin rights on your Windows 11 device. This information is vital for understanding what changes you can make to your system. Use Control Panel: You can also check your admin rights by navigating to Control Panel > User Accounts > User Accounts. Command Prompt: Open Command Prompt and type net user %username% to see detailed account information. User Account Control: Try performing a task that requires admin rights, such as installing software, to see if you're prompted for an admin password. Settings Shortcut: Use the Windows key + I shortcut to open Settings quickly. Admin Accounts: If you're not an admin, consider asking someone who is to change your account type. Admin rights allow a user to make changes to system settings, install software, and manage other user accounts. Only an existing admin can change your account type to admin. Admin rights are needed for tasks that affect the entire system, like installing software or changing security settings. Check the list of user accounts under Settings > Accounts > Family & other users to see who has admin rights. If you need admin rights, you'll have to request them from an existing admin on your device. Open the Start Menu. Open Settings. Navigate to Accounts. Click on Your info. Check Account Type. Knowing how to check if you have admin rights on Windows 11 is a fundamental skill for managing your computer effectively. Admin rights grant you the ability to make significant changes to your system, ensuring you can install necessary software, adjust settings, and maintain your device securely. If you find that you don't have admin rights, consider reaching out to someone who does. This way, you can request the necessary permissions to perform your tasks. Always exercise caution when using an admin account, as improper changes can affect system stability. For further guidance on managing Windows 11, keep exploring our articles and tutorials. The more you know, the better you can maintain and optimize your device. Matthew Burleigh has been writing tech tutorials since 2008. His writing has appeared on dozens of different websites and been read over 50 million times. After receiving his Bachelor's and Master's degrees in Computer Science he spent several years working in IT management for small businesses. However, he now works full time writing content online and creating websites. His main writing topics include iPhones, Microsoft Office, Google Apps, Android, and Photoshop, but he has also written about many other tech topics as well. Read his full bio here. To check whether your account has admin rights from the Settings app, go to the Accounts page and you shall see "Administrator" below the username if it is an administrative account. To check if your account is part of the Administrators group, run the command "Net User [username]" in Command Prompt while replacing [username] with the actual username. You may need administrative privileges from time to time when operating a Windows computer. Admin rights allow you to perform certain tasks on the computer that otherwise aren't allowed to people logged in from all user accounts, like installing or uninstalling apps, running programs with elevated privileges, and making changes to the system in general. Before performing a vital task, you should check whether the user account you are currently logged on from has administrative rights or not. This will prevent mid-way interruptions and prompts telling you that you have insufficient rights. Not all Windows user accounts have administrative rights. While the first-ever account is automatically created with administrative privileges, the built-in Administrator account is disabled by default. Admin accounts are those that are part of the "Administrators" group. Any user account member of this group will automatically inherit the group's policies, allowing them to perform actions that require elevated privileges. With administrative rights, you can perform the following tasks which a standard account cannot: The Administrator account has full control of the files, directories, services, and other resources on the local device. Create other local users, assign user rights, and assign permissions. The Administrator account can take control of local resources at any time by changing the user rights and permissions. Run apps with elevated permissions without using the "Run as Administrator" option. Install and uninstall system-wide applications. Change Group Policies and Windows Registry. Make changes to other user accounts. Change system security settings. And this is just the tip of the iceberg. As a developer or an advanced user, you will find that having administrative rights helps in getting a job done without encountering privilege and access errors. Press the Windows key + I to open the Settings app. Go to Accounts. Check account type from Settings app. Here, you will see what type of account you are currently logged in from below your account name. Press the Windows key + R to open the Run Command box. Type in "control" and press Enter to launch the Control Panel. Click "User accounts." Open user accounts in Control Panel. Click "User Accounts" again. Click User Accounts again. On this page, you will find what type of account you are currently using, and whether or not it has administrative privileges. Check type of user account from the Control Panel. The Local Users and Groups manager is a Microsoft Management Console used to manage exactly what it names; the user accounts and the groups. Here is how it can be used to check whether your account or another account has administrative rights: Press the Windows key + R to open the Run Command box. Type in "lusrmgr.msc" and press Enter to open the Local Users and Groups management console. Click "Users" from the left navigation pane. Double-click the account you want to check the status of in the middle section. Open user properties from Local Users and Groups. In the properties window, switch to the "Member of" tab. Now check if the user account is a member of the "Administrators" group. Check type of user account from the Local Users and Groups console. If you find that the user is not a part of the Administrators group, it means that the account does not have admin rights. You can also check if your account has administrative privileges from the Command Prompt with a single, simple command. Here are the steps: Press the Windows key + R to open the Run Command box. Type in "cmd" and press Enter to launch the Command Prompt. Now execute the following command while entering the username of the account to check its status: Net User [username] / Check if account has admin rights from Command Prompt. By running this command, you will also be able to see the groups the user account is a member of. If it is a member of the "Administrators" group, it means that the account has administrative rights. You can also verify if your current user account has administrative rights or not using PowerShell. This is a two-part command that checks whether your account is part of the Administrators group. To check whether your user account is part of the Administrators group, you must run the following script in PowerShell. Note that you do not need to run PowerShell with elevated rights to execute this command. if ((Get-LocalGroupMember -Group "Administrators" | Select -ExpandProperty Name) -contains "\$env:ComputerName;\$env:USERNAME") { Write-Host "Your account is an Administrator account." } else { Write-Host "Your account is a Standard account." } Check whether account has administrative rights using Windows PowerShell. Running this tiny script in PowerShell will tell you whether your account is a member of the Administrators group or not. If it is, it will output "Your account is an Administrator account." Of course, you can change what the script shows at the end before running it. Knowing whether your account has administrative rights is important, especially before performing critical system tasks that could turn fatal for the OS if not done correctly. Imagine you are in the middle of replacing critical system files and midway you are prompted that you do not have enough privileges. This is why we have compiled a list of methods to check whether your user account has sufficient privileges, and is part of the local Administrators group so that you can check it before beginning your tasks. Want to know how to check if your user account is an administrator account or not? This guide will show you whether your Windows 11 user account is an administrator account or a standard user account. As you likely know, Windows 11 supports both standard and administrator accounts. An administrator account or a user account with admin rights can install programs, create and delete user accounts, and make changes to Windows 11 operating system at their will. However, a standard user account does not allow you to do all these. Now that you know the difference between a standard and administrator user account, it's time to understand how to check if your Windows 11 user account is an admin account or not. Method 1 of 4 Check if your Windows 11 user account is an administrator account via the Settings app Step 1: Open the Settings app. On the left side, click Accounts. Step 2: Now, on the right side, the user account details will appear. An "Administrator" text near your user name indicates that your user account is an administrator account or your user account has admin rights. Method 2 of 4 Check if you have admin rights in Windows 11 via Settings Step 1: Open the Settings app. Click on the Accounts in the left pane and then click Your info on the right side. Step 2: The resulting page (Settings > Accounts > Your info) shows your user account details. If your account has admin rights, an Administrator word will appear below your user account name. Method 3 of 4 Check if you have administrator rights in Windows 11 via Control Panel Step 1: Use search to open the classic Control Panel. Step 2: Change the Control Panel View to Small icons (refer to the picture below). Step 3: Next, click the User Accounts link. Step 4: The resulting window displays your user account name, account picture, and account details. If your account is an administrator account, you will see the "Administrator" word right below your user account name. Method 4 of 4 Use PowerShell or Command Prompt to know if your Windows 11 account is an administrator account Step 1: Open the Command Prompt, PowerShell, or Terminal. Step 2: Next, type the net user accountname command and then hit the Enter key. Please note that, in the above command, you need to replace the "accountname" with your actual user account name. So, for instance, if your account name is Test, the command would be net user Test. Step 3: The Local Group Memberships field tells you your Windows 11 user account type. You will see either Administrators or Users here. Windows 11, the latest operating system from Microsoft, comes with a host of features and improvements over its predecessor, Windows 10. One of the critical aspects of managing a Windows system is understanding user permissions, particularly administrative rights. Users typically require admin rights to install software, modify system settings, or perform advanced troubleshooting tasks. This article will guide you through various methods to check if you have admin rights in Windows 11, providing step-by-step instructions, illustrations, and tips to enhance your understanding of user permissions. Understanding Admin Rights Before diving into how to check for admin rights, let's clarify what administrative rights are and why they matter. In Windows systems, users can have different permission levels. There are mainly two types: Standard User: This account type can perform everyday tasks, such as running applications and managing personal settings. However, standard users cannot install software or make system-wide changes without administrative approval. Administrator: Administrators have full control over the system. This user type can install software, change security settings, manage user accounts, and access all files on the system. They can also grant or revoke permissions to others. Having admin rights is crucial, especially for users who need to install applications, run system utilities, or troubleshoot various issues. Now that we understand the importance of admin rights, let's explore several methods to check if your account has these rights in Windows 11. Method 1: Using the Settings App The easiest way to check your account status in Windows 11 is through the Settings app. Step-by-Step Guide Open the Settings App: Click on the Start button (the Windows logo) in the taskbar or press the Windows + I keys simultaneously. Navigate to Accounts: In the Settings window, click on Accounts from the left-hand menu. Check Your Account Type: Under the "Your info" section, you will see your account name and type. If it says "Administrator," you have admin rights. Conversely, if it shows "Standard User," you do not. Tips If you're unsure which account type your account is, click on "Family & other users." Here, you can see the accounts under your management and their respective types. For more detailed information about your account, including permissions and group memberships, you may want to explore other methods. Method 2: Using User Accounts Settings Another method to check your user permissions is by accessing the User Accounts settings. Step-by-Step Guide Open Run Dialog: Press Windows + R on your keyboard to open the Run dialog box. Launch User Accounts: Type netplwiz and press Enter. This command will bring up the User Accounts window. Review Account Type: In the User Accounts window, you will see a list of users. Highlight your account name and check the "Group" column. If it says "Administrators," you have admin rights. Important Note This method is particularly useful for those managing multiple accounts. You can see not only your rights but also which other users have admin rights on the system. Method 3: Using Command Prompt For users who prefer using the command line, you can check your account privileges via Command Prompt. Step-by-Step Guide Open Command Prompt: Click on the Start button, type cmd, and press Enter. Alternatively, you can press Windows + X and select Windows Terminal (Admin) for elevated permissions. Run the Command: Type in the following command and hit Enter: net localgroup administrators Review the List: This command will display all accounts that are part of the Administrators group, including your own. If you see your username listed, you have administrative privileges. Benefits of Using Command Prompt Using Command Prompt is a powerful way to gather information about your system. It can also serve as a troubleshooting tool if you encounter permission-related issues. Method 4: Using Windows PowerShell PowerShell offers advanced capabilities for system administrators and experienced users, including checking user account permissions. Step-by-Step Guide Open PowerShell: Click on the Start button, type PowerShell, and select Windows PowerShell or Windows Terminal. Run the Command: Type the following command: Get-LocalGroupMember -Group "Administrators" Check the Output: This command will list all members of the Administrators group. Your username should appear in the results if you have admin rights. Why Use PowerShell? PowerShell scripts can be automated and used for batch processes, making it an appealing option for IT professionals working in enterprise environments. Method 5: Checking via Local Security Policy For users interested in security settings and permissions, the Local Security Policy tool can provide insights into account rights. Step-by-Step Guide Open Run Dialog: Press Windows + R to open the Run dialog box. Access Local Security Policy: Type secpol.msc and hit Enter. This will open the Local Security Policy window. Navigate to Local Policies: In the left panel, expand Local Policies and select User Rights Assignment. Check for Admin Rights: Look for the policy titled "Log on as a service" or "Create a token object." If your user name appears in these lists, you have administrative privileges. When to Use Local Security Policy This method is particularly useful for users managing complex user permissions or those running Windows Pro or Enterprise editions. Method 6: Using Group Policy Editor The Local Group Policy Editor is available in Pro and Enterprise versions of Windows 11 and allows you to manage user permissions. Step-by-Step Guide Open Run Dialog: Press Windows + R on your keyboard. Access Group Policy Editor: Type gpedit.msc and hit Enter. Navigate to Users: On the left side, navigate to Computer Configuration > Windows Settings > Security Settings > Restricted Groups. View Members of Administrators Group: Double-click on "Administrators" to view its members. Your username should be listed if you have admin rights. The Importance of Group Policy Editor This tool is commonly used in organizational settings to apply permissions across multiple users, making it a vital aspect of Windows network management. Method 7: Identifying Admin Rights When Installing Software Sometimes, you may not need to check directly for admin status but can discover it when attempting to install new software. Step-by-Step Guide Initiate Software Installation: Launch the installation process for any software of your choice. Observe the Prompt: If you're prompted with a User Account Control (UAC) dialog asking for permission to proceed, this indicates that your account requires admin rights to continue. If you can proceed without this prompt, your account likely has administrative privileges. User Account Control (UAC) is a security feature in Windows that prevents unauthorized changes to the operating system, making it a useful indicator of your permissions. Method 8: Using the Windows Registry For more advanced users, the Windows Registry can also provide information about user permissions. Step-by-Step Guide Open Run Dialog: Press Windows + R. Access Registry Editor: Type regedit and hit Enter. Navigate to the User Key: Find your user SID in the following path: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList Check Group Membership: Locate your user profile and see the values associated. If you have permissions for Admin, you'll typically see entries allowing administrative changes. Caution Editing the registry can lead to severe issues if done improperly. Always create a backup before proceeding. Verifying Admin Rights Through Windows Features Sometimes, specific Windows features such as the Control Panel or Task Manager can provide insights into your account status. Control Panel Method Open Control Panel: Press Windows + R, type control, and press Enter. Navigate to User Accounts: Click on User Accounts followed by Manage another account. Here you will see the account type listed next to your profile. Task Manager Method Open Task Manager: Press Ctrl + Shift + Esc. Check User Accounts: Click on the Users tab. If your name is listed with administrative rights, you will see "Admin" under the "Group" column. Summary Checking if you have admin rights in Windows 11 can be accomplished through various methods, each catering to different levels of expertise and preference. Whether you prefer the simplicity of the Settings app or the depth of command-line tools, understanding your account permissions is vital for maximizing your Windows experience. Admin rights empower you to install software, change system settings, and troubleshoot effectively, making it a cornerstone of system management. Final Thoughts If you discover that you do not have admin rights and require them for essential tasks, consider reaching out to the system administrator or, if you're the sole user, modifying your account settings using an administrator account to elevate your privileges. Knowledge of your account type not only helps in managing your device more effectively but also enhances the overall security and functionality of your Windows 11 experience. On the Windows-based operating system, administrator rights are required to perform many tasks, such as making system changes, installing and launching the software, etc. Here are four ways you can quickly check if you have administrator rights in Windows 10. Method 1: Check for administrator rights in Control Panel 1. Open Control Panel, and then go to User Accounts > User Accounts. 2. Now you will see your current logged-on user account display on the right side. If your account has administrator rights, you can see the word "Administrator" under your account name. Method 2: Check for administrator rights in Settings 1. Open Settings using Win + I key, and then go to Accounts > Your info. 2. Now you can see your current signed-in user account. If you are using an administrator account, you can see an "Administrator" word under your user name. Method 3: Check for administrator rights using Command Prompt 1. Open a Command Prompt window. You can first open the Run dialog using Win + R keys, then type in cmd and click OK. 2. Type in command: net user and hit Enter. Replace with the name of your user. You will get a list of attributes of your account. Look for the "Local Group Memberships" entry. If your account belongs to the Administrator group, it should have administrator rights. Method 4: Check for admin rights in Local Users and Groups 1. Open the Computer Management. You can first right-click on the Windows icon, then select Computer Management from the menu. 2. Expand Local Users and Groups and select Users folder. You will see a full list of all user accounts on your computer. Double-click on your user account to open the Properties dialog. 3. Now go to the Member Of tab. If you can see the Administrators group appear here, your user should have administrator rights. Related Articles To perform specific tasks, your account needs to have administrative privileges. That would explain why when you try to follow instructions, things don't turn out the way you expected them to. You may have made a mistake following instructions, or maybe your account doesn't have the administrative privileges it needs to complete the task. The good news is that there are easy ways to check what type of account you have. 1. Check for Administrative Privileges in Settings To open settings, press the Windows and I keys. Go to account, and below your profile picture, you should see if you have administrative privileges. 2. Check Account Type in Local Users and Groups The fastest way to open Local Users and Groups is to type lusrmgr.msc in the search bar. If you prefer, you can also right-click on the Windows start menu and click on Computer Management. When the new window appears, click on Local Users and Groups, followed by the Groups option. Locate the Administrators option and double-click on it. The Administrator Properties window should appear, and when it does, you'll see what accounts have administrative privileges in the Members box. 3. Use the Command Prompt to Check Account Type The Command Prompt also offers you a quick way to check if you have a standard user account or not. Open the Command Prompt by using the search bar and type: net user (accountname) So, the entry would look like this: net user judys If in the Local Group Memberships section, you only see Users, then you have a standard user account. But, if you see both Administrators and users, then you have Administrative privileges. 4. Use Computer Management to Check Account Type Look for the Computer Management option in the search bar. If it's not already expanded, click on the System Tools drop-down menu. Now, click on the Local Users and Groups option. Choose the Users branch and find the account you want to check. Right-click on the account and choose the Properties option. Click on the Member Of tab, and if it says both Administrators and Users, you have administrative privileges. If it only says users, you have a standard account. 5. Determine Account Type with Windows PowerShell With PowerShell, things are a little different, but it's still possible to see if you have a local account or not. Open PowerShell by right-clicking on the Windows start menu and choose the one that says, Administrator. The first command you'll need to enter is whoami and press enter. The second command to enter is: Get-LocalUser -Name username | Select -ExpandProperty Replace "username" with the username displayed with the whoami command. If you only have a local account, it'll say Local. 6. Use Windows Account Type Using Control Panel Use the search bar to look for the Control Panel option and press Enter to open it. Once it's open, go to User Accounts and click on the User Accounts option. You'll click on the same option twice. To the right of your profile picture and under your email, you'll see if your account is an Administrator. Conclusion Having an administrative account is a must for specific tasks. Now you can check if your account has the clearance to perform those tasks or not. So, is your account an administrative one?