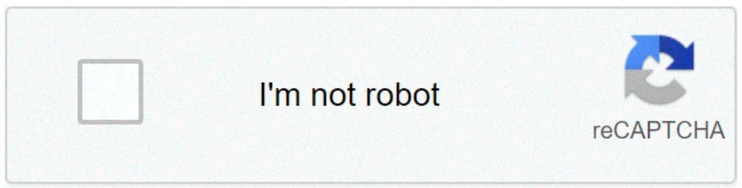

Continue

Windows cannot be installed to this disk the selected disk is of the gpt

By Michael Dance Many desktop and laptop vendors who group Windows XP with the preinstalled computer and have stopped providing the actual Windows XP installation disk. If your computer is fried or you just want to perform a clean reinstallation, you'll need to purchase another Windows XP license. Creating a specific reinstall disk avoids this problem. Back up your entire hard drive. Find a list of free hard disk backup software thefreecountry.com (see Resources). Locate your Windows XP license code (or product key). Often, this number will be recorded on the side of the computer tower or on the underside of the laptop. If you can't find it, see Resources for a list of free key search programs. Download \wxp10,\ a Windows XP boot sector zip folder on your Windows XP installation disks from one of the download mirrors in Nu2.nu (see Resources). Download and install the ImgBurn program at ImgBurn.com (see Resources). Navigate to drive C on your computer, which appears in the My Computer folder. Right-click a blank space in it, point to New, and then click New Folder. Name the folder \reinstall.\ Locate the \i386\ folder in the root of drive C. Right-click it, and then click Copy. Open the \reinstall\ folder. Right-click anywhere in it and click Paste. After a loading period (which can be long because the i386 folder is about half a gigabyte in size), a replica of the i386 folder will appear. Open Notepad (available on the Start menu > programs > accessories). Type \Windows\ (without the quotation marks), and then press the spacebar once, and then press Enter only once. Then navigate to File > Save and save the file as \WIN51\ (this time include quotation marks) in the reinstall folder. If you installed your computer with XP Home Edition, copy the WIN51 file and paste it into the reinstallation folder as WIN51IC. If you installed your computer with XP Professional, do the same except for the WIN51IP copy name. Open the wxp10.zip. Go to cDs > wxphome > files > w2ksect.bin. Drag the w2ksect.bin file to the root folder of drive C (not the reinstallation folder). Copy the text below the letter and paste it into Notepad. Save the file (anywhere) with the name \XPSETUP.ibb\ (quotation marks INCLUDED). IBB[START_BACKUP_OPTIONS] BuildMode=1 Destination=0 TestMode=0 Verify=1 WriteSpeed=0 Copies=0 FileSystem=0 RecurseSubdirectories=1 IncludeHiddenFiles=0 IncludeSystemFiles=0 IncludeArchiveFilesOnly=0 AddToWriteQueueWhenDone=0 ClearArchiveAttribute=0 VolumeLabel_ISO9660=VRMHOEM_EN VolumeLabel_Joliet= VolumeLabel_UDF= Identifier_System= Identifier_VolumeSet= Identifier_Publisher= Identifier_Preparer= Identifier_Application= Dates_FolderFileType=0 Restrictions_ISO9660_InterchangeLevel=0 Restrictions_ISO9660_AllowMoreThan8DirectoryLevels =1 Restrictions_ISO9660_AllowMoreThan255CharactersInP ath=1 ath=1 Restrictions_ISO9660_DontAddVersionNumberToFiles=1 Restrictions_Joliet_InterchangeLevel=1 Restrictions_Joliet_AddVersionNumberToFiles=0 BootableDisc_MakeImageBootable=1 BootableDisc_MediaEmulationType=0 BootableDisc_BootImageFile=C:\w2ksect.bin BootableDisc_DeveloperIdentifier= BootableDisc_LoadSegment=07C0 BootableDisc_LoadSectorCount=4 [END_BACKUP_OPTIONS][START_BACKUP_LIST] C:\XPSETUP [END_BACKUP_LIST] Open ImgBurn and select Mode > Build from the menu, and then click File > Load Project. In the box that appears, navigate to XPSETUP.ibb and press \Open.\ Insert an empty CD or DVD into the CD/DVD burner. Wait a minute, and then make sure that the blank disk appears in the Destination section of ImgBurn (which, depending on the version, is most likely located in the lower left corner of the window). Click the Write or Build icon at the bottom of the ImgBurn window. If you receive a \Have you selected only one folder, does it represent the root?\ and then click Yes. It then creates the Windows XP reinstall disk. Windows 10 sometimes uses encryption by default and sometimes it doesn't: it's complicated. Here's how to check if your Windows 10 PC's storage space is encrypted and how to encrypt it if not. Encryption is not just about shuting down the NSA, it's about protecting sensitive data in case of PC loss, which everyone needs. Unlike all other modern consumer operating systems - macOS, Chrome OS, iOS and Android - Windows 10 still doesn't offer built-in encryption tools at all. You may need to pay for the Professional edition of Windows 10 or use a third-party encryption solution. If your computer supports it: Related Windows Device Encryption: Windows 8.1 will start encrypting hard drives by default: everything you need to know Many new PCs that come with Windows 10 will have automatically enabled Device Encryption. This feature was first introduced in Windows 8.1 and there are specific hardware requirements for this. Not all PCs will have this feature, but some will. There is also another limitation: it actually encrypts the drive only if you sign in to Windows with a Microsoft account. The recovery key is then loaded on to microsoft servers. This will help you recover your files if you can never access your PC. (This is also why the FBI probably isn't too worried about this feature, but we're just recommending encryption as a means to protect your data from laptop thieves here. If you're worried about the NSA, you might want to use a different encryption solution.) Device encryption enabled even if you enter an organization's domain. For example, you could access a domain owned by your employer or school. The recovery key will then be loaded on to the domain servers in your organization. However, this doesn't apply to the average person's PC, but only to PC PCs to domains. To see if device encryption is enabled, open the Settings app, go to System > About, and search for a Device Encryption setting at the bottom of the Info pane. If you don't see anything about device encryption here, YOUR PC doesn't support device encryption and isn't enabled. If device encryption is enabled, or if you can enable device encryption by signing in with a Microsoft account, you'll see a message saying it here. For windows pro users: BitLocker RELATED: Do I need to upgrade to

the professional edition of Windows 10? If device encryption is not enabled or if you want a more powerful encryption solution that can also encrypt removable USB drives, for example, you want to use BitLocker. Microsoft's BitLocker encryption tool has been part of Windows for several versions and is generally well considered. However, Microsoft still limits BitLocker to the Professional, Enterprise, and Education editions of Windows 10. BitLocker is safer on a computer that contains Trusted Platform Module (TPM) hardware, as most modern PCs do. You can quickly check if your PC has TPM hardware from Windows or check with your computer manufacturer if you're not sure. If you've created your PC, you may be able to add a TPM chip to it. Look for a TPM chip sold as an additional module. You will need it to support the exact motherboard inside your PC. RELATED: How to use BitLocker without a Windows Trusted Platform Module (TPM) normally says bitlocker requires a TPM, but there is a hidden option that allows you to enable BitLocker without a TPM. You will need to use a USB flash drive as the boot key that must be present every boot if you use this option. If you already have a Professional edition of Windows 10 installed on your PC, you can search for BitLocker on the Start menu and use the BitLocker control panel to enable it. If you upgraded for free from Windows 7 Professional or Windows 8.1 Professional, you should have Windows 10 Professional. If you don't have a Professional edition of Windows 10, you can pay $99 to upgrade Windows 10 Home to Windows 10 Professional. Just open the Settings app, go to Update & >'activation, and click the Go to Store button. You will have access to BitLocker and the other features included with Windows 10 Professional. Security expert Bruce Schneier also loves a proprietary full-disk encryption tool for Windows called BestCrypt. It is fully functional on Windows 10 with modern hardware. However, this tool costs $99, the same price as an upgrade to Windows 10 Professional, so updating Windows to take advantage of BitLocker could be a Best. For everyone else: VeraCrypt RELATED: 3 alternatives to the now-defunct TrueCrypt for your encryption needs spend an additional $99 just to encrypt your hard drive for some some security can be a difficult sale when modern Windows PCs often cost only a few hundred dollars in the first place. You don't have to pay the extra money for encryption, because BitLocker isn't the only option. BitLocker is the most integrated and well-supported option, but there are other encryption tools you can use. The venerable TrueCrypt, an open source full-disk encryption tool that is no longer in development, has some issues with Windows 10 PCs. It cannot encrypt GPT system partitions and start them using UEFI, a configuration that most Windows 10 PCs use. However, VeraCrypt, an open source full disk encryption tool based on TrueCrypt source code, supports EFI system partition encryption depending on versions 1.18a and 1.19. In other words, VeraCrypt should allow you to encrypt the system partition of your Windows 10 PC for free. RELATED: How to protect sensitive files on your PC with the developers of VeraCrypt TrueCrypt famously shut down development and declared TrueCrypt vulnerable and unsafe to use, but the jury is still out if that's true. Much of the discussion around this focuses on whether the NSA and other security agencies have a way to crack this open source encryption. If you're just encrypting your hard drive so thieves can't access your personal files if they steal your laptop, you don't have to worry about that. TrueCrypt should be quite safe. The VeraCrypt project has also made security improvements and should potentially be safer than TrueCrypt. Whether you're encrypting just a few files or the entire system partition, that's what we recommend. We would like Microsoft to offer more Windows 10 users access to BitLocker or at least extend device encryption so that it can be enabled on multiple PCs. Modern Windows computers should have built-in encryption tools, just like all other modern consumer operating systems do. Windows 10 users should not pay extra or hunt down third-party software to protect their important data if their laptops are ever moved or stolen. Stolen.