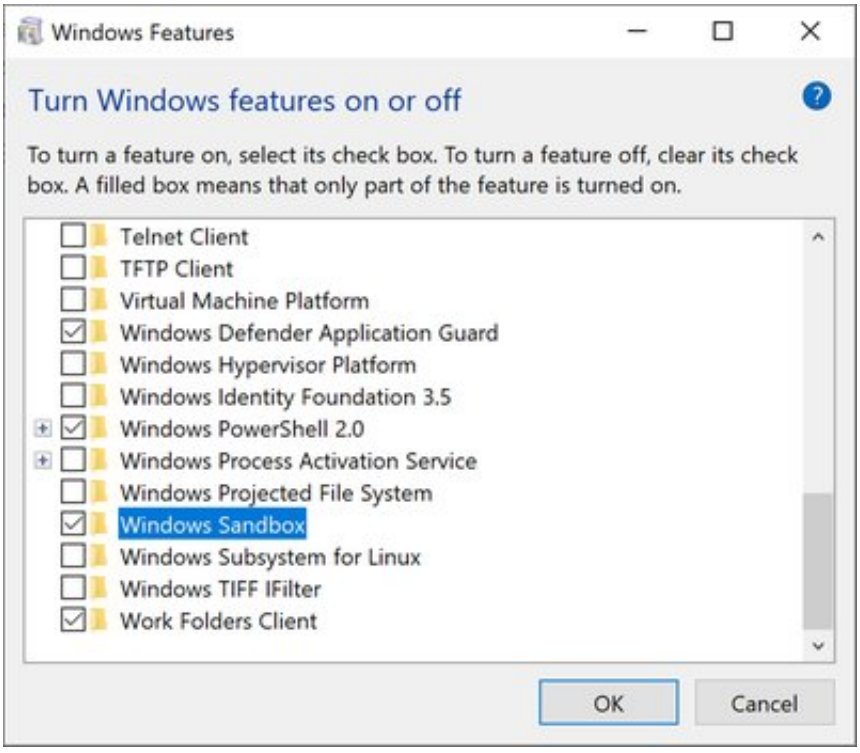
Windows Sandbox offers safe zone if app looks suspicious

December 21 2018, by Nancy Cohen



Credit: Microsoft

Windows Sandbox is getting a lot of press and for good reason: Windows watchers say it's going to be a safe place to park "hmmm" executables, the ones than could (or could not) be your pathway to malicious software.

Microsoft's Hari Pulapaka posted ample introductions, describing

Sandbox as "tailored for safely running applications in isolation."

Pulapaka, Margarit Chenchev, Erick Smith and Paul Bozzay are those on the Microsoft Windows Sandbox team.

For certain Windows users, this will be a nice gift that they can open—and, oh yeah, for select versions of the operating system. According to *ExtremeTech*, "this won't come to the base version of Windows 10, but maybe it'll convince a few people to upgrade."

Specifically, "Windows Sandbox will be available in Insider builds of Windows 10 Pro and Enterprise starting with build 18305," said Peter Bright, *Ars Technica*. (It's built in to Windows 10 but exclusively in Pro and Enterprise flavors.)

In fact, here are the prerequisites, in addition to the Windows 10 Pro or Enterprise Insider build 18305 or later. So if you plan to use this feature, here is the list, from Pulapaka: AMD64 architecture; virtualization capabilities enabled in BIOS; at least 4GB of RAM, while 8GB is recommended; at least 1 GB of free disk space with SSD recommended; at least 2 CPU cores, while 4 cores with hyperthreading are recommended.

Why is Sandbox for advanced and enterprise users only?

Well, even the "quick start" does not sound very simple to a novice user content to e-mail, watch movies and surf Amazon. This is an excerpt from the Windows Sandbox page: "Quick start; Install Windows 10 Pro or Enterprise, Insider build 18305 or newer; Enable virtualization: If you are using a physical machine, ensure virtualization capabilities are enabled in the BIOS. If you are using a virtual machine, enable nested virtualization with this PowerShell cmdlet:

Set-VMProcessor -VMName -ExposeVirtualizationExtensions $true."

If this sounds like something that would help you, and you meet the criteria (your machine needs to be 64-bit, have at least 4GB (8GB ideally) of RAM, 1GB of disk space (preferably SSD) and at least a dual-core processor (though 4 hyperthreaded is recommended), then you can explore Windows Sandbox in Insider Build 18305.

How have computer users tested suspicious files in the past? *ExtremeTech*, Ryan Whitwam said virtual machines have served to test such files. When the Windows Sandbox comes along, it will be "like a streamlined virtual machine," as Whitwam put it. Richard Speed in *The Register* said that in those instances where one was suspicious over an app, "we'd spin up a new Windows 10 Virtual Machine using Hyper-V and run the thing in there, but we'd be the first to admit it is inconvenient, and licensing is a pain."

Speed described how Sandbox lightens the load. "The Windows Sandbox uses the hypervisor to do something similar, but rather than faffing about with Hyper-V, adds a Windows Sandbox app which will spin up a fresh desktop, isolated from the host. The app, or installer, can be pasted into the desktop window and then run without fear of OS borkage."

He said Sandbox treats the installed OS as a base image, and there is no need to download or create new VHD images.

So, the idea is to go ahead and run any app in a virtual machine and it is disposable, sparing the host OS from any trouble. Disposable – as in nothing persists on the device; everything is discarded after you close the application (Sandbox "gets destroyed and reset whenever it's closed, so no changes can persist between runs," said Bright in *Ars Technica*.)

"Any software installed in Windows Sandbox stays only in the sandbox

and cannot affect your host. Once Windows Sandbox is closed, all the software with all its files and state are permanently deleted," said Pulapaka.

Whitwam said, "the machine will be able to create a small 100MB Windows 10 installation that is completely isolated from your real operating system via Microsoft's Hypervisor to run a separate kernel. This is a 'hybrid' approach that doesn't need a full OS image like a regular virtual machine."

More information: techcommunity.microsoft.com/t5 … -Sandbox/ba-p/301849