

# Security Management / Global Authorized Files



Authorized file	Authorized process	Authorized operation	Enabled	Description	Access Control	Workspace Control
%ProgramFiles%\*.tmp	winhlp32.exe	read modify	Yes	Allow winhelp to write tmpfiles where it wants. Apparently windows XP winhelp wants to do this	All users	All workspace containers
%ProgramFiles%\RES PowerFuse Workspace Extender\pfwsext.exe	*	read execute	Yes	Allow the RES Workspace Extender to run. When installed it writes itself into autolaunching through HKLM\...\Windows\Run.	All users	All workspace containers
%ProgramFiles%\vmware\vmware tools\tools.conf	vmwareuser.exe	read execute modify	Yes	Allows VMware to write this config file at logon if Read-Only Blanketing is enabled. It really needs execute to work too, it's not a mistake	All users	All workspace containers
%ProgramFiles%\vmware\vmware tools\vmware*.exe	explorer.exe	read execute	Yes	Authorize VMware tray and user apps. This is good to allow for demo/lab environments	All users	All workspace containers
%ProgramFiles%\vmware\vmware tools\vmwaretray.exe	vmwaretray.exe	read execute	Yes	This is the VMware systemtray. It's being launched for all users when a VM is started. This is good to allow for demo/lab environments	All users	All workspace containers
%reshomedrive%\windows\desktop\*	*	read	Yes	This rule is for locking down desktops for anything but shortcuts. This rule specifically allows any app to read the contents of the desktop	All users	All workspace containers

# Security Management / Global Authorized Files



Authorized file	Authorized process	Authorized operation	Enabled	Description	Access Control	Workspace Control
%reshomedrive%\windows\desktop\*.lnk	*	read modify	Yes	This rule is for locking down desktops for anything but shortcuts. Only allow shortcuts (*.lnk) files to be placed on the desktop	All users	All workspace containers
%reshomedrive%\windows\desktop\*.url	*	read modify	Yes	This rule is for locking down desktops for anything but shortcuts. Allow internet shortcuts to be dragged-and-dropped onto the desktop	All users	All workspace containers
%reshomedrive%\windows\desktop\new shortcut	*	read modify	Yes	This rule is for locking down desktops for anything but shortcuts. This rule enables the New Shortcut wizard to run correctly, allowing a user to create any shortcut of his choice	All users	All workspace containers
%systemdrive%\autoexec.bat	winlogon.exe	read modify	Yes	Winlogon wants to tamper with the autoexec.bat for some reason. Doesnt seem to modify anything?	All users	All workspace containers
%systemdrive%\autoexec.bat	*	read	Yes	Apparently alot of windows processes need to read autoexec.bat	All users	All workspace containers
%systemdrive%\documents and settings	rundll32.exe	read modify	Yes	Rundll32 want's to write something here when users rightclick the desktop and select explore. That ofcourse makes sense to everyone, right?	All users	All workspace containers




# Security Management / Global Authorized Files



Authorized file	Authorized process	Authorized operation	Enabled	Description	Access Control	Workspace Control
%systemdrive%\documents\ap pverifierlogs\vmwaretray*.log	vmwaretray.exe	read modify	Yes	Enable the tray to write a logfile. Apparently it wants to do this on a 2003 server	All users	All workspace containers
%systemdrive%\offline%\usern ame%	cmd.exe	read modify	Yes	Allows CMD to create a userfolder for the user in the offline folder on the computer. This is not necessary per default, but very usefull if you want to setup an offline folder for laptops	All users	All workspace containers
%SystemRoot%\security\logs\w inlogon.log	winlogon.exe	read modify	Yes	Allow winlogon to write it's logfile	All users	All workspace containers
%SystemRoot%\security\templ ates\policies\*	winlogon.exe	read modify	Yes	Allow winlogon.exe some freedom in the security templates folder	All users	All workspace containers
%SystemRoot%\system32\dum prep.exe	*	read execute	Yes	Allow the dump report to run, in the odd chance that the machine should suffer a BSOD. Dumpprep.exe is being called normally by explorer.exe and itself	All users	All workspace containers
%SystemRoot%\system32\dw wdumprep.exe	in.exe	read execute	Yes	This is Dr. Watson for Windows. Needed if an application unexpectedly explodes.	All users	All workspace containers
%SystemRoot%\system32\mob sync.exe	explorer.exe	read execute	Yes	Enabled so Windows offline Folder sync works for everybody	All users	All workspace containers
%SystemRoot%\system32\oobe chk.exe	explorer.exe	read execute	Yes	This is the Window Genuine validation thingy which windows aparently wants to run when you start up a session.	All users	Workspace Container: Citrix Servers

# Security Management / Global Authorized Files



Authorized file	Authorized process	Authorized operation	Enabled	Description	Access Control	Workspace Control
 %SystemRoot%\system32\rundll32.exe	explorer.exe	read execute	Yes	Needed at startup in order for desktop to initialize properly	All users	All workspace containers
 %SystemRoot%\windowsupdate.log	explorer.exe	read modify	Yes	Another system thingy. Explorer needs to write to this file when you've installed Microsoft updates	All users	All workspace containers
 %SystemRoot%\winhlp32.exe	*	read execute	Yes	Any app should be allowed to call winhelp	All users	All workspace containers