How to bypass the security warning "Unknown Publisher" with the checkbox "Always Ask Before Opening this File"

BrentgMS 19 Jun 2009 1:00 PM 21

Hi everyone!

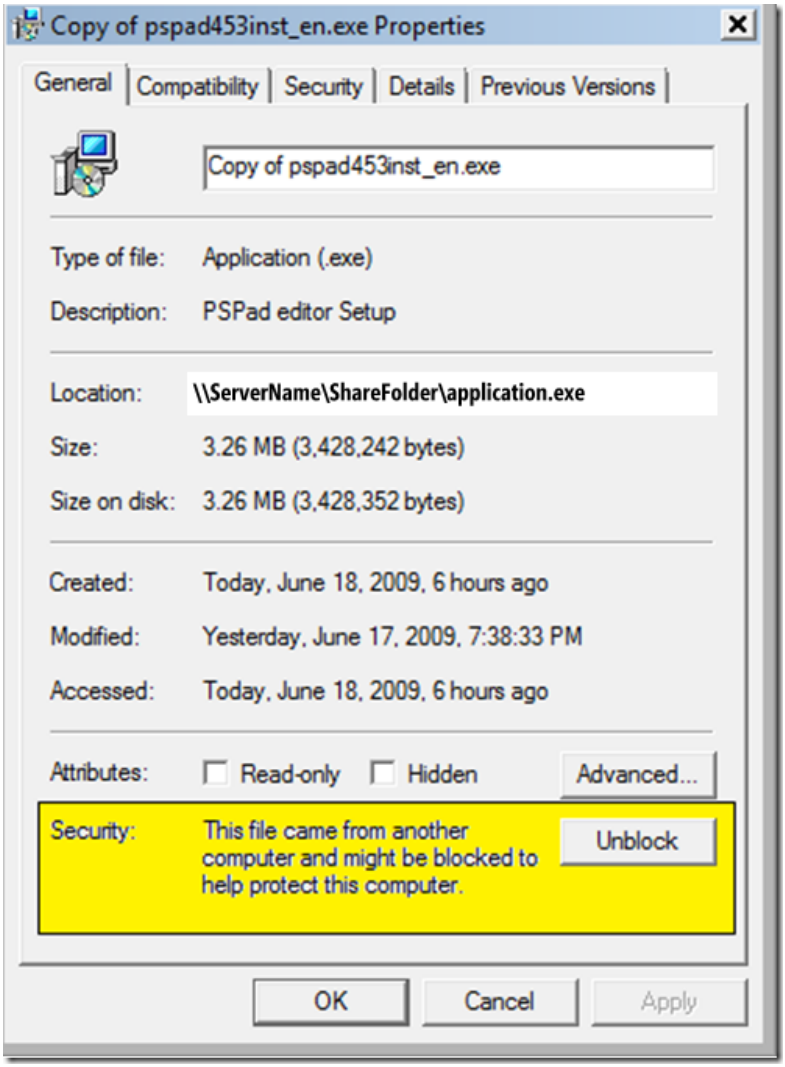
Axel here from the IE Escalation team with a scenario related to Security Warning - *Unknown Publisher* pop-up when executing a file that came from a non trusted source.

> ***Please note:*** The example below sets ***HIGH RISK*** files types to ***LOW RISK*** so that they can be executed without having to honor the warning dialog. We are creating this example because many corporate customers request this change to make their day-to-day operations easier to maintain. With that said, setting these options in attachment manager can put your system at risk, so please fully read the external documentation available on Attachment Manager and weigh the risks involved before making the decision to allow these files types to be executed without warning the user.

I am sharing this out because the immediate assumption is that by just adding the server name to the Local or Trusted Site zone will allow the file to be executed, which is not accurate. Once the file comes down from the **untrusted source** and with the Block file stream (see Fig. 1.1), until you remove the attribute you wont be able to run it without first getting the warning mentioned in this blog, see fig. 1.0.

Fig. 1.0 [Screenshot of the Warning with the checkbox "Always ask before opening this file" option]

Fig. 1.1 [Screenshot of the executable properties, showing the Security Unblock option]



Here is what it may look like once you have unchecked the option next to **"Always ask before opening this file".**

Fig. 1.2 [Here is what you will still get, even after you have removed the checkbox]

Once you add the unc path to either the Local or Trusted Sites Zone, you will no longer get the warning.

In the above example, we can see that the application did not have a digital signature that verifies its publisher, so we will have to do more work to bypass the warning. You can either have the executable signed using signcode.exe or use the Build in Windows Attachment Manager Policy.

The reason why you get the warning in the first place is because in Windows XP/SP2 and Windows 2003/SP1 we have introduced a new feature called Attachment Manager. This feature was added to help protect your computer from unsafe file attachments. This include accessing files across your network (e.g \\servername\share), files that you might receive with an e-mail message and from unsafe files that you might save from the Internet.

If the Attachment Manager identifies an attachment that might be unsafe, the Attachment Manager prevents you from opening the file, or it warns you before you open the file.

Here are the steps to bypass the warning using Attachment Manager Group Policy. I am also including the registry key modified by the policy.

From Start Run type: gpedit.msc

From User Configuration> Administrative Template> Windows Components> Attachment Manager

Set the following:

Configuration Settings:

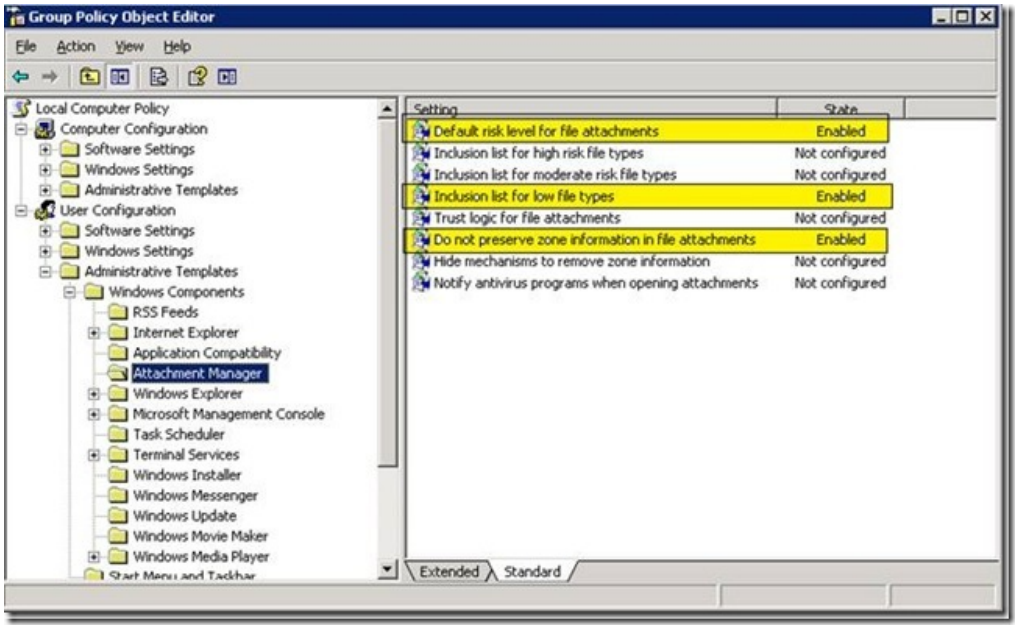
> Default risk level for file attachments: Set it to Enabled and Set the default risk level to[Low Risk]

> Inclusion list for low file types: Set it to Enabled and add the file extension [.exe;.vbs;.msi]

> Do not preserve zone information in file attachments: Set it to Enabled.

Close Gpedit.msc and run gpupdate /force

Screenshot of the policy:



Final Step:

> Add the UNC to Local Intranet or Trusted Sites

> Log off and log back in

> Test accessing the UNC share

Registry keys:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies]

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Associations]

"LowRiskFileTypes"=".exe;.vbs;.msi"

"DefaultFileTypeRisk"=dword:00001808

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments]

"SaveZoneInformation"=dword:00000001

Article below explains everything about Attachment Management.

- 883260 Description of how the Attachment Manager works in Windows XP Service Pack 2
  http://support.microsoft.com/default.aspx?scid=kb;EN-US;883260
- How would you sign your file. You could use signcode.exe from Microsoft. Here is also an article:
- Steps for signing a .cab file: http://support.microsoft.com/default.aspx?scid=kb;en-us;247257

Regards,

The IE Support Team

Comments

KS 22 Jun 2009 6:54 AM #

There is a much better fix for this. It doesn't require changing the risk type of a file. Add the respective file server NETBIOS name in your intranet to your Local Intranet zone. e.g. if the name of the machine you get the files from is "mymachine.example.lan" you want to add "mymachine" (without protocol) to Internet Options > Security > Local Intranet > Sites > Advanced. Depending on your Windows and SP/IE version this will add as "file://mymachine" or just "mymachine" to the list of Intranet sites. If you now open a "risky" filetype like .mdb or .exe on a shared network drive on this server you won't get this security warning anymore.

Obviously, this can also be done via GP. In my eyes this is a much safer and better way than your proposed solution.

Frank Meade 21 Jan 2010 11:20 AM #

The fix offered by KS worked perfect.

VFR Boy 27 Jan 2010 5:23 PM #

I am getting this when running a .cmd file at startup - I have a shortcut to the .cmd file in the Startup folder, and the file is local on the 2nd (D:\) drive.

I have about 320 machines I need to deploy to so can you help with the GP or Registry update required?

Thanks,

VFR Boy

samhalsey 4 Mar 2010 8:12 AM #

i want this popup to go away without running file?

P. Drummond 16 Apr 2010 1:01 PM #

I got so fed up with Win7 security popups before I could even run my good old text editor, I finally created a batch file with just the path to the EXE. The batch program sits in the taskbar until you exit the editor but I'll put up with that just to get some work done. I'm just about ready to axe UAC. I am using an Admin account and can't for the life of me understand constant nagging just to run my everyday applications.

P. Drummond 16 Apr 2010 1:02 PM #

I got so fed up with Win7 security popups before I could even run my good old text editor, I finally created a batch file with just the path to the EXE. The batch program sits in the taskbar until you exit the editor but I'll put up with that just to get some work done. I'm just about ready to axe UAC. I am using an Admin account and can't for the life of me understand constant nagging just to run my everyday applications.

Nic 28 Apr 2010 9:05 PM #

The UAC is rubbish. Even when set on the most minimum level, Windows 7 will continually bring up

security messages when installing software, which is quite frustrating to an IT Desktop Support guy like myself.

And it gets better.. Microsoft introduced this level of "security" to Server 2008, so that even Domain Administrators are expected to confirm that they want to run the DNS or DHCP tools, despite that, to someone with a bit of common sense, if someone doesn't know what they're doing they shouldn't be a Domain Administrator to begin with.

But I think the reason why Windows 7 is so pedantic is because Microsoft develops their software to cater to the only country in the world where you can sue somebody else for your own stupid mistakes.

/rant

Anyway.. if anyone has found a method of turning off these annoying security messages for software installs, please comment. Thanks! :)

Rico 26 May 2010 12:22 PM #

Nic,

You are dead-on about this country! Always looking to cover your ace instead of solving a problem.

Rico

Merry 7 Sep 2010 7:57 PM #

I tried Configuration Settings as above attachment.

it works. thank you

mpm 13 Nov 2010 2:10 PM #

I'd rather see a solution which *totally* prevents creating ALL Alternative Data Streams alltogether (other than using the totally outdated FAT32, of course).

Logic would dictate that those files would not created when the policy 'Do not preserve zone information' is enabled.

Unfortunately, the ADS-files are (sometimes?) STILL created with that setting enabled - be it not attachments (it can even happen with a simple downloaded JPG-file from a site like rapidshare, even if that JPG-extension is in the "Inclusion list for low file types" (which shoud be "Inclusion list for low risk file types", BTW).

But there seems to be no other setting available 'Do not preserve zone information' in gpedit.msc. At least, a web search for 'Do not preserve zone information' did only find the above setting. (It's *very* weird anyway, that there isn't a search option in gpedit!).

Sometimes, even when killed the ADS-file with "Marx NTFS ADS Viewer" (and more importantly: killer), Windows still comes with the stupid warning. It seems there's some memory caching of the ADS-info involved here or something like that (if i move it to a NTFS-subfolder and back, the warning is gone; but if i rename the file and back, the warning is not gone - even whereas the warning does not appear with the renamed file!).

herbert 16 Nov 2010 10:03 PM #

KS, your suggestion works perfectly. It's better for you to have your own website for any IT FAQ or etc.

herbert 16 Nov 2010 10:04 PM #

I mean free IT information website KS :)

tom 20 Jun 2011 4:33 AM #

the links option in windows is for web links, its ie shortcuts/bookmarks

-you get security warnings when you click on them-

to make links that don't have the warning, create a separate folder and

put the program shortcuts in there. then add a toolbar and choose that folder

location.

if its not a "links", no error. ez if you know.

Daniel Brockman 2 Sep 2011 8:48 AM #
Msft advice is incomprehensible and therefore useless.

Babar 2 Sep 2012 11:27 PM #
KS - Very Good . .. . . . It has solved my old problem. . . . . .THANKS ALOT _ _ _ _ _ _ _ _

Hitesh 31 Mar 2013 10:21 AM #
Thanks a lot ! Solved my problem :)

Geoff 5 Jun 2013 5:39 AM #
Thanks KS - works a treat. Moved an application from local drive to NAS and started getting the error, now fixed.

Slamdunkbear 28 Jun 2013 7:16 AM #
We have our own software but after install to the Win 8, it will pop up "Unknow Publisher" & will not allow us to open it(User does not have permission to open the file).

Can any one tell me how to fix it for our software?

Please let me know - how to register with MicroSoft and avoid this message to pop up?

AxelRMSFT 8 Jul 2013 9:06 PM #
@Slamdunkbear

Is this an EXE?

Where is the file access from? (network share, local file, url...?)

Did you added the url or network share to the proper zone to help bypass the warning?

If the steps shared in this blog dialog did not helped, I suggest opening a ticket with support to further assist you.

Jamie 7 Aug 2013 9:29 AM #
I need to know how to change my settings so that I can view Attachments in Facebook , I am running XP on my HP Desktop? Please can some one help me?

Nasro Min Allah 11 Oct 2013 4:56 AM #
Thanks Ks , its working for me....nice

" KS 22 Jun 2009 6:54 AM #

There is a much better fix for this. It doesn't require changing the risk type of a file. Add the respective file server NETBIOS name in your intranet to your Local Intranet zone. e.g. if the name of the machine you get the files from is "mymachine.example.lan" you want to add "mymachine" (without protocol) to Internet Options > Security > Local Intranet > Sites > Advanced. Depending on your Windows and SP/IE version this will add as "file://mymachine" or just "mymachine" to the list of Intranet sites. If you now open a "risky" filetype like .mdb or .exe on a shared network drive on this server you won't get this security warning anymore.

Obviously, this can also be done via GP. In my eyes this is a much safer and better way than your proposed solution"