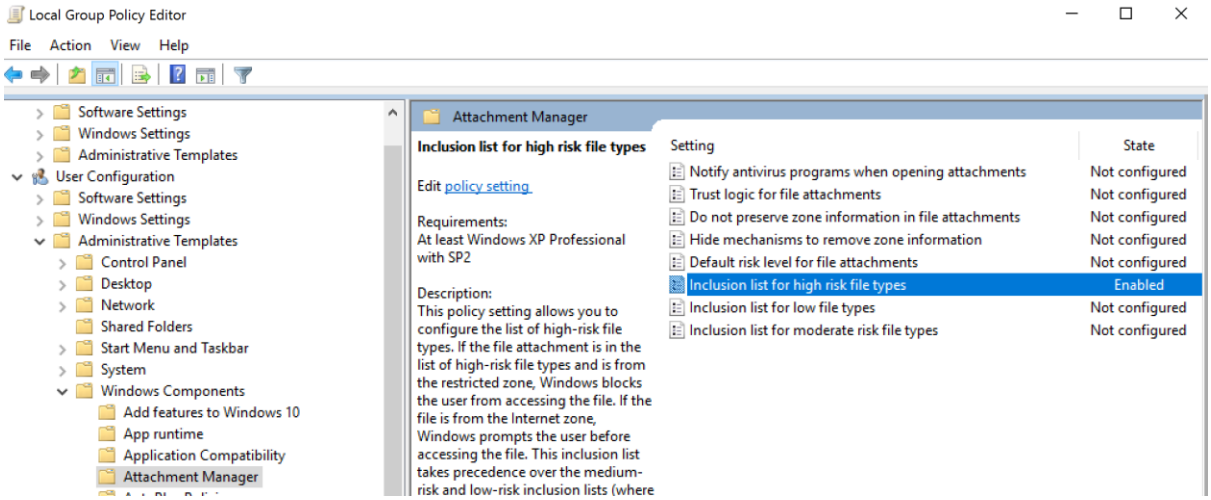
Please note that this is a guide only.

Indelible Data cannot be held responsible for any issues that may arise to your systems / devices after following this guidance. Microsoft sometimes change the functionality associated to some settings from time-to-time so we cannot guarantee constant behaviour.

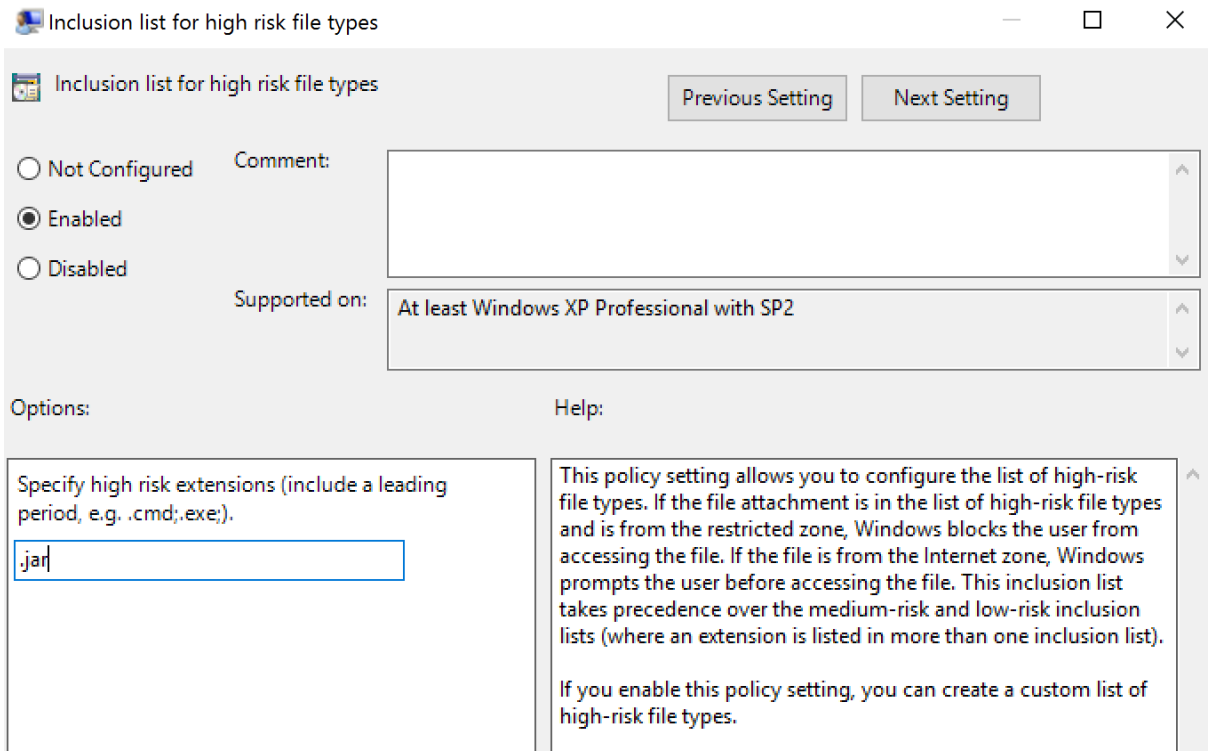
You must ensure that any changes are fully tested before deploying.

Sample use of Attachment Manager (to prevent .jar files running without warning):

1. Open gpedit.msc / Group Policy editor



2. Double click “Inclusion list for high risk file types”



3. If multiple files are entered, they should be separated by a semi-colon (.jar;.py;.sh)
4. A suggested list can be found below (remember to test that adding these extensions does not adversely affect workflow)
5. Don't forget to force an update:
    - Gpupdate / force
    - Restart browser

File types that are often prevented by companies (not exhaustive):

Programs

.EXE – An executable program file. Most of the applications running on Windows are .exe files.

.PIF – A program information file for MS-DOS programs. While .PIF files aren't supposed to contain executable code, Windows will treat .PIFs the same as .EXE files if they contain executable code.

.APPLICATION – An application installer deployed with Microsoft's ClickOnce technology.

.GADGET – A gadget file for the Windows desktop gadget technology introduced in Windows Vista.

.MSI – A Microsoft installer file. These install other applications on your computer, although applications can also be installed by .exe files.

.MSP – A Windows installer patch file. Used to patch applications deployed with .MSI files.

.COM – The original type of program used by MS-DOS.

.SCR – A Windows screen saver. Windows screen savers can contain executable code.

.HTA – An HTML application. Unlike HTML applications run in browsers, .HTA files are run as trusted applications without sandboxing.

.CPL – A Control Panel file. All of the utilities found in the Windows Control Panel are .CPL files.

.MSC – A Microsoft Management Console file. Applications such as the group policy editor and disk management tool are .MSC files.

.JAR – .JAR files contain executable Java code. If you have the Java runtime installed, .JAR files will be run as programs.

Scripts

.BAT – A batch file. Contains a list of commands that will be run on your computer if you open it. Originally used by MS-DOS.

.CMD – A batch file. Similar to .BAT, but this file extension was introduced in Windows NT.

.VB, .VBS – A VBScript file. Will execute its included VBScript code if you run it.

.VBE – An encrypted VBScript file. Similar to a VBScript file, but it's not easy to tell what the file will actually do if you run it.

.JS – A JavaScript file. .JS files are normally used by webpages and are safe if run in Web browsers. However, Windows will run .JS files outside the browser with no sandboxing.

.JSE – An encrypted JavaScript file.

.WS, .WSF – A Windows Script file.

.WSC, .WSH – Windows Script Component and Windows Script Host control files. Used along with with Windows Script files.

.PS1, .PS1XML, .PS2, .PS2XML, .PSC1, .PSC2 – A Windows PowerShell script. Runs PowerShell commands in the order specified in the file.

.MSH, .MSH1, .MSH2, .MSHXML, .MSH1XML, .MSH2XML – A Monad script file. Monad was later renamed PowerShell.

Shortcuts

.SCF – A Windows Explorer command file. Could pass potentially dangerous commands to Windows Explorer.

.LNK – A link to a program on your computer. A link file could potentially contain command-line attributes that do dangerous things, such as deleting files without asking.

.INF – A text file used by AutoRun. If run, this file could potentially launch dangerous applications it came with or pass dangerous options to programs included with Windows.

Documents

.DOCM, .DOTM, .XLSM, .XLTM, .XLAM, .PPTM, .POTM, .PPAM, .PPSM, .SLDM – New file extensions introduced in Office 2007. The M at the end of the file extension indicates that the document contains Macros.