

Windows Enterprise Announcement

January 9, 2009 – Enterprise Domain Policy Change Jan 26 - Disable AutoPlay

The decision has been made to make a change to the Windows Enterprise Domain policy to disable the use of "AutoPlay" facilities on all mountable drives (including CD-ROM, DVD, and USB drives). This policy change will happen on **January 26, 2009** (a Monday morning).

This policy change was discussed in the December 2008 WinAdmin and CCSG meetings and the January WinAdmin meeting. See the December 2008 and January 2009 WinAdmin meeting notes for more details:

<http://www.tech.ait.iastate.edu/win2000/admin/WinAdmin.2008.12.12.pdf>

<http://www.tech.ait.iastate.edu/win2000/admin/WinAdmin.2009.01.09.pdf>

The proposal was also mailed to the WinAdmin and CCSG mailing lists on Dec 19, 2008 (subject "Proposed Enterprise Domain Policy - Disable AutoPlay"). Discussion at the meetings and on the WinAdmin and CCSG mailing lists produced only positive feedback (with many IT managers indicating they had already made such a policy change).

The AutoPlay facility makes something (like a software installer, a presentation, or a selectable menu) start up automatically when a mountable drive is mounted. It does this by looking for an "autorun.inf" file on the drive and performing the operations defined by it. While this has some nice "ease of use" advantages, the authors of computer viruses find this a great facility to infect computer systems. A specially crafted AutoPlay startup file can spread infections quite rapidly as users plug devices into their systems. At Iowa State there have been at least three known outbreaks of AutoPlay viruses in the past few weeks.

Disabling the AutoPlay facility does not mean the software or features on the media will not run. Users will have to open a Windows Explorer window or use a command line to launch the desired executable.

The specific domain policy setting that will be changed January 26, 2009, is as follows:

Default Domain Policy

Computer Configuration

Administrative Templates

System

Turn off Autoplay: Turn off AutoPlay on "All drives"

As with all group policy, policy precedence remains as follows (in order of application):

1. Local
2. Site (ISU has none)
3. Domain
4. OU

An OU policy can be used to override the domain policy for a selected group of computers if desired.

A good Microsoft article on policies (both OU and local) for disabling AutoPlay is here:

<http://support.microsoft.com/kb/953252>

It is important to note from the above article that Microsoft has a non-critical patch that is required to completely disable all AutoPlay features on all systems. This patch is NOT currently installed by the Microsoft automatic update process.

Send any comments to either Steve Kunz (skunz@iastate.edu) or Wayne Hauber (wjhauber@iastate.edu).