

## Re: Restrict use of AMI, ADSI and WScript.Shell

**Source:**

<http://www.tech-archive.net/Archive/Internet-Server/microsoft.public.inetserver.iis/2004-04/1196.html>

---

**From:** David Wang [Msft] (*someone\_at\_online.microsoft.com*)

**Date:** 04/13/04

Date: Mon, 12 Apr 2004 20:01:57 -0700

You can use Filesystem ACL on %windir%\System32\wshom.ocx to control who can create the WScript.Shell object (as well as all the WScript.\* objects) in one shot. Can't use Filesystem ACL to allow one users to create WScript.Network but not WScript.Shell, for example.

I'm not certain if ADSI has anything comparable to WMI, but you can use the same Filesystem ACL approach on %windir%\system32\adsii.dll to prevent users to access all of the IIS:// ADSI namespace.

```
--
//David
IIS
This posting is provided "AS IS" with no warranties, and confers no rights.
//
"Peter Johansen" <peterJohan13384@hotmail.com> wrote in message
news:ZFFec.132167$Bk31.35595@twister01.bloor.is.net.cable.rogers.com...
Hi, I would appreciate any tips on restricting WMI, ADSI, and WScript.Shell
from being used in ASP pages by anyone other than the Administrators group
in a shared hosting environment. WMI seems like it can be restricted fairly
easily via the "WMI Control" MMC snap-in. But how about ADSI and
WScript.Shell? This is for IIS 6.0 on W2K3.
By the way, each web site has it's own IUSR account and application pool.
The application pool's identity is also a unique user account for each web.
This allows me to restrict access to files between different webs. However,
I would still like to restrict WMI, ADSI and Wscript.Shell from being used
at all, except by the Administrators group.
Thanks for any tips and advice.
```