Securing the ColdFusion MX Administrator

Posted At : July 20, 2005 3:36 PM | Posted By : Steven Erat
Related Categories: Adobe, ColdFusion, Macromedia

UPDATE June 2010:: You should read the the 2010 article on Adobe.com: ColdFusion 9 Lockdown Guide [PDF] for the most recent security advice at this time.

While there are Macromedia technotes and documentation on securing the ColdFusion 5 Administrator, there hasn't been much published on securing the Administrator in ColdFusion MX.

You would think that you could just remove the physical /CFIDE directory from the external webroot, or remove the /CFIDE mapping for the website from the IIS Management Console, but some ColdFusion features like CFFORM or CFGRID have dependencies on files under CFIDE, so removing it entirely would likely break applications or limit them if those features haven't been used yet, and of course, you'd have to restore the /CFIDE everytime you want to adjust ColdFusion Admin settings.

A practical solution that would provide application dependencies under CFIDE while also making the Administrator publicly *unavailable* and secure follows:

- Find the physical ColdFusion MX CFIDE directory on the system, and zip archive it to a backup
- If using IIS, remove the virtual mapping for /CFIDE from the IIS MMC
- Make the physical CFIDE directory available in the external web server document root
- From that CFIDE, remove the subdirectory administrator/ but leave everything else. The ColdFusion Admin runs entirely from the administrator/ directory.
- Use a different webserver instance or the built-in JWS webserver to serve the ColdFusion Administrator, but restrict that webserver instance to listen only on a private interface such as localhost/127.0.0.1 or an intranet IP on a seperate NIC
- To restrict the interface in the built-in JWS webserver that comes with ColdFusion, edit the jrun.servlet.http.WebService section in jrun.xml to change the attribute name="interface" element from * to localhost or the internal IP and then restart the server instance. Refer to vendor documentation if restricting the interface on an external webserver.
- Copy the full CFIDE directory with its administrator/ subdirectory to the document root for this *private* website instance.

The result of this configuration is a publicly facing external webserver that can serve your application and any dependencies from the /CFIDE directory without making the CF Admin available, and another webserver instance that will serve only the Administrator on a private internal IP or localhost. Since the CF Admin isn't accessible publicly, there's no risk of someone attempting to tamper with it.