# Protecting the CFIDE directory in IIS

Posted At : May 10, 2013 12:34 PM | Posted By : Mark Kruger
Related Categories: Coldfusion Security

Yesterday I had a server with IIS and a few hundred sites on it. Some, though not all, of the sites had an unprotected CFIDE directory mapped. So my task was to protect these directories by denying all IPs from access except a specific IP range. Before I describe the task and my trick let me remind you that this is not time to tout Linux or Apache or bash Microsoft in the comments. The muse welcomes comments but enjoys variety. We all know about Apache and its manifest benefits. We don't need you to remind us in spite of your excellent credentials and biting wit. IIS is fine platform with many strong points too and there are folks who need this information. They should not feel like they are sneaking into the adult section of the video store to get it. Now back to the Muse' usual good humor. Here's the scoop....

In IIS 7.5 before you are able to do that you must make sure that the "IP and Domain Restrictions" role service is installed. In prior versions of IIS (before 7.0) IP restrictions were a native part of IIS and you could access them from the security tab. But in 7.5 this is a separate service that has to be installed and is not "pre-selected" when you install IIS. In case you are scratching your head (how do I install a role service) try the following. Open server manager, click on features, scroll down to IIS and click on the "add role services" box. Under the security items you will see what you are looking for. Make sure the box is checked. It looks like this.

Next you will need to find the directory you are looking for in IIS. Using IIS manager navigate to CFIDE/Administrator and select it in the tree on the left hand side. Then click on the task icon that says "IPv4 Address and Domain Restrictions". You will see a blank screen with some link to the right. Click on the link that says "Edit Feature Settings" and you will see 2 options - allow and Deny. Like this.

Change the setting to "deny". In other words we are telling IIS to *deny all IP addresses any access to this directory*. Not to worry, we are now going to add exceptions. In the task pane click on the link for "add Allow" entry. You should see this dialogue.

It's pretty straightforward. If you wanted to allow a subnet on your local network for example, you might add 10.1.1.0/255.255.255.0.

**Lots of Busy Work**

Ok, but that's modifying the properties of one site. It's useful and easy and you could walk someone through it over the phone if you had to - all advantages of a GUI interface right? But as I said, I had to go through hundreds of sites looking for this problem. If I have to do these steps over and over for administrator and adminapi I'm going to poke my eye out. I have a solution for that. Before I describe it let me make sure of one thing. You must have exclusive access to the server. In other words, no one *else* should be making any IIS changes while you do this. As long as that condition is met you can do the following.

**ApplicationHost.config Magic**

Navigate to Windows/system32/inetsrv/config and open a file called applicationHost.config in an editor. You might note a lot of backup files here - applicationHost.config.1-n - IIS does this to keep previous copies of the file. I always make my own backup of the file anyway before I begin. Once you are editing the file go to the bottom of the file. Your new IP restrictions should exist there as the last entries. They look like this:

```
<location path="mywebsite/CFIDE/adminapi">
<system.webServer>
<security>
<ipSecurity allowUnlisted="false">
<add ipAddress="10.1.1.0" subnetMask="255.255.255.0" allowed="true" />
<add ipAddress="192.168.18.0" subnetMask="255.255.255.0" allowed="true" />
</ipSecurity>
</security>
</system.webServer>
</location>
<location path="mywebsite/CFIDE/administrator">
<system.webServer>
<security>
<ipSecurity allowUnlisted="false">
<add ipAddress="10.1.1.0" subnetMask="255.255.255.0" allowed="true" />
<add ipAddress="192.162.18.0" subnetMask="255.255.255.0" allowed="true" />
</ipSecurity>
</security>
</system.webServer>
</location>
```

The thing to note here is the "path" attribute and the first part of the path string. It is actually the "name" of the website in IIS. In other words, if the name of the web site (as displayed under sites in the left hand IIS navigation) is "joes barbershop" your path would actually be *path="joes barbershop/CFIDE/Administrator"*. If you are like me and you put the domain name in as the site name then this is not as obvious as you might think.

Using this information I can duplicate these 2 nodes over and over again for each site I need to protect. I can even script the creation of these nodes if I need to. This saved me time on a grueling task. IIS picks up the change immediately too - as soon as you save the file. I Hope this helps you. Happy Admining to one and all.