

## Re: Incoming E-Mail – cant create contact in OU

---

*Source:*

<http://www.tech-archive.net/Archive/SharePoint/microsoft.public.sharepoint.windowsservices/2007-09/msg00026.htm>

---

- *From:* Paul <Paul@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
  - *Date:* Mon, 3 Sep 2007 11:38:07 -0700
- 

I followed your instructions and was able to get it to work.

What I needed to do was

- 1) Go to the OU in security/advanced I added my sharepoint application pool and gave full rights.
- 2) On each WSS front end web server, I added the application pool to local admin

Rebooted all WSS web servers and tried it again, and it worked.

Now, I just need to determine the best way to give the local WSS permissions, as I am not so hip to have a website running as a local administrator!

"callahan" wrote:

Gotcha. I would strongly suggest that, in the future you really make the central admin pool different than the web app. It will really help secure that account a little (if the web app is compromised or something, central admin will be okay and vice versa, that central admin account is kind of precious). It also makes it easier for troubleshooting.

However, under the pressures of production I can see that just getting the darn thing to work is kind of critical. ; )

Now I understand that you have given the account "full rights" of the OU, but if you don't do advanced security, you are still not giving them the same, critical rights that the domain admins get, so you will continue to have problems until the cows come home.

Or at least, that has been my experience. The thing is, it's solid as a rock if the permissions are right (although I must confess that I have only clients using DMS with exchange 2003). My only problem (and I feel it's another security problem) is getting approval to work completely. But that's an issue for another day.

Re: Incoming E-Mail – cant create contact in OU

So I started with giving the app pool account domain admins permissions then went backwards. in other words I checked the special permissions that Administrators and Domain Admins get for the OU (they get lotsa rights straight out of the box, even if you didn't put them there), and gave my app pool account all of the same rights (and yes, that is really out of hand but bear with me).

-->And don't forget to IISRESET /noforce every single time you make a change that you think with work to get sharepoint to notice.<--

Then, when I got it to work, I began to remove the permissions that I didn't think would matter, stripping down what the app pool could do until I figured out (I'm pretty sure, I might still be giving it too much power) which permissions the app pool had to have to do its job with DMS. \*That's\* why I know that you need extra permissions to get that account to work, not just delegating control, even full control. It won't work, at least it didn't for me. Then, even when looking at security, selecting full control in the dialog box is not the same as the "special" permission settings under Advanced. Further, it seems to really, really matter that you don't just allow permissions on that OU but the same permissions on all of its child objects.

Keep in mind that if you got it to work with the app pool as a domain admin, then it works. Period. It is only a permissions issue. You are right, and don't doubt it. It's just a matter of getting those permissions right.

I just finished writing a book on this stuff and have been working on these settings (and much more) for months. I am always open to being wrong (as a matter of fact, if someone has a better way, \*please\* let me know) but this is what has worked for me. And sometimes, when push comes to shove, we can only do what we know works, regardless of what documentation has told us. Believe me, I know. ; )

And please don't be offended by this question, but is there a reason why you need to do Directory Management Service for incoming email? If push came to shove, would your environment support just doing incoming email without DMS's contacts and distribution groups in AD? Incoming email works great (really great) without DMS enabled at all. As a matter of fact I use enabling incoming email without DMS as a troubleshooting technique to isolate DMS problems all the time. I guess I am just trying to let you know if DMS is a pain, do without it. A lot of MS documentation says (or strongly implies) that you have to do DMS to do incoming email with is completely untrue.

-callahan

"Paul" <Paul@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message [news:5D08D12F-671B-477B-A910-5FADC5812A76@xxxxxxxxxxxxxxxxxxxx](mailto:news:5D08D12F-671B-477B-A910-5FADC5812A76@xxxxxxxxxxxxxxxxxxxx)

Thanks for your continued help callahan,

Re: Incoming E-Mail – cant create contact in OU

To better explain my situation, I am using WSS 3.0 and I have 3 WSS web servers connected to a SQL 2005 SP1 cluster.

On all WSS servers, the 2 application pools used are "Sharepoint Central Administration" and "SharePoint\_Company". Both of these application pools are running under the domain user account of "Domain\Sharepoint\_AppID"

The windows service "Windows Sharepoint Services Timer" is also running under this same domain user account "Domain\Sharepoint\_AppID"

On my domain controller, I launched AD Users & Computers and created a new OU called "Sharepoint". On this OU, I then delegated the rights for the same user "Domain\Sharepoint\_AppID" for Create, delete and manage user accounts.

I also added Read All user Info for kicks.

This is my understanding as the documented procedures to make this work.

I have also gone a step further and gone back to the OU and made the account "Domain\Sharepoint\_AppID" with full rights to the OU, and also made this account the local administrator to all WSS web servers.

I am still thinking the problem is this account "Domain\Sharepoint\_AppID" is not having enough rights to access AD in the first place, to even get to the OU level and perform its magic. Again, making this account a domain administrator solves the problem, but not something I am comfortable with.

"callahan" wrote:

Okay, lets see here, you are having problems getting DMS to work and you already have the application pool delegated rights to the OU. It worked when you had that account set as a domain admin for the domain, but not when it is a local admin.

In my experience it is because you didn't quite delegate enough rights to the account in the OU.

Also though, before we go further with that, Daniel was

Re: Incoming E-Mail – cant create contact in OU

wondering if you would delegate the same rights you gave the application account to the OU to the account that is being used for the central administration application pool.

(Actually, come to think of it, this does bring us to a little impasse.

There is a question we need to ask, and that is if you are running WSS 3

as

a single server install or a Web Front end, server farm install?)

I took it for granted (and probably so did Daniel) that you had a server farm installation of WSS because your application pool account was a domain account. I'm going to stay with that assumption until you tell us otherwise.

If your installation of WSS 3 is not a single server installation, then the application pool account for Central Administration (which is considered

the

Farm account because it also is the account that runs the Sharepoint

Timer

Service, and is critical to the functioning of a sharepoint server farm)

also may need access to the OU. You can figure out what account that is

a

couple of different ways: check what account identity the Sharepoint

Timer

service is running in the services MMC; or open IIS, go to the Central

Administration's application pool's identity is.

Once you figure out what that account is, you could try delegating it

rights

to the OU. Specifically, don't forget to delegate it delete rights so it

Re: Incoming E-Mail – cant create contact in OU

can  
delete things from the OU if need be.

Overall, I suspect that what happened was that you did not delegate enough rights to your web application's application pool at the OU. Instead of using the delegate control wizard, you might want to go to the View menu in the ADUC MMC and select Advanced features. That will let you, when you right click the OU, go to properties and see the Security tab (that you can't see without the advanced features view enabled). In the security tab you can see the permissions that are available. Check the domain admins rights, then click the Advanced button at the bottom. Notice that the domain admin actually has much more than just the standard full control of the OU (which is above what you might've given the account originally— while a domain admin they get stuff that trumps that delegate control you gave it), they have control of all child objects under the OU as well (not because domain admins explicitly get that but because they are members of the Administrator's group that gets that). It's the domain admin like control that you need to give the app pool so it can do its work with the OU— \*without\* giving it that kind of control elsewhere in the domain.

Please check that out and see if it works for you. Don't give up hope, I have it working with Exchange 2003 in several places without the application pool being a domain admin. The permissions on this thing are tricky but it can be done.

Re: Incoming E-Mail – cant create contact in OU

So— make sure you application pool for your web application that contains the sites that will using incoming email has the correct advanced rights for the OU.

-- make certain that your central administration app pool account has rights to the OU.

-- make certain that you do an IISRESET /noforce after you make any changes to the settings in the OU or in sharepoint. You will not see any results of your changes in sharepoint for up to 15 minutes (in my experience) after you make them unless you force it by using IISRESET.

-callahan

"Paul" <Paul@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message

[news:FFBE285C-FF21-4CC5-910C-73D74F2677C9@xxxxxxxxxxxxxxxxxxxx](mailto:news:FFBE285C-FF21-4CC5-910C-73D74F2677C9@xxxxxxxxxxxxxxxxxxxx)

I apologize if I dont understand your suggestion. My current/initial setup is delegating the application pool rights to the OU, and that doesnt seem to work.

Today I have added the application pool account as a local administrator to all my WSS 3.0 boxes, and rebooted the boxes to be entirely sure.

I then enabled email, and logged into my sharepoint site and attempted to add an email to a discussion and it still fails.

I am pretty sure its an AD/OU issue, not a

Re: Incoming E-Mail – cant create contact in OU

local WSS issue. Reason?  
Because  
if I add the Application Pool user to Domain  
Admins, it then works.  
There  
is  
something missing in AD or possibly  
Exchange rights that is not  
allowing  
WSS  
to create the contact in an OU. Again, to  
confirm – I am delegating  
rights  
to the new OU for my sharepoint application  
pool user account.

"Daniel Bugday" wrote:

Paul,  
i think you have to follow  
callahans suggestion of  
adding the account  
to  
the  
local admin froup of that  
server.

Could you try one other  
thing..

Try to delegate permission  
to the account which is  
running the IIS  
pool  
for  
the central administration  
site without adding to admin  
group and then  
do  
an  
IISReset.

/Daniel Bugday

"callahan"  
<cacallahan@xxxxxxxxxxxxxxxxxxxx>  
wrote in message  
[news:%23NTN2SR7HHA.4436@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:%23NTN2SR7HHA.4436@xxxxxxxxxxxxxxxxxxxxxxxx)

Re: Incoming E-Mail – cant create contact in OU

The application pool account, in my experience, must be a local admin of the sharepoint server that is doing incoming email and hosting DMS.

Also the account must have those permissions to all the child objects for that OU as well.

In addition, if you are going to do approval for the groups, I found that I had to give the farm account rights to the OU as well in order to be able to delete a group. Please let me know if that is the case for

Re: Incoming E-Mail – cant create contact in OU

you.

Frankly, I  
am  
impressed. I  
personally  
have never  
gotten it to  
work  
with  
Exchange  
2007.

–callahan  
"Paul"

<Paul@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

wrote in  
message

[news:E9308C36-1A8C-4071-93EB-BAB58A0C7DD8@xxxxxxxxx](mailto:news:E9308C36-1A8C-4071-93EB-BAB58A0C7DD8@xxxxxxxxx)

Running  
Windows  
2003  
R2  
AD,  
Exchange  
2007  
and  
WSS  
3.0.

I  
have  
WSS  
website  
application  
pool  
running  
as  
a  
domain  
user  
account,  
not  
network  
service.  
I  
created  
an  
OU  
called

Re: Incoming E-Mail – cant create contact in OU

Sharepoint  
and  
delegated  
rights  
to  
this  
user  
account  
(Create,  
delete  
and  
manage  
user  
accounts  
+  
Read  
All  
User  
Information).

When  
I  
create  
a  
site  
and  
attempt  
to  
enable  
email,  
it  
gives  
me  
"Error  
in  
the  
application."  
"

However  
to  
prove  
its  
a  
permission  
issue,  
I  
then  
added  
this  
website

Re: Incoming E-Mail – cant create contact in OU

application  
pool  
account  
to  
domain  
admins,  
rebooted  
my  
WSS  
to  
be  
sure  
and  
tried  
again  
–  
now  
it  
works!  
Obviously  
I  
dont  
want  
to  
run  
this  
as  
domain  
admin,  
so  
removal  
of  
domain  
admin  
kills  
the  
ability  
to  
add  
email.

There  
must  
be  
other  
AD  
OU  
permissions  
that  
are  
not

Re: Incoming E-Mail – cant create contact in OU

listed  
in  
the  
Microsoft