

# Re: ADFS with ASP application

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2007-01/msg01786](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-01/msg01786)

---

- *From:* "Joe Kaplan" <[joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 23 Jan 2007 10:00:25 -0600
- 

Mapping an incoming group claim to a user in the resource forest is one way to do it. You basically have three options:

- Map user to user via the userPrincipalName attribute (this can go through a transformation on the UPN suffix if needed)
- Map inbound group to single user
- Map inbound group(s) to groups in resource forest to create a token that doesn't belong to any specific user in the resource forest but allows authorization based on group SIDs

I think the first option isn't really that useful, as you have to provision "shadow" users for each potential federation user and that (to me) defeats much of the purpose of federation. The other two options are more interesting, with the third being the most flexible but the most complex as well.

I have no idea what is going wrong with your app, but I'd suggest trying to figure out why it is hanging. There really isn't anything wrong per say with doing redirects and such, but you'd need to stay within the same ADFS-protected application.

Joe K.

--

Joe Kaplan-MS MVP Directory Services Programming  
Co-author of "The .NET Developer's Guide to Directory Services Programming"  
<http://www.directoryprogramming.net>

--

<[rajendersaini@xxxxxxxxxx](mailto:rajendersaini@xxxxxxxxxx)> wrote in message  
[news:1169563760.730904.294040@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:1169563760.730904.294040@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

Hi Joe

thanks for your help .

Now I am able to bring up the token app .To make it working I went to account partner and in UPN mapping i went to group tab and mapped incoming group claim to user on resource computer .Is it correct ?

## Re: ADFS with ASP application

The real asp application which i mapped has a default page which is doing many redirection to webserver and downloads .js and .vbs files ,currently it hangs there . Can we do this kind of redirection in adfs enabled web application ?

Thanks

Rajender saini

Joe Kaplan wrote:

If ADFS is properly enabled on the resource application, you should not be able to bypass ADFS to get into the application. Make sure the ADFS web agent is enabled properly (although it sounds like it is if you got redirected to log in).

Generally, when you get errors from ADFS on the federation server side, there will be a useful error message in the event log. If not, there should be a useful error message in the detailed tracing logs. Make sure you have that enabled and turned all the way up.

When troubleshooting token based apps, you obviously can't turn on logging with web.config. Instead, there are registry settings that enable this. They are documented in the troubleshooting section of the ADFS Operations Guide on Technet. Turn everything on. :)

My experience with token apps that blow up in this manner is that usually, the SAML token doesn't contain a user that can be mapped or any groups that can be mapped to resource groups, so ADFS gives up and attempts to log in the user as "NT AUTHORITY\ANONYMOUS" (null token). However, ASP and ASP.NET don't like this at all and simply blow up. :) I'm not convinced that this default behavior of ADFS is good, but I also don't know what else they should do here.

The important thing is that when you have to shadow something valid. If you are using shadow users, there HAS to be a user with a matching UPN in the resource forest. If you are using shadow groups, there has to be at least 1 group claim in the SAML token that maps to a resource group in the organizational claims of the resource FS forest. If not, you'll have

Re: ADFS with ASP application

these  
problems.

It is generally much easier to troubleshoot this with a claims app first using the standard test page.

Also, make sure you didn't forget to enable a claim somewhere. I've had the "doh!" moment many times where added a claim but forget to enable it for the apps I needed to have use it and they were never getting it.

Looking in the logs to see the detailed SAML token for the user is also very helpful.

Good luck!

Joe K.

---

Joe Kaplan—MS MVP Directory Services Programming  
Co-author of "The .NET Developer's Guide to Directory Services Programming"

<http://www.directoryprogramming.net>

---

<rajendersaini@xxxxxxxx> wrote in message  
<news:1169217713.440833.293720@xx>

Hi Joe

I am also trying to set up adfs for token base application .I followed the same steps as mentioned in above conversation.

I have used shadow group mapping. I am able to see the discovery page from client computer .But when I select the account domain and click submit .It fails on resource computer saying could not verify credential

and on web page is throws error "Server error /adfs "

"ASP.NET" does not have access permission to /adfs/ls ...bla bla

When I try to access the application from "Web computer (where token app is hosted )" ,by logging in as terrya .I am able to access

Re: ADFS with ASP application

application !!

I have gone through logs on both adfs server it seems that clients adfs sends users credential and groups info correctly .Problem lies with resource computer ...

Can you help me ? how to move further .

Thanks

Rajender saini

Joe Kaplan wrote:

Did you try the token test page I have here:

<http://www.joekaplan.net/DiscoveringTheUsersNameAndGroupsInTheirWindowsTok>

I like it better than the approach Nick outlines, although either should work.

In a token-based app, the token can be mapped from the ADFS SAML token in one of two ways. ADFS will either find the user's UPN in SAML token and look up that user in AD and create a Windows token for that user (with all of their groups) using protocol transition/S4U (or the custom auth package if your AD in 2000 instead of 2003 FFL), OR ADFS will look at the SAML token and attempt to build a custom Windows token based on the group claims in token that correspond to organizational claims in the resource federation server that map to resource groups in AD.

Re: ADFS with ASP application

This mapping is often referred to as "shadow users" or "shadow groups" in the ADFS docs and presentations.

When you log in with a user defined in the resource federation server's user store, only the direct user mapping will be performed, but if you log in with a user from an external account partner, the type of mapping done is configured in the properties for the account partner in the resource federation server and you have 4 options on that tab.

If you go with shadow users, the user's UPN in the SAML token must exist in the resource federation server's AD and if you go with shadow groups, the SAML token must contain at least 1 group claim that maps to an organizational group claim with mapping to a security enabled group in AD.

This part of ADFS is really powerful, but also very confusing, so hopefully this helps and doesn't confuse you more. :)

Joe K.

--  
Joe Kaplan—MS MVP Directory Services Programming  
Co—author of "The .NET Developer's Guide to Directory Services Programming"  
<http://www.directoryprogramming.net>

--  
<viveque.kumar@xxxxxxxx> wrote in message  
[news:1168411494.482859.284300@xx](mailto:news:1168411494.482859.284300@xx)

Re: ADFS with ASP application

Hi Joe,

We were facing issues with setting up the undermentioned page itself, the 'sids' object is coming up as null .

I think we are stuck with Claims as far as setting up ADFS in conjunction to the step-by-step guide. I am now using the non-sharepoint token-based app setup as described in Nick's blog. We get till the discovery page and after selecting the realm, asp error page appears where in it says the credentials could not be verified at the resource partner adfs web site.

Will setting up claims only as much is asked in the step-by-step document suffice? I read in some posts of your's that you don't quite follow that and set up UPN-UPN claims instead, could you pls help me set up the claims? In production we will need group mapping but for now I am ok with any setting.

Another question is what should be the security level at ADFS site, when it gets installed (after installing ADFS) the default permissions are anon on both the sites,

Re: ADFS with ASP application

but that does not work and  
the error  
description on the adfs error  
page prompts to set it to  
Integrated,..  
Just wanted to make sure it  
is expected to be set at  
that??

Thanks a lot,  
– Vivek

Joe Kaplan wrote:

The first  
thing I'd do  
is set up the  
test page  
that I  
discuss in  
this  
blog  
posting so  
you can see  
what  
Windows  
token is  
being  
created by  
ADFS  
as  
a  
result of the  
federated  
login. That  
will help  
you figure  
out  
what's  
going  
on so you  
can apply  
that  
knowledge  
to to the  
ASP app  
(which is  
likely  
more  
difficult to  
troubleshoot

Re: ADFS with ASP application

as you don't  
has this  
kind of easy  
access  
to  
the  
authenticated  
user's token  
like you do  
in .NET).

<http://www.joekaplan.net/DiscoveringTheUsersNameAndGroupsInTh>

Joe K.

--

Joe  
Kaplan-MS  
MVP  
Directory  
Services  
Programming  
Co-author  
of "The  
.NET  
Developer's  
Guide to  
Directory  
Services  
Programming"  
<http://www.directoryprogramming.net>

--

<viveque.kumar@xxxxxxxx>

wrote in  
message

<news:1168277603.416111.172830@xx>

Hi  
Joe,  
I  
followed  
the  
step  
by  
step  
guide  
to  
achieve  
the  
token-based  
authentication

Re: ADFS with ASP application

but  
we  
were  
not  
successful  
in  
doing  
so.  
Could  
you  
mail  
me  
some  
steps  
that  
you  
might  
have  
tried  
on  
your  
own.

Thanks  
in  
advance,  
Vivek

Joe  
Kaplan  
wrote:

ADFS  
can  
work  
here  
if  
you  
use  
the  
Windows  
token  
model  
for  
integration  
(using  
the  
stuff  
integrated  
into  
the

Re: ADFS with ASP application

IIS  
MMC  
UI).  
In  
that  
mode,  
ADFS  
can  
work  
with  
any  
app  
that  
runs  
on  
IIS.  
The  
app  
doesn't  
need  
to  
be  
.NET  
2.0  
(although  
.NET  
2.0  
must  
be  
installed  
on  
the  
machine  
for  
ADFS  
to  
be  
installed  
and  
used).

You  
would  
change  
the  
setting  
in  
IIS  
from  
integrated  
to

Re: ADFS with ASP application

anonymous,  
but  
ADFS  
would  
actually  
create  
a  
Windows  
token  
for  
you  
with  
the  
ADFS  
agent  
and  
the  
app  
would  
continue  
to  
function  
as  
if  
it  
was  
working  
like  
integrated  
auth.

The  
real  
trick  
here  
is  
coming  
up  
with  
a  
viable  
strategy  
for  
how  
you  
want  
to  
map  
user  
tokens  
(shadow

Re: ADFS with ASP application

users  
or  
shadow  
groups).

Joe  
K.

--  
Joe  
Kaplan-MS  
MVP  
Directory  
Services  
Programming  
Co-author  
of  
"The  
.NET  
Developer's  
Guide  
to  
Directory  
Services  
Programming"  
<http://www.directoryprogramming.net>

--  
<viveque.kumar@xxxxxxxx>  
wrote  
in  
message  
<news:1168012536.605350.251840@xxxxxxxxxxxxxxxx>

Hi,

We  
have  
a  
legacy  
ASP  
application  
and  
we  
are  
looking  
at  
SSO  
for  
an  
integration  
project.

Re: ADFS with ASP application

Our application works on Integrated authentication mechanism and the requirement is that users from other domains when accessing this application need not sign in again.

So after some research I stumbled upon ADFS to achieve this.

My question is this, given the above scenario, will ADFS work here?

Re: ADFS with ASP application

Doesn't  
ADFS  
require  
ASP.NET  
applications?  
Will  
the  
application  
security  
settings  
need  
to  
be  
changed  
from  
Integrated  
to  
Anonymous?

TIA,  
–  
Vivek