

Re: ADFS Proxy Error

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-01/msg02306

- *From:* Eric <Eric@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 29 Jan 2007 07:59:00 -0800
-

Thx Joe, I have it working now. Everything was set up write I just needed to reinstall in .Net Framework now it works like a charm.

"Joe Kaplan" wrote:

Answering the second question first, it is the app that is responsible for redirecting the client to the logon site. You don't have to do some sort of "click-through". The flow looks like:

app -> resource FS (home realm discovery if needed) -> account FS -> resource FS -> app

The redirect from the account FS to the resource FS is a POST redirect of the SAML token (done with a little javascript trickery), as is the redirect from the resource FS back to the app. The second POST redirect is basically where the resource FS gets a chance to change the claims in the token and issues a new token from it. This makes it such that the app only has to trust its resource FS and doesn't have to trust anyone else. It is the resource FS only that is responsible for trusting all of its account partners.

On to the error...

Unfortunately, I don't know quite what the problem is. On the FS-P, the clientlogon.aspx is different from the FS in that it shows the forms-based logon page. If that page is the name of the page designated in the FS as the logon page, then that will get displayed when a sign on is requested (unless ADFS basic auth must be used instead, but that's a picky detail here).

I'd generally hope that the error would at least have a stack trace in it that would provide more details or you'd see a more interesting error page.

Make sure you have your ADFS file-based logging enabled and cranked all the way up and then check to see if you get any interesting details in the log file. Oftentimes, the important stuff that actually tells you how to resolve an error.

Re: ADFS Proxy Error

I've never actually used the FS-P yet (I did steal the clientlogon.aspx to use on the FS to enable ADAM logon), so I'm not real deep on it, but I have debugged a myriad of other ADFS issues and am hopeful we can figure this one out too. :)

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>

--

"Eric" <Eric@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:0DEF92C5-9D08-4D78-A278-A9FCF5AC40BC@xxxxxxxxxxxxxxxxxxxx>

I am trying to bring a proxy server into my ADFS test environment. I don't really have a dmz but I am trying to create one using host records to simulate the DNS entries required.

On my test client I have a host file entry to redirect any requests to my FS to my FS-Proxy. That seem to be working correctly from the log files I have looked at on my proxy.

My FS-Proxy is picking up the actual ip, from it's DNS server, to the FS for which it is proxying when I use a ping test.

The error I am getting is an ASP.Net Event ID 1309 occurring on the FS-proxy. Below is the ierror that is shown in the event viewer.

Event code: 3005
Event message: An unhandled exception has occurred.
Exception information:
Exception type: HttpUnhandledException
Exception message: Exception of type 'System.Web.HttpUnhandledException' was thrown.
Request information:
Request URL: <https://ridev-adfs01.test.dev/adfs/ls/clientlogon.aspx>
Request path: /adfs/ls/clientlogon.aspx
User host address: xxx.xxx.xxx.104
User:
Is authenticated: False
Authentication Type:
Thread account name: NT AUTHORITY\NETWORK SERVICE

The error is pretty vague. I there something I missed in IIS? I certs I believe are correct as I am using the same cert on both my FS and my

Re: ADFS Proxy Error

FS-Proxy

as mentioned in other discussions. Any assistance will be appreciated.

An additional question is when I have outside clients trying to access Federated Web sites and Apps directly, will the web agents automatically redirect the authentication requests through proxy or will all outside clients

have to first enter the url of the FS-proxy to authenticate before try to access any of the apps or sites protect by federated services? I am trying

to get a good picture of the information flow for a proxy configuration as opposed to one without.

Thanks,
Eric