

## Re: ADFS June 2006 Step-by-step guide

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2006-08/msg01226](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-08/msg01226)

---

- *From:* Noremac <[Noremac@xxxxxxxxxxxxxxxxxxxx](mailto:Noremac@xxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 1 Aug 2006 15:16:02 -0700
- 

I will turn on the extra logging to the log files and go over what you said. In the mean time, this is the Security Failure Audit that it generated on the resource web server:

The client presented a valid XML token, but an error occurred during the attempt to generate a Windows NT token from the security IDs (SIDs). The error code was 1317.

Token ID: \_857d7b3b-3d41-4460-94c1-f667a9c36e0b

Issuer: urn:federation:treyresearch

Identity: alansh@xxxxxxxxxx

Error code: 1317

Nothing showed up on a google search. I am sure it is something silly on my part. I may try and see if I can get the claim-app working since that is not mixed up with Sharepoint in the step-by-step guide.

"Joe Kaplan (MVP - ADSI)" wrote:

Under ADFS, the app (site or virtual directory) needs to be set to anonymous auth. The ADFS web service extension actually "intercepts" the request and creates a Windows security token based on the claims in the FS token for IIS to use before your code actually gets to execute against the request. The whole "anonymous" thing in IIS takes a little getting used to, but that's the way a lot of other SSO products like this actually work.

The contents of the windows token you'll get depends entirely on the claims supplied to the app from ADFS and the type of user mappings you are allowing in your trust policy. If you are allowing only user to user mapping, then the claim must contain a UPN claim that matches the UPN of a user in your forest. If you just allowing groups, then the user must have at least one resource FS claim with a resource group associated with it their federation token. There are also the hybrid settings as well.

Typically, I use user-to-user for accounts in the resource FS and use groups-only mapping for users fro