

## PHP AD LDAP Authenticator - Bug # 363: Subdomain accounts give error "User does not have a email address in AD"

<b>Status:</b>	New	<b>Priority:</b>	Normal
<b>Author:</b>	Northwestern State University	<b>Category:</b>	
<b>Created:</b>	17 Feb 2014	<b>Assignee:</b>	
<b>Updated:</b>	21 Feb 2014	<b>Due date:</b>	
<b>Subject:</b>	Subdomain accounts give error "User does not have a email address in AD"		
<b>Description:</b>	<p>We have multiple domains. One primary domain, and sub domains of that primary. All of our accounts use email addresses and UPNs as though they are in the primary domain. For example the following two users</p> <pre># primary\user1 - user1@primary # sub1\user2 - user2@primary</pre> <p>Rather than sub1\user2 having an email/UPN of user2@sub1.primary</p> <p>We have configured the plugin to look to our main Active Directory servers, and configured it with the global port: \$ad_port = 3268</p> <p>Accounts in the primary domain log in fine. However we get the error "User does not have a email address in AD" for sub domain users. Even though the mail field is populated when doing an LDAP search against the global catalog. The logs show success in authenticating the user:</p> <pre>[02-17-14 - 13:22] ldap_account_suffix: '@primary' [02-17-14 - 13:22] ldap_base_dn: 'DC=primary' [02-17-14 - 13:22] ldap_domain_controllers: array (   0 =&gt; 'server1.primary',   1 =&gt; 'server2.primary', ) [02-17-14 - 13:22] KAYAKO_LDAP_TEST: false [02-17-14 - 13:22] Authenticated: true [02-17-14 - 13:22] Type: Empty (Default to user) [02-17-14 - 13:22] User does not have a email address in AD [02-17-14 - 13:22] -----[ Session End ]-----</pre> <p>A global catalog search of the user should return all the fields necessary for authentication to take place, but somewhere in the code this plugin is not looking up that information properly.</p> <p>Due to our UPN/email information matching for each of the domains if we try to list both domains in \$ldap_domain_info and \$ldap_domain_controllers, only subdomain users can login, not primary domain users. This is due to the key for both domains being the same and thus being overwritten:</p> <pre>\$ldap_domain_info = array ( '@primary' =&gt; 'dc=primary', '@primary' =&gt; 'dc=sub1,dc=primary')</pre>		

### History

#### 02/21/2014 04:37 pm - Bryan Heath

I am not sure if I know of a good way to fix your problem.

Sounds like adLDAP is having a problem looking up your mail from your subdomain. I tried researching your problem but I do not see anything that suggests the same issue before with their library. With out the ability to research the problem I am not sure what I can do to assist. Which I will be more than happy to do if you want to set me up with the ability to look at your issue. You can contact me directly if you want to proceed with that.

Probably the best way to solve the problem with the current problem would be to rewrite the authentication so it checks for those elements before passing the authentication check. Maybe even writing it so it combines the results of both attributes to see if it can form a proper result. However again with out the ability to test and work on this properly I don't see me doing anything on this.

