

## Re: Domain Trusts and LDAP

**Source:**

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2005-01/0855.html](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-01/0855.html)

---

**From:** Chriss3 [MVP] (*noSpamHere\_at\_chrisse.se*)

**Date:** 01/13/05

Date: Thu, 13 Jan 2005 17:42:24 +0100

Another solution may could be to use ADAM (Active Directory in Application Mode) for the web application, and create ProxyUser Accounts that relays to an Account in the Active Directory but thats not really secure.

For security reasons I recommend you to use IIFP Identify Integration Feature Pack for synchronize accounts between the external and internal domain. Trusting Domains/Forests are not secure. IIFP is free as long you have a copy of Windows Server 2003

--

Regards

Christoffer Andersson

Microsoft MVP - Directory Services

No email replies please - reply in the newsgroup

-----  
<http://www.chrisse.se> - Active Directory Tips

"GMartin" <gmartin@gmartin.org> skrev i meddelandet  
news:emcCvAY%23EHA.1604@TK2MSFTNGP12.phx.gbl...

> We're building an AD infrastructure to authenticate users of our external  
> web via LDAP. We already use AD internally. We need a mechanism to allow  
> internal users to authenticate to the external system without creating new  
> credentials for them.

>

> My idea is to create one-way trust from the external domain to the  
> internal domain. This should allow one-stop shopping for the  
> authentication (vs. LDAP referral and a hole in the firewall from the app  
> svr to the internal AD). I think this will work, but I have several  
> questions

>

> 1 - How do we authenticate? We typically do a search & bind to  
> authenticate against LDAP. If I understand correctly, the search would  
> not work as the external AD wouldn't search the internal. Would we use  
> UPN?

>

> 2 - When we create an account externally, how can we ensure (dow e need to  
> ensure) the account is unique in both domains (I guess is we use UPN this  
> wouldn't matter)

>

> Thought on these or other suggestion on approaching the problem?

>

> \\Greg