

# Re: What LDAP Ports thru DMZ

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2006-09/msg00041.html>

---

- *From:* "Joe Kaplan" <[joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Mon, 11 Sep 2006 15:35:30 -0500
- 

At a minimum you need port 389 to query the domain and 3268 to query the global catalog. If you will use SSL/LDAP, you need 636 and 3269 respectively.

Depending on the type of authentication you will do to AD, you may also need Kerberos (port 88 TCP and UDP) and may need RPC (135 at a minimum).

When you say the LDAP server will be in the DMZ, are you setting up some kind of LDAP proxy server or are you saying that the LDAP client application (like a web server) will be in the DMZ? Generally you wouldn't need a different LDAP server to talk to AD, although I suppose you could do that.

There is also another way to communicate with AD using the DSML server. It allows you to make HTTP/SOAP calls to a web server that is essentially an LDAP proxy. In that case, your firewall issues are just standard HTTP things (80/443) if you put the DSML server behind the firewall. There is a fairly straightforward way to program this if you are using .NET 2.0 and the System.DirectoryServices.Protocols namespace.

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>

—  
"Chris Davoli" <[ChrisDavoli@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:ChrisDavoli@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
[news:629D56D8-DAA7-40FD-8F70-8DE6204CFB09@xxxxxxxxxxxxxxxxxxxxx](mailto:news:629D56D8-DAA7-40FD-8F70-8DE6204CFB09@xxxxxxxxxxxxxxxxxxxxx)

I am going to use LDAP to look up userids on an active directory server.  
The  
LDAP server is on the outside in the DMZ. The Active Directory server is  
on  
the inside, so holes need to be poked into the firewall. My question is,  
what  
ports need to be poked into the firewall so I can read active directory?

—  
Chris Davoli

Re: What LDAP Ports thru DMZ