

# Kerberos authentication

---

*Source:*

[http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active\\_directory/2007-02/msg00572](http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2007-02/msg00572)

---

- *From:* Jorge Azcuy <[JorgeAzcuy@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:JorgeAzcuy@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 7 Feb 2007 06:44:01 -0800
- 

This issue is occurring in a Windows 2003 R2 AD environment with Windows XP SP2 workstations. We have a NAC device that acts as a firewall before a user is authenticated and the pc passes a security check. Before authentication, the following ports are open to the 2 Domain Controllers:

TCP: 53,88,123,135,139,389,445,636,1025,1600,1601,3268,3269

UDP: 53,88,135,137,138,389,445,636,3268

TCP 1600 and 1601 are the ports we have limited RPC traffic to according to <http://support.microsoft.com/kb/154596/>

Everything works fine, until we set a user's home directory to a mapped drive on a file server. The following traffic is allowed to the File Server pre-authentication:

TCP: 135,139,445

UDP: 135,137,138,445

The issue occurs with about 30% of users. The 'Applying Personal Settings' screen goes on for over 5 minutes, and the following event log errors are logged:

Event Type: Warning  
Event Source: LSASRV  
Event Category: SPNEGO (Negotiator)  
Event ID: 40960  
Date: 2/7/2007  
Time: 8:26:59 AM  
User: N/A  
Computer: xxxxxxxx  
Description:

The Security System detected an attempted downgrade attack for server LDAP/Axxxxxxx.com. The failure code from authentication protocol Kerberos was "There are currently no logon servers available to service the logon request. (0xc000005e)".

## Kerberos authentication

Event Type: Warning  
Event Source: LSASRV  
Event Category: SPNEGO (Negotiator)  
Event ID: 40961  
Date: 2/7/2007  
Time: 8:26:59 AM  
User: N/A  
Computer: xxxxxxxx  
Description:  
The Security System could not establish a secured connection with the server LDAP/xxxxxxxxxx.com. No authentication protocol was available.

When this first occurred, I followed the steps on <http://support.microsoft.com/kb/244474> to force Kerberos authentication to use TCP instead of UDP. For this particular user, this issue was resolved, so I pushed the registry changes throughout the network.

However, this morning, multiple users reported the same logon issue and generated the same event log errors even with Kerberos using TCP.

If I remove the Home Directory mapping from the user's profile, everyone can logon without any problems.

Any help would be greatly appreciated.