

## Event ID 680 – 529 in Server Security Log

**Source:**

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.general/2004-11/1602.html>

---

**From:** ServerDude (*ServerDude\_at\_discussions.microsoft.com*)

**Date:** 11/19/04

Date: Fri, 19 Nov 2004 12:29:05 -0800

Server 2003 and Windows XP SP2.

When I am logged into a PC with a local XP user account I am getting hundreds of logon failures in my Server security log – Events 680 and 529. The PC is part of the domain, but the local user is not.

Events in detail:

---

Date: 11/19/04

Time: 11:48:19AM

Type: Failure Aud

User: NT AUTHORITY/SYSTEM

Computer: (Domain Controller)

Source: Security

Category: Account Logon

Event ID: 680

Description:

Logon attempt by: MICROSOFT\_AUTHENTICATION\_PACKAGE\_V1\_0

Logon account: (Any local user account currently logged in)

Source Workstation: (PC Name)

Error Code: 0xC000006A

---

Date: 11/19/04

Time: 11:48:19AM

Type: Failure Aud

User: NT AUTHORITY/SYSTEM

Computer: (Domain Controller)

Source: Security

Category: Logon/Logoff

Event ID: 529

Description:

Reason: Unknown user name or bad password

    User Name: (Any local user account currently logged in)

    Domain: (PC Name)

    Logon Type: 3

    Logon Process: NtLmSsp

    Authentication Package: NTLM

    Workstation Name: (PC Name)

There are groups of 48 Event failures recorded during the same second. This occurs randomly throughout the entire day.

I have read some posts regarding possible attacks using generic usernames but that cannot be the case here. I can configure a fresh install using a completely unique username, add the PC to the domain, and in a little while there are 48 failures from this username in my server security log. Microsoft Article 811082 seems to be similar but this is using a different Logon Process and these occur while logged in – not during the logon or logoff action.

I have read about issues with NTLM and 2000 mixed mode environments but I am running Server 2003.

I am still running at the interim functional level because of some older PC™s on the domain. I don™t get errors from those older PC™s, only from XP local users.

Has you seen this?  
Any suggestions?

Thanks.  
ServerDude