

# Troubleshooting Server Message Block Inbound Connection Limit in Windows Peer-to-Peer Workgroup

The information in this article applies to:

- Microsoft Windows XP Home Edition
  - Microsoft Windows XP Professional
  - Microsoft Windows 2000 Professional
  - Microsoft Windows NT Workstation 4.0
- 

This article was previously published under Q328459

**IMPORTANT** : This article contains information about modifying the registry. Before you modify the registry, make sure to back it up and make sure that you understand how to restore the registry if a problem occurs. For information about how to back up, restore, and edit the registry, click the following article number to view the article in the Microsoft Knowledge Base:

[256986](#) Description of the Microsoft Windows Registry

## SYMPTOMS

In a peer-to-peer workgroup, when you try to connect to the network resources of a computer that is running any of the products listed at the beginning of this article, you may receive either of the following error messages:

Operating system error 71.

No more connections can be made to this remote computer at this time because there are already as many connections as the computer can accept.

-or-

System error 71 has occurred.

This remote computer has reached its connection limit, you cannot connect at this time.

## CAUSE

A Windows client workstation may have opened a pipe connection to the named pipe \PIPE\spoolss on either a print server or a workstation that has a shared printer. This typically occurs when you start a program (such as Microsoft Word) that queries printers, or if you open the Printers folder in Control Panel. Printer spooling on both the client and the server will open a handle related to this connection.

A Remote Procedure Call (RPC) requires one named pipe instance for every active RPC call (like OpenPrinter). If an OpenPrinter call stops responding, RPC keeps open the named pipe connection. RPC does not disconnect this connection until the context handle (that is OpenPrinters) has been closed.

If both the following conditions are true, you may open an anonymous connection (also known as *null session connection*) that never closes to the named pipe \PIPE\spoolss on the workstation that acts as the server in your peer to peer network:

- Your client has connected a shared printer on the computer that acts as a 'print server'.
- You have set up a local shared printer on one or more clients.

## RESOLUTION

Use one of the following methods to restrict null session connections on your workstation that is acting as a print server. The preferred method is the first one.

### Method 1

Disable null session connections on the Windows computer that exceeds its incoming connection limit and shows some additional null session connections either by using the Group Policy GUI or by setting a registry key.

### Using the Group Policy User Interface (Local Security Policy MMC Snap -In)

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Local Security Policy**.

**NOTE:** If you cannot perform this step because **Administrative Tools** does not appear in the **Program** list, click **Start**, point to **Settings**, point to **Control Panel**, double-click **Administrative Tools**, and then click **Local Security Policy**.

2. In **Security Settings**, double-click **Local Policies**, and then click **Security Options**.
3. Double-click **Additional restrictions for anonymous connections**, and then under **Local policy setting:**, click **No access without explicit anonymous permissions**.
4. Restart the computer.

This policy restricts null session connections.

## Using Registry Editor

**WARNING:** If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

To restrict null session connections (or disable null session access):

1. Start Registry Editor.
2. Locate, and then click the following key in the registry:

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\LSA**

3. On the **Edit** menu, click **Add Value**, and then add the following registry value:

Value Name: **RestrictAnonymous**  
Data Type: **REG\_DWORD**  
Value: **2**  
Default: **0**

A value of 2 restricts null session connections.

To set the **RestrictAnonymous** value, change the registry key to 0 or 1 for Windows NT 4.0 or to 0, 1, or 2 for Windows 2000. These numbers correspond to the following settings:

- 0 None. Rely on default permissions.
  - 1 Do not allow enumeration of SAM accounts and names.
  - 2 No access without explicit anonymous permissions
4. Restart the computer.

## Method 2

Use the following method to avoid null session connections that have a high session idle time and that have opened a handle to the named pipe \PIPE\spoolss.

## Remove Printer Share on Clients

Identify clients that have local printer shares enabled (see the "More Information" section for additional information) and remove all local printer shares on these computers:

1. Open the **Printers** folder to verify whether you have shared a local printer.
2. Open the **Properties** window of the shared printer, and then click **Sharing**.
3. Click to select the **Not Shared** option.

## STATUS

Microsoft has confirmed that this is a problem in the Microsoft products that are listed at the beginning of this article.

## MORE INFORMATION

Computers that run Windows NT Workstation 4.0, Windows 2000 Professional, and Windows XP Professional are licensed for a maximum of 10 concurrent client incoming sessions. Computers that run Windows XP Home Edition are licensed for a maximum of 5 concurrent client incoming sessions. All logical drive, logical printer, and transport level connections combined from a single computer are one session.

If the server service already has the maximum number of open sessions and one more user tries to allocate a resource, the computer returns the error messages that are described in the "Symptoms" section of this article.

Typically a computer does not have multiple sessions to another computer. But there are exceptions. For example, computer A is running a service under another user context than the logged-on user, and that service creates a logical connection to computer B. The logical connection can result from file shares, printers, serial ports, and also from communication between computers using named pipes and mail slots.

Use the following commands to get information about sessions and open files and shared resources.

### Information About Active Sessions on the Computer That Is Running the Server Service

To receive information about active sessions on the computer that is running the server service, type the following command:

```
net session
```

Count the number of open sessions to see if the session limit of 10 (or 5 in the case of Windows XP Home Edition) is already reached. Typically there is only one session per remote client.

If there is more than one session from a remote client, view the **User name** context on the remote client that has set up more than one session:

- View all the services that are running, and find out if one is running under the user context of the username shown in the session table.
- Look for scheduled tasks that are running in a logon script and are using a different user account than the one logging in.
- Look for rows where the **User name** column is empty and examine the idle time.

A session that has an empty user context is a *null session*.

Temporary null sessions are usually caused by IPC\$ connections as the first step in establishing a connection. They stay active for 30 seconds to 90 seconds.

**NOTE:** To disconnect client computer sessions, use the following command:

```
net session /delete \\computername
```

This command disconnects all sessions from that computer and closes all open files. This command may cause data loss if open files that have not been saved are closed.

### Information About Open Files

To receive information about open files, on the computer that is running the server service, type the following command:

```
net files
```

If you have seen permanent null user sessions in the session table, determine which file or pipe the null user is using.

### Information About NetBIOS Connection Table

To see a listing of incoming and outgoing connections and the amount of traffic carried on these connections, type the command:

```
nbtstat -s
```

### Information About Shared Resources

To see file shares, hidden administrative shares and shared printers, type the following command:

```
net share
```

You may have to perform further troubleshooting to determine the causes for multiple client sessions.

Use Network Monitor to find out which component initiates an additional session and what security context is used for the Server Message Block (SMB) session. To filter the traffic that printer spooling causes, use the R\_WINSPOOL parser in Network Monitor. If a Windows-based computer looks for computers that are acting as a Print Queue Server, it uses NetShareEnum transactions through the RemAPI protocol (also known as the *Microsoft Windows Lanman Remote API Protocol*). By default, when you use a NetShareEnum transaction, you require only anonymous access to make NetServerEnum2 and NetServerEnum3 requests. By default, Windows operating systems have anonymous access enabled.

For additional information, click the article number below to view the article in the Microsoft Knowledge Base:

[122920](#) Inbound Connections Limit in Windows  
[132679](#) Local System Account and Null Sessions in Windows NT  
[143474](#) Restricting Information Available to Anonymous Logon Users  
[149522](#) System Error 71 and License Manager  
[154541](#) Clients Open Many \Pipe\Spoolss Connections to WinNT Print Server  
[156431](#) XFOR: Error 71 When Using NT Server from MSDN Select CD  
[179483](#) Error Msg: No More Connections Can Be Made At This Time  
[191611](#) Symptoms of Multihomed Browsers  
[246261](#) How to Use the RestrictAnonymous Registry Value in Windows 2000  
[258837](#) Services That Use Remote Connections Leak User Sessions  
[289655](#) HOW TO: Enable Null Session Shares on a Windows 2000-Based Computer  
[302099](#) Windows 2000 Clients Use Multiple Connections When Mapping Drives to a Single Server  
[314882](#) Inbound Connections Limit in Windows XP

**Last Reviewed:** 1/27/2003

**Keywords:** kbprb kbtshoot w2000smb KB328459

Send  Print  Help 

Last reviewed Monday, January 27, 2003

© 2003 Microsoft Corporation. All rights reserved. [Terms of use](#) [Security & Privacy](#) [Accessibility](#)