

Goal:

How do I synchronize files using my Internet connection?

Requirements:

- **PeerSync™** with the **TCP WAN Connector (TCP)** option
- **PSListener** installation on the remote Windows device(s)
- High speed Internet connection

Important Notes:

- We strongly recommend the use of a VPN when transferring files over the public Internet for security purposes. Otherwise, you should use our Encryption feature with a **user name** and **password** to protect data and all communication as it is being transferred.
- Know the **IP address** of the remote source or target device. You will need to check the IP address for devices that receive dynamic frequently-changing IP addresses from their service providers before running PeerSync.
- Install the **PSListener** tool on the remote Windows device and configure it with the same **Encryption** and **Port** settings as the corresponding PeerSync Job.
- You may need to adjust your firewall settings to allow communication between PeerSync and the PSListener. Depending on your firewall, opening the selected port (default 7333) will be sufficient. In some cases you may also have to identify the IP address of the computer hosting the PSListener software.

Preparation:

PeerSync may be installed on any Windows machine involved in the replication process or a completely separate machine. The requirement is that PeerSync is running on the same network as either the Source or Target machine so that it has full access to its folders and files. Generally performance will be optimal when PeerSync is installed on one of the machines involved in the replication. The PeerSync Listener (PSListener) tool must be installed on the machine where to/from replicating via TCP. For example, if you are using a TCP Source, the PSListener is required to run on the Source machine and PeerSync on the Target or on the same network as the Target machine.

Limitations:

- Cannot combine a TCP source with an FTP Target within the same Job
- Folder compression and Transfer of NT Security Descriptions (ACL's) are not supported

1. PeerSync

BASIC CONFIGURATION

Follow the online tutorials for directions on how to setup PeerSync in Real-Time or Scheduled mode:
<http://www.peersoftware.com/support/peersync.aspx>

1. In the **Folder Selection** window select **TCP** for the Source or Target.
2. When you first select the TCP option, the **Source** or **Target TCP/Port Configuration** window will open automatically. Otherwise click on the **Configuration** button below the TCP path you wish to configure.
3. In the **Host Name** field enter the IP address of the remote host. The default IP address is your loopback address 127.0.0.1 which represents the machine you are currently on. If the remote machine resides on the same network as that on which PeerSync is running you may enter the machine name instead of the IP address.
4. Enter the complete remote folder path in the **Path on Host** field (i.e. C:\My Documents\Target).
5. **(Optional)** Select the **Port Configuration** tab to modify the port settings. By default PeerSync uses port **7333** for TCP and byte level communication. This value needs to be identical to the port number specified in the **PSListener Configuration** tool running on the remote site. The port number can be any value between 1024 and 65535.
6. **(Optional)** By default **Encryption** is enabled and an internal strong DES cipher is used to encrypt all the data and communication between the two locations. For enhanced security we recommend you provide a **User Name** and/or **Password** as key values. These values, along with the default cipher will be used by PeerSync's internal algorithm to encrypt data and communication transmitted over the Internet, LAN, WAN or VPN.

To enter your own key values fill in the **User Name** and/or **Password** field(s). Make sure these values are entered accordingly in the **PSListener Configuration** tool running on the remote device. Just like the port number, the key values need to be identical on both sides.
7. **(Optional)** In the **ByteReplicator** window, check the **Use block/byte level synchronization** box. This option will enable byte level replication in a pull and push scenario.

Note: *This feature requires that your PeerSync license includes the [ByteReplicator](#) option.*

2. PSListener

START/STOP THE LISTENER SERVICE OR APPLICATION

The following steps are carried out on the remote machine. You must install the PSListener in order to proceed. When you install the PSListener you may choose to install and configure it as a Service. The PSListener.exe tool is located in the "C:\WINDOWS\system32" directory by default.

To install the Listener as a Service (skip this if you have done so during the installation process)

- Go to your **C:\WINDOWS\system32** directory
- Right-click the **PSListener.exe** file and select **Create Shortcuts Here**
- Right-click on the PSListener shortcut and select **Properties**
- Click on the **Shortcut** tab and type **/install** at the end of the **Target** field
- Hit **Apply** then **OK**
- Double click the PSListener shortcut to run the service installation

To Start/Stop the Listener Service

- Open your Windows **Services** utility
- Right click on the **PSListener Utility Software** service and select **Start** or **Stop**

To Run the Listener as an Application

- Go to your **C:\WINDOWS\system32** directory
- Double click on the **PSListener.exe** file to run the PSListener as an Application
- To **Stop** the PSListener application open the **Windows Task Manager** and terminate the **PSListener.exe** process

To Uninstall the PSListener Service

- Stop the **PSListener Utility Software** service if it is running (open Windows **Services**, right click on the **PSListener Utility Software** service, and select **Stop**)
- Go to the **C:\WINDOWS\system32** directory
- Right-click the **PSListener.exe** file and select **Create Shortcuts Here**
- Right-click on the PSListener shortcut and select **Properties**
- Click on the Shortcut tab and type **/uninstall** at the end of the **Target** field
- Hit **Apply** then **OK**
- Double click on the PSListener shortcut to uninstall the PSListener service

3. PSListener Configuration

PSLConfig.exe CONFIGURATION

The following steps are carried out on the remote machine. You must install the PSListener in order to proceed. The PSLConfig.exe utility will be located in the PeerSync installation folder by default (i.e. "C:\Program Files\PeerSync Listener").

1. Go to the **PeerSync Listener** installation folder and double click on **PSLConfig.exe**
2. Check that the **TCP Port** value is the same as the one specified in your PeerSync Profiler.
3. If you are using **Encryption**, provide the **UserName** and/or **PassWord** keys you specified in your PeerSync Profile.
4. **(Optional)** Specify a **RootPath** if you want the PSListener to behave similar to an FTP server which sets Root Paths to limit user access to the local file system. Entering a path in this field limits PeerSync's ability to access directories on the remote device. PeerSync will only be able to access directories bellow or at the same level as the specified **RootPath** provided that it meets the **Port** and **Encryption** requirements. In no circumstances can PeerSync access directories located above this path. If the remote path you enter in PeerSync references a directory above the **RootPath**, PeerSync will create that folder structure at runtime bellow the **RootPath**.

Example:

PSListener "RootPath" = C:\Backup\Users\Admin

Path in PeerSync = C:\Backup\My Documents

Actual Remote Path = C:\Backup\Users\Admin\C\Backup\My Documents

Note: *The **RootPath** value will be ignored when not running in TCP mode (i.e. doing Byte Replication using Local or UNC paths)*

5. Increase the **CPU Utilization** value to **High**.
6. **Save** your settings by clicking on the right lower corned of the application or by going to the **File** menu and selecting **Save**. You may then close or **Exit** the application (this will not terminate the PSListener if it is running).
7. Restart the **PSListener** service or application if you have made any changes to the **PSLConfig.exe** utility to ensure the changes take effect.

4. Troubleshooting

ERROR MESSAGES

Message 1

```
Could not initialize target device: TCP:\\190.186.170.170\c$\Testing...  
Connection Failure: TCP:\\190.186.170.170\c$\Testing - Job: Replication  
(Connection Retry is Enabled!)
```

Solution:

- Check that the Listener is up and running on the target device and is listening on the same port number as PeerSync.
- Check that the **User Name** and/or **PassWord** used in the **PSLConfig** utility are the same as the one you entered in the PeerSync Profiler (**Folder Selection** -> **Configure** button -> **Port Configuration** tab)
- Make sure you have a single PSLlistener running on the remote machine. It is possible that you may have a PSLlistener running as a service, another as an application, or simply running two different versions. Check the **Windows Task Manager** for the **PSListener.exe** process, terminate all instances and restart the PSLlistener.
- Save and/or restart **PeerSync**, **PSListener**, and **PSLConfig** utility once you modify any settings in order for them to take effect.

Message 2

```
PSListener responded with - Update Failure [LockFiles] Error Opening  
Handle: C:\Target\Document.doc (The process cannot access the file because  
it is being used by another process) (Added To Retry List)
```

Solution:

- This message indicates that the target file may not be accessible usually because it is open or being used by another application.
- PeerSync will attempt to update the file on an interval based on your retry settings (Global Settings -> Global Recovery/Offline Options)

5. Glossary

TCP REPLICATION TERMINOLOGY

Transmission Control Protocol (TCP)

Used along with the Internet Protocol (IP), TCP allows for the creation of connections between hosts over the Internet, LAN, WAN or VPN for the purposes of file backup and synchronization.

Encryption

The process of converting data into a ciphertext to make it unreadable without the possession of a key or password to decrypt it.

Cipher

A series of well-defined steps or algorithm used to perform encryption and decryption.

Data Encryption Standard DES

Takes a fixed-length string of plaintext and converts it through a series of operations into another cipher of the same length. This form of encryption algorithm is recommended and approved by the Federal Information Processing Standard (FIPS).