FTP Server Configuration

(*WHM >> Home >> Service Configuration >> FTP Server Configuration*)

Overview

The *FTP Server Configuration* interface allows you to customize your chosen FTP server's behavior.

> **Note:**
> This interface is only available when you enable FTP services on your server. For more information, read our Service Manager docume ntation.

How to configure your ProFTPd server

To configure your ProFTPd server, perform the following steps:

1. From the *TLS Encryption Support* menu, select a setting for TLS encryption of FTP connections:

   > **Note:**
   > As of cPanel & WHM version 68, we only support Transport Layer Security (TLS) protocol version 1.2. However, you can use TLSv1.1 or TLSv1.2 to manage your Pure-FTPd server.

   - *Optional* — FTP users choose whether to use TLS encryption. This setting offers the best compatibility.
   - *Required (Command)* — Requires TLS encryption on all commands that users issue to the FTP server. This setting hides passwords and usernames.
   - *Required (Command/Data)* — Requires TLS encryption on commands that users issue to the FTP server and on data that comes through the FTP server. This setting protects all traffic from eavesdroppers.
2. Enter the list, in standard format, of the TLS ciphers that you wish your FTP server to use in the *TLS Cipher Suite* text box.
   - `HIGH:MEDIUM:+TLSv1:!SSLv2:+SSLv3` is the default setting.
   - Typically, you should only adjust this setting for PCI Compliance.
   - For more information about TLS ciphers, read OpenSSL's Cipher documentation.
3. From the *Allow Anonymous Logins* menu, select whether users can log in to your FTP server anonymously.

   > **Warning:**
   > We do **not** recommend that you enable anonymous FTP, because it seriously compromises the security of your server.

4. In the *Maximum Idle Time (seconds)* text box, enter the number of seconds that an FTP connection may remain idle before the server disconnects it.
5. In the *Maximum Number of FTP Processes* text box, enter the maximum number of active processes the FTP server may create. Because each connection creates a process, this setting limits the total number of FTP connections.

   > **Note:**
   > To disable limits on the number of FTP processes, enter *none*.

6. Click *Save*.

> **Notes:**
> - For more information about ProFTPd, visit the ProFTPd website.
> - To access ProFTPd's debug mode, run the following commands:

```
/usr/local/cpanel/scripts/restartsrv_proftpd --stop
/usr/sbin/proftpd -nd9
```

Configure your Pure-FTPd server

Notes:
- The system stores your configuration in the `/etc/pure-ftpd.conf` file.
- By default, Pure-FTPd only returns the first 10,000 files in a directory. To increase this number, perform the following steps:
    1. Create the `/var/cpanel/conf/pureftpd/local` file with the `touch` command, if one does not exist.
    2. In a text editor, open the `local` file and add the following line, where `15000` representss the value that you wish to increase to:

       ```
       LimitRecursion 15000 8
       ```

    3. Run the `/usr/local/cpanel/scripts/setupftpserver pure-ftpd --force` command to update the `/etc/pure-ftpd.conf` file.

To configure your Pure-FTPd server, perform the following steps:

1. From the *TLS Encryption Support* menu, select a setting for TLS encryption of FTP connections:
   - *Disabled* — Disables TLS encryption.
   - *Optional* — FTP users choose whether to use TLS encryption. This setting offers the best compatibility.
   - *Required (Command)* — Requires TLS encryption on all commands users issue to the FTP server. This setting hides passwords and usernames.
   - *Required (Command/Data)* — Requires TLS encryption on commands users issue to the FTP server and on data that comes through the FTP server. This setting protects all traffic from eavesdroppers.
2. Enter the list, in standard format, of the TLS ciphers you wish your FTP server to use in the *TLS Cipher Suite* text box.
   - `HIGH:MEDIUM:+TLSv1:!SSLv2:+SSLv3` is the default setting.
   - Typically, you should only adjust this setting for PCI compliance.
   - For more information about TLS ciphers, read OpenSSL's [Cipher documentation](#).
3. From the *Allow Anonymous Logins* menu, select whether users can log in to your FTP server anonymously.

   > **Warning:**
   > We do **not** recommend that you enable anonymous FTP, because it seriously compromises the security of your server.

4. From the *Allow Anonymous Uploads* menu, select whether anonymous users can upload files to your FTP servers.

   > **Warning:**
   > We do **not** recommend that you enable anonymous FTP, because it seriously compromises the security of your server.

5. Enter the maximum load for anonymous downloads in the *Maximum Load for Anonymous Downloads* text box. If the system's load average exceeds this setting, your FTP server will prevent downloads by anonymous users.

   > **Warning:**
   > We do **not** recommend that you enable anonymous FTP, because it seriously compromises the security of your server.

6. In the *Maximum Idle Time (seconds)* text box, enter the number of seconds an FTP connection may remain idle before the server disconnects it.
7. Enter the maximum number of FTP connections in the *Maximum Connections* text box.

   > **Note:**
   > Your FTP server applies this limit server-wide and **not** on a per-user basis.

8. In the *Maximum Connections Per IP Address* text box, enter the maximum number of FTP connections to allow from a single IP address.
9. From the *Allow Logins with Root Password* menu, select whether to allow the `root` password to access all FTP accounts.
10. From the *Broken Clients Compatibility* menu, select whether your FTP server will ignore some protocol standards in order to improve compatibility with buggy FTP clients and firewalls.

> **Note:**
> If you select *Yes,* your FTP server will perform the following actions:
>
> - Create symbolic links (symlinks) as actual files and directories. For more information about symlinks, visit Wikipedia's Symbolic link entry.
> - Prompt for a dummy password for an anonymous user.
> - Disable *Extended Passive Mode.*

11. Click *Save.*

For more information about Pure-FTPd, visit the Pure-FTPd website.

Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- FTP Server Configuration
- The setupftpserver script
- FTP Server Selection
- Raw FTP Log Download
- How to Deny FTP Access

- FTP Connections
- Anonymous FTP
- FTP Accounts
- Webalizer FTP

- How to Enable FTP Passive Mode
- FTP Server Configuration
- LiteSpeed Web Server
- The setupftpserver script
- FTP Server Selection

- cPanel API 2 Modules - FTP
- UAPI Modules - Ftp
- cPanel API 1 Functions - Ftp::delftp
- cPanel API 2 Functions - Ftp::delftp
- cPanel API 2 Functions - Ftp::addftp