

# ProFTPD Configuration for Host Access Control

[Overview](#)

[System Requirements:](#)

[Configuration instructions](#)

[Main IP address](#)

[Additional IP addresses](#)

[Additional documentation](#)

## Overview

ProFTPD® does not automatically reference `/etc/hosts.allow` or `/etc/hosts.deny` to restrict access to the FTP service. The purpose of this document is to provide an example of how to configure ProFTPD to utilize the [Host Access Control](#) feature from the command line to restrict access by IP address to FTP.

### Warning

This document describes an unsupported workaround that is not guaranteed to work in the future.

- After these steps are performed on a server, it is the system administrator's responsibility to manage and maintain the server's database software.
- We recommend that only experienced system administrators attempt to perform these steps.
- We are **not** responsible for any data loss that is caused by an attempt to perform these steps.

## System Requirements:

To configure ProFTPD, you must have the following installed on your server:

- ProFTPD version 1.3.3 or higher
- `mod_wrap`

As the `root` user, run the following command to confirm that you have the correct version of ProFTPD and `mod_wrap` installed on your server:

```
proftpd -V | awk '/Version/ {print $0}; /mod_wrap/ {print "mod_wrap is installed"}'
```

The output will resemble the following:

```
root@testserver [~]# proftpd -V | awk '/Version/ {print $0}; /mod_wrap/ {print "mod_wrap is installed"}'
Version: 1.3.5rc1 (devel)
mod_wrap is installed
root@testserver [~]#
```

## Configuration instructions

To configure ProFTPD, perform the following steps as the `root` user:

### Main IP address

1. Open the `/etc/proftpd.conf` file with a text editor, add the following lines after the comments.

```
TCPAccessFiles /etc/hosts.allow /etc/hosts.deny
TCPServiceName ftp
```

2. Run the following command to restart ProFTPD:

```
/scripts/restartsrv_proftpd
```

**Warning:**

You must specify both `/etc/hosts.allow` and `/etc/hosts.deny` or you will receive an error.

3. Add deny rules and test.

**Note:**

When ProFTPD rejects connections due to Host Access Control configuration, those failures are reported as authentication failures.

```
root@testserver [~]# ftp 10.1.1.1
Connected to 10.1.1.1.
220 ProFTPD 1.3.5rc1 Server (ProFTPD) [::ffff:10.1.1.1]
Name (10.1.1.1:root): cptest
331 Password required for cptest
Password:
530 Access denied
ftp: Login failed
ftp> quit
221 Goodbye.
```

## Additional IP addresses

Each Virtual Host that requires Access Control will need an entry in the file `/etc/proftpd.conf`. Add the following lines to each Virtual Host container.

```
TCPAccessFiles /etc/hosts.allow /etc/hosts.deny
TCPServiceName ftp
```

The following is an example of a VirtualHost container.

```
<VirtualHost 10.1.1.1>
  ServerName ftp.testserver.tld
  AuthUserFile /etc/proftpd/wcraft
  MaxClients 3 "Sorry, this ftp server has reached its maximum user count
(%m). Please try again later"
  DirFakeGroup On ftpgroup
  DirFakeUser On ftpuser
  DefaultRoot ~
  TCPAccessFiles /etc/hosts.allow /etc/hosts.deny
  TCPServiceName ftp
[truncated]
```

## Additional documentation

[Suggested documentation](#) [For cPanel users](#) [For WHM users](#) [For developers](#)

- [ProFTPD Configuration for Host Access Control](#)
- [How to Enable Additional CGI Scripts](#)
- [How to Enable FTP Passive Mode](#)
- [LiteSpeed Web Server](#)
- [FTP](#)

## Content by label

There is no content with the specified labels



- [ProFTPD Configuration for Host Access Control](#)
- [How to Enable Additional CGI Scripts](#)
- [How to Enable FTP Passive Mode](#)
- [LiteSpeed Web Server](#)
- [FTP](#)
  
- [cPanel API 1 Modules - DenyIp](#)
- [cPanel API 1 Functions - DenyIp::deldenyip](#)
- [cPanel API 1 Functions - DenyIp::adddenyip](#)
- [cPanel API 1 Functions - Htaccess::set\\_protect](#)
- [cPanel API 1 Functions - Htaccess::setindex](#)