

# Host Access Control

(WHM >> Home >> Security Center >> Host Access Control)

## Overview

Allow or deny access for an IP address

Allow or deny IP addresses on the command line

CentOS, CloudLinux™, or Red Hat® Enterprise Linux (RHEL) 6, or Amazon Linux  
CentOS 7, CloudLinux 7, or RHEL 7

Additional notes

Additional documentation

## Overview

### Warning:

If you accidentally lock yourself out of WHM when you use this interface, edit the `/etc/hosts.allow` file through the command line to regain access.

### Note:

The [Create Support Ticket](#) interface (WHM >> Home >> Support >> Create Support Ticket) automatically adds cPanel Support's IP addresses to the server's `/etc/hosts.allow` file. For more information, read our [Create Support Ticket](#) documentation.

Use this interface to allow or deny access to the following services for specific IP addresses:

- cPanel (`cpanel`)
- WHM (`whostmgrd`)
- Webmail (`webmaild`)
- Web Disk (`cpdavd`)
- FTP (`ftpd`)
- SSH (`sshd`)
- SMTP (`smtp`)
- POP3 (`pop3`)
- IMAP (`imap`)

### Notes:

- To control access to the `ftpd` daemon, you **must** use the ProFTPD FTP server. Pure-FTP does **not** support TCP wrappers.
  - To choose an FTP server, use WHM's [FTP Server Selection](#) interface (WHM >> Home >> Service Configuration >> FTP Server Selection).
  - For more information, read our [ProFTPD Configuration for Host Access Control](#) documentation.
- To control access to the POP3 or IMAP services, you may use the Dovecot® mail servers.

## Allow or deny access for an IP address

To allow or deny an IP address to access a service, perform the following steps:

1. Enter the service name in the *daemon* text box.
2. Enter the IP address or hostname in *Access List* text box.
  - You may enter wildcards in this text box.
  - You **cannot** enter a range of IP addresses with CIDR notation.
  - To specify a network range, add a network mask to the IP address.
    - For example, `192.168.0.0/255.255.255.0`, where `255.255.255.0` is the desired network mask you want to use.
3. Enter the desired action in the *Action* text box.
  - Enter `allow` to allow access.
  - Enter `deny` to deny access.
4. Describe the rule in the *Comment* text box.
5. Click *Save Host Access List*, or click *Reload* to delete any changes.

### Note:

You can also enter `ALL EXCEPT IP address` in the *Access List* text box. When you enter `allow` as your action, the system will allow all of the addresses **except** for addresses that you entered in the *Access List* text box.

## Allow or deny IP addresses on the command line

For greater host access control flexibility, you can create rules in the command line. To do this, perform the following steps:

1. Log in to your server as the `root` user.
2. Open the `/etc/hosts.allow` file with your preferred text editor.
3. Enter the desired rules in the following format:

```
service : IP address : action
```

See the following example to allow 192.168.0.0 IP address to access the cPanel service:

```
cpaneld : 192.168.0.0 : allow
```

### Notes:

- When you configure your firewall directly, you can use CIDR notation.
- WHM does **not** use a `hosts.deny` file. Add deny statements to the `/etc/hosts.allow` file.

## CentOS, CloudLinux™, or Red Hat® Enterprise Linux (RHEL) 6, or Amazon Linux

On a CentOS, CloudLinux, or RHEL 6, or Amazon® Linux system, use the `iptables` utility to manage your firewall.

- You can block a specific IP address with the `iptables` command. For example, to block 192.168.0.0, run the following command:

```
iptables -A INPUT -s 192.168.0.0 -j DROP
```

- You can block a specific port for an IP address. For example, to block port 23 on 192.168.0.0, run the following command:

```
iptables -A INPUT -s 192.168.0.0 -p tcp --destination-port 23 -j DROP
```

## CentOS 7, CloudLinux 7, or RHEL 7

On a CentOS 7 or CloudLinux 7 system, use the `firewalld` utility to manage your firewall.

For example, to block traffic for a single IP address, run the following command, where 192.168.0.0 is the IP address that you wish to block:

```
firewall-cmd --add-rich-rule='rule family="ipv4" source address="192.168.0.0" drop' --permanent
```

For more information, read [Red Hat's firewalld documentation](#).

## Additional notes

You **must** enter your `allow` rules before your `deny` rules. For example, to allow access for two IP addresses, but deny access from all other addresses, use either of the following methods:

Create two separate rules:

- Create one rule that allows 192.168.0.0/255.255.255.0
- Create a second rule that denies access to ALL IP addresses.

Create one rule:

- Enter `all except 192.168.0.0/255.255.255.0` in the *Access List* text box.
- Enter `deny` in the *Action* text box.

## Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- [Host Access Control](#)
- [cPHulk Brute Force Protection](#)
- [Purchase and Install an SSL Certificate](#)
- [Manage Service SSL Certificates](#)
- [Apache mod\\_userdir Tweak](#)
  
- [SSH Access](#)
- [SSL TLS Wizard](#)
- [SSL TLS](#)
- [Virus Scanner](#)
- [Security Policy](#)
  
- [How to Configure Your Firewall for cPanel Services](#)
- [Basic Security Concepts](#)
- [How to Purchase an Imunify360 License](#)
- [How to Install KernelCare](#)
- [Additional Security Software](#)
  
- [WHM API 1 Functions - fetch\\_security\\_advice](#)
- [WHM API 1 Functions - installssl](#)
- [WHM API 1 Functions - get\\_autosslog](#)
- [WHM API 1 Functions - get\\_autossproviders](#)
- [WHM API 1 Functions - get\\_autosspending\\_queue](#)