

# How to Configure Your Firewall for cPanel Services

- Overview
- Ports
- Example configurations
- CentOS 7, CloudLinux 7, and RHEL 7 firewall management
- Additional documentation

## Overview

cPanel & WHM installs and manages many different services on your system, most of which require an external connection in order to function properly. Because of this, your firewall **must** allow cPanel & WHM to open the ports on which these services run.

This document lists the ports that cPanel & WHM uses, and which services use each of these ports, to allow you to better configure your firewall.

### Warning:

- We **strongly** recommend that you **only** open ports for services that you use.
- When you work with firewall rules, always make **certain** to include a way to log back in to your server, and **always** maintain console access to your server.

## Ports




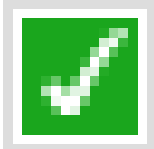

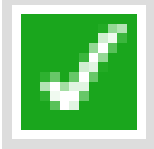
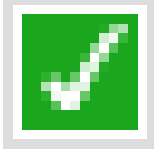
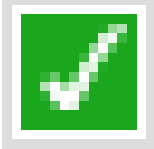
### Important:

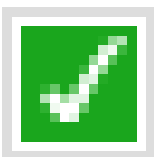
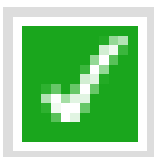
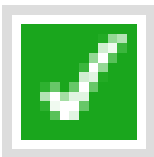
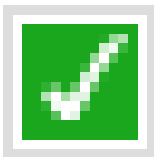
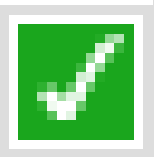
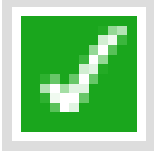
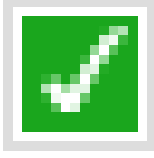
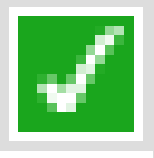
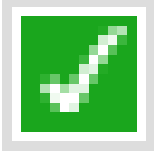
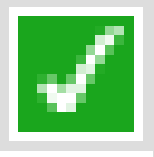
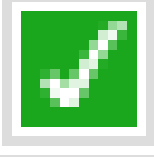
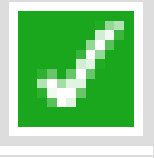
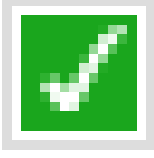
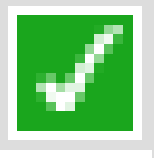
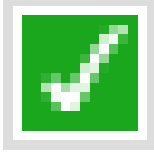
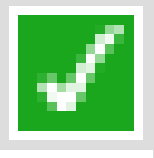
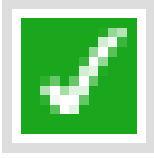
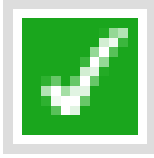

We **strongly** recommend that you use the SSL version of each service whenever possible.

- The use of non-SSL services can allow attackers to intercept sensitive information, such as login credentials.
- Always ensure that valid SSL certificates exist for your services in WHM's *Manage Service SSL Certificates* interface (*WHM >> Home >> Service Configuration >> Manage Service SSL Certificates*).

### Note:

For more information on how to access cPanel & WHM services, read our [How to Access cPanel & WHM Services](#) documentation.

Port	Service	TCP	UDP	Inbound	Outbound	Localhost	Notes
1	CPAN						The <i>Show Available Modules</i> option in cPanel's <i>Perl Modules</i> interface ( <i>cPanel &gt;&gt; Home &gt;&gt; Software &gt;&gt; Perl Modules</i> ) uses this port to improve the speed in which it appears.
20	FTP						Instead of FTP, we recommend that you use the more secure SFTP via SSH.
21	FTP						




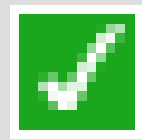

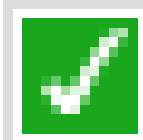



22	SSH						<p><b>Important:</b> You must open this port before you use WHM's <i>Transfer Tool</i> interface (WHM &gt;&gt; Home &gt;&gt; Transfers &gt;&gt; Transfer Tool).</p>
25	SMTP						
26	SMTP						cPanel & WHM <b>only</b> uses this port if you specify it in WHM's <i>Service Manager</i> interface (WHM >> Home >> Service Configuration >> Service Manager).
37	rdate						
43	whois						
53	bind						cPanel & WHM <b>only</b> uses this port if you run a public DNS server.
80	httpd						<p>This port serves the HTTP needs of services on the server.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• In cPanel &amp; WHM view</li> </ul>







**Important:** We strongly recommend that you encourage your users to use port 443, which uses the more secure SSL/TLS security protocol. For more information, read our [More about TLS and SSL documentation](#).

110	POP3					
113	ident					
143	IMAP					
443	httpd					<p>This port serves the HTTPS needs of services on the server.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"><li>• <a href="#">Incpanel &amp; WHMve</a></li></ul>

rsion 7.6 and later, the cPanel Server Daemon (cpsrvd) lists on this port when you disable the Web Server

If you enable the *Service subdomains* and *Service subdomain creation* settings in the *Domains* section of WHM's *Tweak Settings* interface (*WHM >> Home >> Server Configuration >> Tweak Settings*), users can access cPanel or WHM via the following subdomains:



- `cpanel.example.com` delivers to the user's [cPanel Home](#) interface.
- `whm.example.com` delivers to the user's [WHM Home](#) WHM interface.
- `webmail.example.com` delivers to the user's [Webmail](#) interface ([cPanel >> Home >> Email >> Email Accounts](#)).
- `webdisk.example.com` delivers to the user's [Web Disk](#) interface ([cPanel >> Home >> Files >> Web Disk](#)).

WHM's [Manage AutoSSL](#) interface ([WHM >> Home >> SSL/TLS >> Manage AutoSSL](#)) requires outbound access to the `store.cpanel.net` server.

465

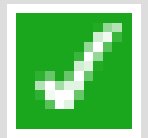

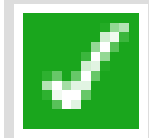



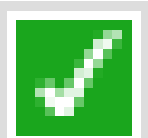
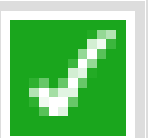
SMTP, SSL/TLS



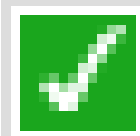

**Warning:**  
As of cPanel & WHM version 68, we only support Transport Layer Security (TLS) protocol version 1.2.



• We will only support applications that use TLS v1.2.

• We strongly recommend that you enable TLS v1.2 on your server.

579	cPHulk						This port should <b>only</b> accept connections on the 127.0.0.x IPv4 address. Your system does <b>not</b> require that this port accept external traffic.
783	Apache SpamAssassin™						
873	rsync						
993	IMAP SSL						

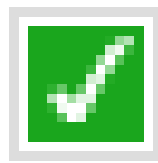
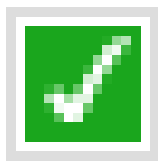
995	POP3 SSL						
2703	Razor						Razor is a collaborative spam-tracking database. For more information, visit the <a href="#">Razor website</a> .
2077	WebDAV						cPanel's <i>Web Disk</i> interface ( <i>cPanel &gt;&gt; Home &gt;&gt; Files &gt;&gt; Web Disk</i> ) uses these ports.
2078	WebDAV SSL						
2079	CalDAV and CardDAV						cPanel's <i>Calendars and Contacts</i> interface ( <i>cPanel &gt;&gt; Home &gt;&gt; Email &gt;&gt; Calendars and Contacts</i> ) uses these ports.
2080	CalDAV and CardDAV (SSL)						

2082	cPanel						<p><b>Note:</b>  To disable logins via this port and only allow SSL logins, set the <i>Choose the closest matched domain for which that the system has a valid certificate when redirecting from non-SSL to SSL URLs.</i> Formerly known as "Always redirect to SSL/TLS" option to <i>On in WHM's Tweak Settings interface (WHM &gt;&gt; Home &gt;&gt; Server Configuration &gt;&gt; Tweak Settings)</i>. This will redirect users to secure ports with the <code>/cpanel</code>, <code>/whm</code>, and <code>/webmail</code> aliases.</p>
2083	cPanel SSL						


2086	WHM						<p><b>Note:</b>  To disable logins via this port and only allow SSL logins, set the <i>Choose the closest matched domain for which that the system has a valid certificate when redirecting from non-SSL to SSL URLs.</i> Formerly known as "Always redirect to SSL/TLS" option to On in WHM's <i>Tweak Settings</i> interface (<i>WHM &gt;&gt; Home &gt;&gt; Server Configuration &gt;&gt; Tweak Settings</i>). This will redirect users to secure ports with the <code>/cpanel</code>, <code>/whm</code>, and <code>/webmail</code> aliases.</p>
2087	WHM SSL						

2089

cPanel Licensing



**Warning:**  
You must open this port in order to contact the cPanel license servers.

2095	Webmail						<p><b>Note:</b>  To disable logins via this port and only allow SSL logins, set the <i>Choose the closest matched domain for which that the system has a valid certificate when redirecting from non-SSL to SSL URLs.</i> Formerly known as "Always redirect to SSL/TLS" option to <i>On in WHM's Tweak Settings interface (WHM &gt;&gt; Home &gt;&gt; Server Configuration &gt;&gt; Tweak Settings)</i>. This will redirect users to secure ports with the <code>/cpanel</code>, <code>/whm</code>, and <code>/webmail</code> aliases.</p>
2096	Webmail SSL						



2195	APNs						cPanel & WHM only uses this port for the Apple® Push Notification Service (APNs). For more information, read our <a href="#">How to Set Up iOS Push Notifications</a> documentation.
3306	MySQL®						MySQL uses this port for remote database connections.
6277	DCC						For more information, read Apache's <a href="#">DCC</a> and <a href="#">NetTestFirewallIssues</a> documentation.
24441	Pyzor						For more information, read Apache's <a href="#">Pyzor</a> and <a href="#">NetTestFirewallIssues</a> documentation.

## Example configurations

The following examples explain how to add rules with CSF, APF, and the `iptables` application.

### Important:

- We do **not** recommend that you use these examples for your personal configurations. Instead, make **certain** that your firewall rules match the way in which you use cPanel & WHM's services.
- CentOS 7, CloudLinux™ 7, and Red Hat® Enterprise Linux (RHEL) 7 servers have additional requirements. For more information, read the [CentOS 7, CloudLinux 7, and RHEL 7 firewall management](#) section below.

## CSF

ConfigServer provides the free WHM plugin CSF, which allows you to modify your `iptables` rules within WHM.

To install CSF, run the following commands as the `root` user:

```
cd /usr/src
rm -fv csf.tgz
wget https://download.configserver.com/csf.tgz
tar -xzf csf.tgz
cd csf && ./install.sh
```

To configure CSF, use WHM's *ConfigServer & Firewall* interface (*Home >> Plugins >> ConfigServer & Firewall*).

### Note:

For more information about how to install and use CSF, visit the [CSF website](#).

## APF

APF acts as a front-end interface for the `iptables` application, and allows you to open or close ports without the use of the `iptables` syntax.

The following example includes two rules that you can add to the `/etc/apf/conf.apf` file in order to allow HTTP and HTTPS access to your system:

```
# Common ingress (inbound) TCP ports
IG_TCP_CPORTS="80,443# Common egress (outbound) TCP ports
EG_TCP_CPORTS="80
```

**Note:**

For more information about APF, visit the [APF site](#).

## iptables

The `iptables` application offers more customization options for your packet filtering rules. This application requires that you understand the TCP/IP stack.

The following example includes `iptables` rules for HTTP traffic on port 80:

**Note:**

This example assumes that a DMZ exists on `eth0` for the `192.168.1.1` port, and the `66.66.66.66` broadcast IP address.

```
$IPTABLES -A FORWARD -p TCP -i 66.66.66.66 -o eth0 -d 192.168.1.1 -dport 80
-j allowed
$IPTABLES -A FORWARD -p ICMP -i 66.66.66.66 -o eth0 -d 192.168.1.1 -j
icmp_packets
```

**Note:**

For more information about the use of `iptables`, visit the [iptables site](#), or run the `man iptables` command from the command line.

## CentOS 7, CloudLinux 7, and RHEL 7 firewall management

Servers that run the CentOS 7, CloudLinux 7, and RHEL 7 operating systems require that you use the `firewalld` daemon.

**Important:**

We recommend that you **only** use the `firewall` utilities on CentOS 7, CloudLinux 7, and RHEL 7 servers.

**Note:**

For more information about the `firewall` utilities and the `firewalld` daemon, read Red Hat's [Using Firewalls](#) documentation.

## The cpanel service

**Important:**

The `/usr/local/cpanel/scripts/configure_firewall_for_cpanel` script clears all existing entries from the `iptables` application. If you use custom rules for your firewall, export those rules before you run the script and then re-add them afterward.

cPanel & WHM version 11.50 and later also includes the `cpanel` service, which manages all of the rules in the `/etc/firewalld/services/cpanel.xml` file. This allows TCP access for the server's ports.

To replace your existing `iptables` rules with the rules in the `/etc/firewalld/services/cpanel.xml` file, perform the following steps:

1. Run the `yum install firewalld` command to ensure that your system has `firewalld` installed.
2. Run the `systemctl start firewalld.service` command to start the `firewalld` service.
3. Run the `systemctl enable firewalld` command to start the `firewalld` service when the server starts.
4. Run the `iptables-save > backupfile` command to save your existing firewall rules.
5. Run the `/usr/local/cpanel/scripts/configure_firewall_for_cpanel` script.
6. Run the `iptables-restore < backupfile` command to incorporate your old firewall rules into the new firewall rules file.

## Additional documentation

Suggested documentation For cPanel users For WHM users For developers

- [How to Configure Your Firewall for cPanel Services](#)
- [How to Troubleshoot PCI Compliance Scans](#)
- [Service and Proxy Subdomains](#)
- [Service Subdomains Explanation](#)
- [Basic Security Concepts](#)
  
- [Service Subdomains Explanation](#)
- [How to Use cPanel API Tokens](#)
- [Security](#)
- [Man-in-the-Middle Attacks](#)
- [How to Configure Microsoft Windows 7 to use TLS Version 1.2](#)
  
- [How to Configure Your Firewall for cPanel Services](#)
- [How to Troubleshoot PCI Compliance Scans](#)
- [Service and Proxy Subdomains](#)
- [Service Subdomains Explanation](#)
- [Basic Security Concepts](#)
  
- [WHM API 1 Functions - fetch\\_security\\_advice](#)
- [WHM API 1 Functions - get\\_autossll\\_log](#)
- [WHM API 1 Functions - get\\_autossll\\_providers](#)
- [WHM API 1 Functions - get\\_autossll\\_pending\\_queue](#)
- [WHM API 0 Functions - installssl](#)