

Parallels[®] Panel

Achieving PCI Compliance for Servers Managed by Parallels Plesk Panel 9.5

Contents

Preface	3
<hr/>	
Typographical Conventions	3
Feedback	4
Securing Servers in Compliance with PCI Data Security Standard	5
<hr/>	
Securing Linux and FreeBSD-Based Servers	6
Securing Microsoft Windows-Based Servers	12

Preface

In this section:

Typographical Conventions	3
Feedback	4

Typographical Conventions

Before you start using this guide, it is important to understand the documentation conventions used in it.

The following kinds of formatting in the text identify special information.

Formatting convention	Type of Information	Example
Special Bold	Items you must select, such as menu options, command buttons, or items in a list.	Go to the System tab.
	Titles of chapters, sections, and subsections.	Read the Basic Administration chapter.
<i>Italics</i>	Used to emphasize the importance of a point, to introduce a term or to designate a command line placeholder, which is to be replaced with a real name or value.	The system supports the so called <i>wildcard character</i> search.
Monospace	The names of commands, files, and directories.	The license file is located in the http://docs/common/licenses directory.

Formatting convention	Type of Information	Example
Preformatted	On-screen computer output in your command-line sessions; source code in XML, C++, or other programming languages.	<pre># ls -al /files total 14470</pre>
Preformatted Bold	What you type, contrasted with on-screen computer output.	<pre># cd /root/rpms/php</pre>
CAPITALS	Names of keys on the keyboard.	SHIFT, CTRL, ALT
KEY+KEY	Key combinations for which the user must press and hold down one key and then press another.	CTRL+P, ALT+F4

Feedback

If you have found an error in this guide, or if you have suggestions or ideas on how to improve this guide, please send your feedback using the online form at <http://www.parallels.com/en/support/usersdoc/>. Please include in your report the guide's title, chapter and section titles, and the fragment of text in which you have found an error.

Securing Servers in Compliance with PCI Data Security Standard

To reduce the risk of compromising sensitive data hosted on your server, you might want to implement special security measures that comply with the Payment Card Industry Data Security Standard (PCI DSS). The standard is intended to help organizations protect customer account data. For detailed information about the standard, refer to

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

The following sections describe the steps required to achieve PCI compliance for Linux, FreeBSD, and Microsoft Windows-based systems.

In this chapter:

Securing Linux and FreeBSD-Based Servers.....	6
Securing Microsoft Windows-Based Servers	12

Securing Linux and FreeBSD-Based Servers

This section describes the steps that you should perform if you want to secure your server and achieve compliance with PCI DSS on a Linux or FreeBSD server.

You first need to run the PCI Compliance Resolver utility available from the Parallels Plesk Panel installation directory. It will disable weak SSL ciphers and protocols for Web and e-mail servers operated by Parallels Plesk Panel.

➤ *To run the utility:*

1. Log in to the server shell.
2. Issue the following command:

```
/usr/local/psa/admin/bin/pci_compliance_resolver--enable all
```

The following table describes all options supported by the utility.

Option	Description
<code>-- enable all --disable all</code>	The option “—enable all” switches off weak SSL ciphers and protocols for Web and e-mail servers. The option “—disable all” reverts all changes made by the utility and restores original configuration files, thereby allowing weak SSL ciphers and protocols for connections to Web and e-mail servers.
<code>-- enable courier --disable courier</code>	Switches off or switches on weak SSL ciphers and protocols for connections to Courier IMAP mail server.
<code>-- enable apache --disable apache</code>	Switches off or switches on weak SSL ciphers and protocols for connections to the Apache Web server that serves users’ sites.
<code>-- enable panel --disable panel</code>	Switches off or switches on weak SSL ciphers and protocols for connections to Parallels Plesk Panel.

Some PCI compliance scanners may require that the medium strength SSL ciphers for access to the Panel be also switched off. For this reason, after you have run the utility, you need to modify a configuration file that was created by it.

1. Open for editing the file
`/usr/local/psa/admin/conf/cipher.lst`.
2. Remove all lines from the file.
3. Insert the following line:

```
ADH-AES256-SHA DHE-RSA-AES256-SHA DHE-DSS-AES256-SHA AES256-SHA KRB5-  
DES-CBC3-MD5 KRB5-DES-CBC3-SHA EDH-RSA-DES-CBC3-SHA EDH-DSS-DES-CBC3-  
SHA DES-CBC3-SHA ADH-DES-CBC3-SHA DES-CBC3-MD5
```

4. Save the file.

5. Restart the Web server:

- On Linux systems, issue the command `/etc/init.d/sw-cp-server restart`.
- On FreeBSD systems, issue the command `/usr/local/etc/rc.d/sw-cp-server restart`.

Now you need to switch off weak SSL ciphers for connections to Qmail or Postfix e-mail server, if you use any of them.

➤ ***If you use Qmail mail server, issue the following commands at the prompt:***

On Linux systems:

```
echo 'ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!SSLv2:RC4+RSA:+HIGH:+MEDIUM' >  
/var/qmail/control/tlsserverciphers  
echo 'ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!SSLv2:RC4+RSA:+HIGH:+MEDIUM' >  
/var/qmail/control/tlsclientciphers
```

On FreeBSD systems:

```
echo 'ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!SSLv2:RC4+RSA:+HIGH:+MEDIUM' >  
/usr/local/psa/qmail/control/tlsserverciphers  
echo 'ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!SSLv2:RC4+RSA:+HIGH:+MEDIUM' >  
/usr/local/psa/qmail/control/tlsclientciphers
```

➤ ***If you use Postfix mail server, modify configuration files:***

1. On Linux systems, open for editing the file `/etc/postfix/main.cf`.
2. On FreeBSD systems, open for editing the file `/usr/local/etc/postfix/main.cf`.
3. Add the following lines to the file:

```
smtpd_tls_protocols = SSLv3, TLSv1  
smtpd_tls_ciphers = medium  
smtpd_tls_exclude_ciphers = aNULL  
smtpd_sasl_security_options = no Plaintext
```

4. Save the file.

5. Restart the mail server:

- On Linux systems, issue the command `/etc/init.d/postfix restart`.
- On FreeBSD systems, issue the command `/usr/local/etc/rc.d/postfix restart`.

You also need to prohibit access to MySQL database server from external addresses. To do this, in a firewall that protects your Panel-managed server, add or enable a rule that prohibits TCP and UDP connections to the port 3306 from all addresses except 127.0.0.1.

➤ ***To use the firewall that comes with your Parallels Plesk Panel for Linux:***

1. Log in to the Panel as administrator.
2. If you did not install the firewall component, install it:
 - a. Go to **Home > Updates** (in the **Help & Support** group).
 - b. Click the link corresponding to your version of the Panel.
 - c. Locate **Plesk Firewall module**, select the corresponding check box, and click **Install**.
3. Configure the firewall rule that blocks external MySQL connections and switch the firewall on:
 - a. Click the **Settings** link in the navigation pane.
 - b. Click **Manage Firewall Rules**, and then **Edit Firewall Configuration**.
 - c. Click the **MySQL server** link.
 - d. Select the **Deny** option and click **OK**.
 - e. Click **Activate** to apply the configuration, and then click **Activate** again to switch on the firewall.

➤ ***To conceal the version of DNS server from potential attackers, do the following:***

1. Open for editing the DNS server's configuration file named.conf. On Linux systems, it is located in /etc/, and on FreeBSD systems, in /etc/namedb/.
2. Locate the `options {}` section, and add the `version "none"` line there.
3. Restart the `named` service:
 - On Deb package-based systems, issue the command `/etc/init.d/bind9 restart`
 - On RPM package-based systems, issue the command `/etc/init.d/named restart`
 - On FreeBSD systems, issue the command `/etc/rc.d/named restart`

➤ ***To conceal the version of the Apache Web server from potential attackers, do the following:***

1. Open for editing the Web server's configuration file.
 - On Debian, Ubuntu, and SuSE Linux, it is located at `/etc/apache2/apache2.conf`.
 - On other distributions of Linux, it is located at `/etc/httpd/conf/httpd.conf`.

- On FreeBSD, it is located at `/usr/local/etc/apache2/httpd.conf`.

2. Add the following lines:

```
ServerTokens ProductOnly
TraceEnable OFF
```

3. Save the file.

4. Restart the Web server.

- On Deb package-based systems, issue the command `/etc/init.d/apache2 restart`
- On RPM package-based systems, issue the command `/etc/init.d/httpd restart`
- On FreeBSD systems, issue the command `/usr/local/etc/rc.d/apache2 restart`

➤ ***If you have Single Sign-On v.2.2 components installed, then you need to disable SSL v.2 and weak SSL ciphers for the single sign-on service:***

1. Open for editing the file `/etc/sw-cp-server/applications.d/sso-cpserver.conf`.

2. Locate the two lines `ssl.engine = "enable"`.

3. After each of these lines, add the following:

```
ssl.cipher-list = "ADH-AES256-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:AES256-SHA:ADH-AES128-SHA:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:AES128-SHA:KRB5-DES-CBC3-MD5:KRB5-DES-CBC3-SHA:ADH-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA:DES-CBC3-SHA:DES-CBC3-MD5:DHE-DSS-RC4-SHA:KRB5-RC4-MD5:KRB5-RC4-SHA:ADH-RC4-MD5:RC4-SHA:RC4-MD5:RC2-CBC-MD5:RC4-MD5"
ssl.use-sslv2 = "disable"
```

4. Save the file.

5. Restart the service:

- On Linux systems, issue the command `/etc/init.d/sw-cp-server restart`.
- On FreeBSD systems, issue the command `/usr/local/etc/rc.d/sw-cp-server restart`.

➤ ***To conceal the version of PHP installed on the server:***

1. Create a file with name `php.ini` in the following directory

- On Linux systems, `/etc/sw-cp-server/`
- On FreeBSD systems, `/usr/local/etc/sw-cp-server/`

2. Add to this file the line `expose_php = Off`.

3. Save the file.

4. Open for editing the following file:

- On Linux systems, `/etc/sw-cp-server/applications.d/sso-cpserver.conf`.
 - On FreeBSD systems, `/usr/local/etc/sw-cp-server/applications.d/sso-cpserver.conf`.
5. Locate the following line:
- On Linux systems, `var.intertpreter = "/usr/bin/sw-engine-cgi"`.
 - On a FreeBSD system, `var.intertpreter = "/usr/local/bin/sw-engine-cgi"`.
6. Replace it with the following line:
- On Linux systems, `var.intertpreter = "/usr/bin/sw-engine-cgi -c /etc/sw-cp-server/php.ini"`.
 - On a FreeBSD system, `var.intertpreter = "/usr/local/bin/sw-engine-cgi -c /usr/local/etc/sw-cp-server/php.ini"`.
7. Save the file.
8. Restart the Web server:
- On Linux systems, issue the command `/etc/init.d/sw-cp-server restart`.
 - On FreeBSD systems, issue the command `/usr/local/etc/rc.d/sw-cp-server restart`.

To alleviate security risks arising from disclosure of information about files and their properties by Apache Web server, configure the `FileETag` directive in the Web server configuration file.

➤ **To do this:**

1. Open for editing the Web server's configuration file.
 - On Debian, Ubuntu, and SuSE Linux, it is located at `/etc/apache2/apache2.conf`.
 - On other distributions of Linux, it is located at `/etc/httpd/conf/httpd.conf`.
 - On FreeBSD, it is located at `/usr/local/etc/apache2/httpd.conf`.
2. Locate the line `FileETag INode MTime Size` and remove the `INode` keyword from this line.
3. Save the file.
4. Restart the Web server.
 - On Deb package-based systems, issue the command `/etc/init.d/apache2 restart`
 - On RPM package-based systems, issue the command `/etc/init.d/httpd restart`

- On FreeBSD systems, issue the command `/usr/local/etc/rc.d/apache2 restart`

Securing Microsoft Windows-Based Servers

This section describes the steps that you should perform if you want to secure your server and achieve compliance with PCI DSS on a Microsoft Windows-based server.

➤ ***To prohibit access to MySQL database server from external addresses, use the firewall that comes with your Parallels Plesk Panel for Windows:***

1. Log in to the Panel as administrator.
2. Click the **Settings** link in the navigation pane.
3. Click **Manage Firewall Rules**.
4. Click **Switch On**.

➤ ***To switch off weak SSL ciphers for Web server in Parallels Panel for Microsoft Windows Server 2003 and 2008:***

1. Copy the following text to the clipboard:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server]
"Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server]
"Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56]
"Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL]
"Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 128/128]
"Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128]
"Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128]
"Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]
```

```
"Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders
\SCHANNEL\Ciphers\RC4_40/128]
"Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders
\SCHANNEL\Ciphers\RC4_56/128]
"Enabled"=dword:00000000
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders
\SCHANNEL\Hashes]
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders
\SCHANNEL\Hashes\MD5]
"Enabled"=dword:00000000
```

2. Log in to the server over a Remote Desktop connection.
3. When in the server's operating system, open Notepad or any other text editor, and create a file with the `reg` extension.
4. Paste the text from the clipboard into this file.
5. Save the file.
6. Double-click the file to open it.
7. When prompted, confirm addition of new keys to the registry.
8. Restart the operating system.

Note: Some applications on the server that use weak SSL ciphers and protocols may stop working.

➤ ***To conceal the version of PHP installed on the server:***

1. Open for editing the following files:
 - `c:\Program Files\Parallels\Plesk\Additional\PleskPHP5\php.ini.`
 - `c:\windows\php.ini.`
 - `c:\inetpub\vhosts\webmail\horde\php.ini.`
2. Locate the lines `expose_php = On.`
3. Change `On` to `Off.`
4. Save the files.
5. Restart the IIS Web server.