Parallels® Plesk Panel

Meeting PCI DSS Requirements for Parallels Plesk Panel Suite

Parallels Plesk Panel 11.5

Revision 1.0

Parallels

Contents

CHAPTER 1

Introduction

The PCI Data Security Standard (PCI DSS)

The *PCI DSS* is a security standard that helps organizations proactively protect customer account data. The standard constantly evolves to remain viable in today's rapidly changing Internet and computing environment. It is reviewed at least every 24 months, and can be updated at any time. To learn more about the standard, visit www.pcisecuritystandards.org.

Compliance with PCI DSS and PA DSS

Credit card companies require compliance with PCI DSS for every entity that is involved in the storage, processing, or transmission of credit card information. Failure to comply can result in denial or revocation of your organization's facility to process credit cards.

Furthermore, as these standards have become widely recognized, non-compliance places your organization at risk of legal and/or civil consequences if credit card information becomes compromised.

Compliance with PCI DSS is necessary whether or not you use Parallels Panel to process transactions online. Even if you use a POS terminal or other methods to process transactions, and simply retain information in Parallels Panel, you must ensure proper use of the program to maintain the security and confidentiality of customer data.

Since July 1, 2010, Credit Card Processors and Bank Card Acquirers have had to ensure that merchants and agents use only Payment Application Data Security Standard (PA DSS) compliant applications. Parallels Panel is certified as compliant under the security standard that applies to software vendors that develop applications for sale to merchants to process and/or store cardholder data.

Panel Suite and PCI DSS

This document explains how to configure Panel Suite to adhere to PCI DSS. By "Panel Suite" we mean Parallels Panel and its two major components - Presence Builder and Business Manager. The first component, Builder, does not work with sensitive information and therefore is not subject to the standard regulations, so we will tune only Panel and Business Manager.

The procedure of achieving the compliance involves two general steps:

- *Tune Panel to comply with the standard*. Take these mandatory steps to improve Panel security even if you use Panel with alternative billing solutions.
- *Tune Business Manager to comply with the standard.* Take these steps only if you use this component. If you use alternative billing solutions, consult the respective software vendors about PCI DSS compliance.

CHAPTER 2

Tune Panel to Meet PCI DSS

To protect sensitive data hosted on your server and to make Panel PCI DSS compliant, you should implement special security measures. Regardless of an operating system type you use, the measures are as follows:

- Ensure that software incorporates all security updates.
- Set up encryption of remote connections.
- Prohibit access to databases server from external addresses.
- Disable weak SSL ciphers and protocols for web servers, mail servers, and components.
- Prevent services from disclosing information about your data and versions of software you use.

Note: If you wish to achieve the PCI compliance for Panel Suite, you should also tune Business Manager (on page 13) to meet PCI DSS.

In this chapter:

Linux-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 server.

Installing the latest version of OpenSSH

Before you begin, make sure that you have *the latest version of OpenSSH* and update it if required. This is achieved by completing the following steps:

1. Install or update the SSH server by running one of the commands:
   - On RPM package-based systems,

   ```
   yum install openssh-server
   ```

   - On DEB package-based systems,

   ```
   aptitude install openssh-server
   ```

2. Change the default SSH server port by removing the leading # symbol and modifying the port value in /etc/ssh/sshd_config, the line

   ```
   #Port 22
   ```

3. Restart the SSH server.

   ```
   /etc/init.d/ssh restart
   ```

Disabling weak SSL ciphers and protocols

Then you 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
-- enable all | --disable all	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.

-- enable courier	--disable courier	Switches off or switches on weak SSL ciphers and protocols for connections to Courier IMAP mail server.
-- enable apache | --disable apache	Switches off or switches on weak SSL ciphers and protocols for connections to the Apache Web server that serves users' sites.
-- enable panel | --disable panel	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 `/etc/sw-cp-server/conf.d/pci-compliance.conf`.
2. Replace all content in the file with the following: `ssl_ciphers 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;`
3. Save the file.
4. Restart the Web server by running the command `/etc/init.d/sw-cp-server restart`.

Switching off weak SSL ciphers for connections to mail servers

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:*

```
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
```

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

1. Open for editing the file `/etc/postfix/main.cf`.
2. 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 = noplaintext
```

3. Save the file.
4. Restart the mail server by running the command `/etc/init.d/postfix restart`.

Prohibiting external access to the MySQL database server

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.

Protecting information about files

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`.
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`

Securing FTP access

➢ ***To prevent ProFTPd from showing information about its version on FTP connections:***

1. Open for editing the ProFTPd configuration file `/etc/proftpd.conf`.
2. Insert the following line into the file: `ServerIdent off`
3. Save the file.

If your ASV (Authorized Scanning Vendor) requires mitigating the BEAST attack as a PCI compliance requirement, you should additionally update the ciphers suite as described below:

1. Open for editing the file `/usr/local/psa/admin/conf/templates/pci_compliance/server/PCI_compliance.php`.
2. Locate the line `SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM`
3. Replace this line with the following one:

```
SSLCipherSuite !aNULL:!ADH:!eNULL:!LOW:!EXP:!MD5:ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4+RSA:+HIGH:+MEDIUM
```

4. Save the file.

If you allow FTP connections to your server, you must prohibit all FTP connections except secure FTPS connections.

➢ ***To allow only FTPS connections to your server:***

1. Go to **Tools & Settings** > **Security Policy**.
2. Select the option **Allow only secure FTPS connections** for **FTP usage policy**.
3. Select the option **Allow only secure FTPS connections** for **FTP usage policy**.

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.

Important: We highly recommend that you configure the Windows firewall in the server operating system to block all remote procedure calls (RPC) and communications to the Windows Management Instrumentation (WMI) services.

Securing Remote Desktop connections

Set up encryption of the remote desktop connections to prevent man-in-the-middle attacks. For instructions, refer to http://technet.microsoft.com/en-us/library/cc782610.aspx.

Changing Remote Desktop connections port

Some PCI scanners report a man in the middle attack if you do not change the RDP port to a custom value. To do it, compete the following steps:

1. Run the `regedit` utility by clicking **Start** > **Run**, typing *regedit*, and then clicking **OK**.
2. Change the port value by modifying the following registry key:
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp\PortNumber

Prohibiting access to MySQL database server from external addresses, use the firewall functions built into your Parallels Plesk Panel

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**.

Switching 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.

Securing FTP connections

If you allow FTP connections to your server, you must prohibit all FTP connections except secure FTPS connections.

➢ *To allow only FTPS connections to your server:*

1. Go to **Tools & Settings** > **Security Policy**.
2. Select the option **Allow only secure FTPS connections** for **FTP usage policy**.

CHAPTER 3

Tune Business Manager to Meet PCI DSS

There are twelve basic requirements (organized in six areas) which a merchant who uses Business Manager must meet in order to become certified as PCI DSS compliant. Each of these requirements, along with the POS vendor's recommendations, is noted in this chapter. However, you must familiarize yourself with the details of each requirement as set out in the PCI Data Security Standard documentation. (Refer to Section 4, **Resources**, for guidance on where to obtain more information.) The following table lists the twelve basic requirements.

- **Requirement 1**. Install and maintain a firewall configuration to protect cardholder data.
- **Requirement 2**. Do not use vendor-supplied defaults for system passwords and other security parameters.
- **Requirement 3**. Protect stored cardholder data.
- **Requirement 4**. Encrypt transmission of cardholder data across open, public networks.
- **Requirement 5**. Use and regularly update antivirus software.
- **Requirement 6**. Develop and maintain secure systems and applications.
- **Requirement 7**. Restrict access to cardholder data by business need-to-know.
- **Requirement 8**. Assign a unique ID to each person with computer access.
- **Requirement 9**. Restrict physical access to cardholder data.
- **Requirement 10**. Track and monitor all access to network resources and cardholder data.
- **Requirement 11**. Regularly test security systems and processes.
- **Requirement 12**. Maintain a policy that addresses information security.

Some of the requirements are met automatically, others require your input. This chapter explains how to change the Business Manager configuration to meet all the requirements. Please note that the sections in this chapter do not sequentially satisfy the given requirements. You should think of the following sections as recommendations: one section can help you meet two or more requirements at once, while other sections can assist with meeting the same requirement but for different parts of the system. Having this in mind, you should read through all the sections of this chapter to ensure you successfully meet all PCI DSS requirements.

In this chapter:

Remove Unprotected Sensitive Data After Upgrade

In accordance with the **PCS DSS Requirement 3.2**, Parallels Customer and Business Manager does not store sensitive authentication data: full magnetic stripes, card validation codes, or PIN block data. However, earlier versions of Parallels Customer and Business Manager may have stored card data insecurely in database log tables. Therefore, if you upgrade your Business Manager from earlier versions, be sure to clear these tables in order to meet the PCI compliance rules.

You must clear the following databases and then apply the `shred` utility to make the data unrecoverable via forensic methods:

- `callback_log`
- `dbg_entries`
- `mbapi_log`
- `source_log_col`
- `system_queue_log`

After clearing these tables, stop the application, back up the database, move it to a server which is not connected to the Internet, then use the `shred` utility to remove the database files and any old backups.

Troubleshooting

Securely delete any sensitive authentication data (pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other data sources received from customers, to ensure that magnetic stripe data, card validation codes or values, and PINs or PIN block data are not stored on software vendor systems. These data sources must be collected in limited amounts and only when necessary to resolve a problem. They must be encrypted while stored, and deleted immediately after use.

The following summarizes the basic guidelines on handling the information used for troubleshooting purposes:

- Collect sensitive authentication data only when needed to solve a specific problem.
- Store such data only in specific, known locations with limited access.
- Collect only the minimum amount of data needed to solve a specific problem.
- Encrypt sensitive authentication data while it is stored.
- Securely delete such data immediately after use.

Protect Stored Cardholder Data

Next in this section:

Purge Stale Cardholder Data

Cardholder data exceeding the customer defined retention period must be purged (see **PCI DSS Requirement 3.1**). In Business Manager, you can set up automatic purge of billing accounts that their owners did not use to pay for your services for a certain time. The control for switching this option on is available on the **Business Setup** > **All Settings** > **Billing Accounts Security** page.

To avoid losing billing accounts that are still in use, we recommend that you set the retention period that is a few days longer than the longest billing cycle of your plans. For example, if your customers pay for domain names once a year, your retention period may be about 370 days.

Securely Delete Cryptographic Material

The **PCI DSS Requirement 3.6.5** requires you to change the encryption key when the current one is suspected of being compromised, for example, is case of the departure of an employee that knows the passphrase. In Business Manager, this means that you should *renew* the encryption key and re-encrypt all data using this key.

➢ *To re-encrypt data with a new encryption key and remove old cryptographic material:*

1. Go to **Business Setup** > **All Settings** > **Encryptions Settings** > **Renew Key**.
2. Specify the new passphrase and other encryption settings:
   - **Private encryption key storage**: **Memory**.
   - **Owner of the encryption key:** an administrator account different from yours.
3. Click **Save**.

This will force the system to generate a new key and encrypt all cardholder data with the new key, thereby making the old key useless. To learn more about configuring encryption settings to comply withthe PCI DSS standard, see the section **Limiting Access to Cardholder Data** (on page 17).

Set Up Strong Access Control Measures

Next in this section:

Limiting Access to Cardholder Data

To meet a number of PCI DSS requirements on limiting access to cardholder data, Business Manager implements the security scheme described in this section.

In Business Manager, access to cardholder data can be granted only to administrators. The data itself is encrypted with a key consisting of two parts:

- *Private encryption key* that encrypts data itself.
- *Passphrase* that encrypts the private encryption key.

PCI DSS Requirement 3.6.6 states that these two parts of the key should be controlled by different owners, but, at the same time, the list of such owners should be as short as possible (see **PCI DSS Requirement 3.6.7**). In Business Manager, this means that the key parts should be owned by different administrators. For example, *admin* (the main Business Manager administrator) knows the passphrase while an additional administrator has access to the private key.

Note that to meet the **PCI DSS Requirement 3.5.2**, the key instance that is currently used by Business Manager should be stored in the server's memory (not on its hard disk).

To meet all the described requirements, configure encryption in Business Manager as described below.

➢ *To configure the encryption according to the PCI DSS:*

1. Go to **Business Setup** > **All Settings** > **Encryption Settings**.
2. Click **Turn On Encryption**.
3. Select the value **Memory** for the **Private encryption key storage** option.
4. Select another administrator account as the **Owner of the encryption key**. If there are no additional administrators in your system, add them on the **All Settings** > **Administrators** page.

   Both these administrators must learn your key management policies and sign a form stating that they understand and accept their key custodian responsibilities (see **PCI DSS requirement 3.6.8**).
5. Enter a passphrase and its confirmation.
6. Click **Turn On**.

Note: To make sure that you will not lose access to the cardholder data, you may distribute the key parts to 3-4 people - each only knowing one part of the key (passphrase or private key).

Administrative and Privileged Access to the Application

The use of unique user IDs for all users with access to sensitive cardholder data is required for PCI compliance. This requirement applies to administrative access to the application as well as server access to the application server or the database server.

Default server accounts must be secured or disabled. A password for the root database account must be set and restricted to local access only. This account should not be granted access to the billing database. Any default user account on these servers must also be secured, even if not being used.

The system will enforce the user's password rules as outlined in **Appendix A: PCI DSS Requirement 8** (on page 25). Some of these settings can be strengthened for application access on the System Configuration screen **Authentication and Password Management**. These settings cannot be disabled. Doing so will result in non-compliance.

General Non-privileged Access to the Application

Access to PCs, servers, and databases with payment applications must require unique user IDs and secure authentication for all users: employees and customers. **PCI Data Security Standard Requirements 8.1** and **8.2**.

- Hosting company employees can be given accounts with a specific list of privileges based on the employee's role within your company. These users should not be given access to customer billing accounts if such access is not needed for the employee to fulfill his duties for the hosting company. These privileges can be grouped by creating additional administrator groups from the **Business setup** > **All Settings** > **Administrators** page.
- Customers and resellers will automatically be granted a unique login when they sign up for service. These accounts are limited to the client interface, with restricted access to the clients' data only. The authentication settings for customers and resellers that you set on the **Business setup** > **All Settings** > **Authentication & Password Management** must comply with the items **8.5.9** to **8.5.13** from the **Appendix A: PCI DSS Requirement 8** (on page 25). Other parts of the **PCI DSS Requirement 8** that are related to customer and reseller authentication Business Manager meets automatically.

Monitor and Test Networks

PCI DSS Requirement 10 states that a payment application must implement an automated audit trail to track and monitor access to the application. To meet the requirement, Business Manager writes information about administrators' and customers' actions in the system to the *audit log*. This log is available in **Business Setup** > **All Settings** > **Audit Log**. On this page, administrators can view the log or download it in the CSV format.

The system rotates the audit log according to the frequency specified on the **Settings** tab of the **Business Setup** > **All Settings** > **Audit Log** page and saves old audit logs in the directory `/var/lib/plesk-billing/action-log/`.

Protect Wireless Transmissions

Next in this section:

Wireless Technology Included in or with the Payment Application

Business Manager does not utilize wireless technology.

According to **PCI DSS Requirement 1.2.3**, you must install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

General Use of Wireless Technology

If wireless technology is (or can be) used to store, process, or transmit cardholder data (for example, point-of-sale transactions, “line-busting”), or if a wireless local area network (WLAN) is connected to or part of the cardholder data environment (for example, is not clearly separated by a firewall), the PCI DSS requirements and testing procedures for wireless environments apply and must be put into effect (for example, **Requirements 1.2.3**, **2.1.1**, and **4.1.1**). Before wireless technology is implemented, a company should carefully evaluate the need for the technology against the risk. Consider deploying wireless technology only for non-sensitive data transmission.

Wireless environments must be implemented and maintained according to the following PCI DSS Requirements:

- **PCI DSS 1.2.3**: Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.
- **PCI DSS 2.1.1**: For wireless environments connected to the cardholder data environment or that transmit cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled with strong encryption technology for authentication and transmission.
- **PCI DSS 4.1.1**: Ensure that wireless networks that transmit cardholder data or are connected to the cardholder data environment use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.
  - For new wireless implementations, it has been prohibited to implement WEP since March 31, 2009.
  - For current wireless implementations, it has been prohibited to use WEP since June 30, 2010.

Keep Sensitive Data on a Separate Server

PA DSS 9.0: Cardholder data must never be stored on a server connected to the Internet. The default installation creates the database and all the required settings on the Plesk server. A separate server needs to be used as a dedicated database server. The steps required to move the database are as follows:

1. Move the Business Manager database to the new server.
2. Define the database server connection information on the Plesk server with the following command:

```
/usr/share/plesk-billing/billing-db --set --host=remote_host --name=remote_name --user=remote_db_user --password=remote_password
```

Important: After installation of Plesk Business Manager, a separate database server must be used as a database server. This server should only allow connections from the Plesk server and should not allow direct connections from the Internet.

Secure Remote Software Updates

Reference: **PA DSS 10.0**: Facilitate secure remote software updates.

Updates to Parallels Customer and Business Manager are initiated by the administrator from within Plesk. Updates are not automatically pulled down. The administrator initiates an update and the Plesk server pulls down code updates.

PCI Data Security Standard Requirements 1 and **12.3.9**.

Secure Remote Access to the System

Next in this section:

Two-factor Authentication

According to the **PCI DSS Requirement 8.3** (see **Appendix A: PCI DSS Requirement 8** (on page 25)) and the **PA DSS Requirement 10.1**, two-factor authentication should be used for the secure remote access of all users to the application.

Two-factor authentication implies using two of the following three authentication methods:

- Something you know (for example, a password).
- Something you have (for example, a smart card or a token).
- Something you are (for example, biometric information).

For example, you can configure SSH on your server so that logging in to the server requires entering a password (something you know) and providing a USB drive with a key (something you have).

Secure Remote Access Requirements

You should take the following actions to ensure that the requirements are met:

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).
- Allow connections only from specific (known) IP/MAC addresses.
- Allow connections only in specific time when you need them and restrict connections immediately after use.
- Use strong authentication and complex passwords for logins, according to **PCI DSS Requirements 8.1, 8.3**, and **8.5.8-8.5.15** (see **Appendix A: PCI DSS Requirement 8 (on page 25)** for details on PCI DSS Requirement 8).
- Enable encrypted data transmission according to **PCI DSS Requirement 4.1**.

  PCI DSS Requirement 4.1: Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are within the scope of PCI DSS are:

  - The Internet
  - Wireless technologies
  - Global System for Mobile communications (GSM)
  - General Packet Radio Service (GPRS)
- Enable account lockout after a certain number of failed login attempts according to **PCI DSS Requirement 8.5.13** (see **Appendix A** of this document for details on PCI DSS Requirement 8).
- Configure the system so a remote user must establish a *Virtual Private Network* (*"VPN"*) connection via a firewall before access is allowed.
- Enable the logging function.
- Restrict access to customer passwords to authorized reseller/integrator personnel.
- Establish customer passwords according to **PCI DSS Requirements 8.1**, **8.2**, **8.4**, and **8.5** (see **Appendix A** for detailed PCI DSS Requirements).

Encrypt Sensitive Traffic over Public Networks

Parallels Customer and Business Manager never sends unencrypted PANs via end-user messaging technologies (for example, e-mail, instant messaging, chat). Sensitive cardholder data is only transmitted over secure socket transmission to the merchant processors.

Encrypt all Non-console Administrative Access

Parallels Customer and Business Manager is only accessible via SSL browser connections. This must not be reconfigured on the server.

CHAPTER 4

Appendix A: PCI DSS Requirement 8

Assign a unique ID to each person with computer access.

- **PCI DSS 8.1**: Assign all users a unique ID before allowing them to access system components or cardholder data.
- **PCI DSS 8.2**: In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
  - Password or passphrase.
  - Two-factor authentication (for example, token devices, smart cards, biometric information, or public keys).
- **PCI DSS 8.3**: Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.
- **PCI DSS 8.4**: Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in the PCI DSS Glossary of Terms, Abbreviations and Acronyms).
- **PCI DSS 8.5**: Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:
  - **PCI DSS 8.5.1**: Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
  - **PCI DSS 8.5.2**: Verify user identity before performing password resets.
  - **PCI DSS 8.5.3**: Set first-time passwords to a unique value for each user and change immediately after first use.
  - **PCI DSS 8.5.4**: Immediately revoke access for any terminated users.
  - **PCI DSS 8.5.5**: Remove/disable inactive user accounts at least every 90 days.
  - **PCI DSS 8.5.6**: Enable accounts used by vendors for remote maintenance only during the time period needed.
  - **PCI DSS 8.5.7**: Communicate password procedures and policies to all users who have access to cardholder data.
  - **PCI DSS 8.5.8**: Do not use group, shared, or generic accounts and passwords.
  - **PCI DSS 8.5.9**: Change user passwords at least every 90 days.
  - **PCI DSS 8.5.10**: Require a minimum password length of at least seven characters.
  - **PCI DSS 8.5.11**: Use passwords containing both numeric and alpha characters.
  - **PCI DSS 8.5.12**: Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.

- **PCI DSS 8.5.13**: Limit repeated access attempts by locking out the user ID after not more than six attempts.
- **PCI DSS 8.5.14**: Set the lockout duration to a minimum of 30 minutes or until the administrator enables the user ID.
- **PCI DSS 8.5.15**: If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.
- **PCI DSS 8.5.16**: Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.