How Can Remote Desktop Manager Help You Become PCI Compliant

Devolutions

IF YOUR BUSINESS IS GOVERNED BY PCI DSS, THEN COMPLIANCE IS HIGH ON YOUR PRIORITY LIST.

PCI DSS is an acronym for Payment Card Industry Data Security Standard. It's a set of worldwide protection standards developed by major payment card companies, and it's mandatory for businesses that store, process, or transmit payment card data. Guidance is also provided to software, app and device creators that facilitate payment card transactions. It is intended to protect both consumers and businesses.

The consequences for companies that do not meet these requirements can be damaging in many ways. Without being PCI DSS compliant, companies would risk monetary loss, loss of client confidence, and they could incur legal costs, fines and penalties, and even bankruptcy. The PCI requirements, in other words, are not to be taken lightly.

Obviously, if your business is governed by PCI DSS, then compliance is high on your priority list. And guess what? **Remote Desktop Manager can help you meet the requirements that are bolded in the list below.**

Here are the 12 PCI DSS requirements:

1. Install and maintain a firewall configuration to protect cardholder data.
2. **Do not use vendor-supplied defaults for system passwords and other security parameters.**
3. **Protect stored cardholder data.**
4. Encrypt transmission of cardholder data across open, public networks.
5. Protect all systems against malware and regularly update anti-virus software or programs.
6. **Develop and maintain secure systems and applications.**
7. Restrict access to cardholder data by business justification (i.e., “need to know”).
8. **Identify and authenticate access to system components.**
9. Restrict physical access to cardholder data.
10. **Track and monitor all access to network resources and cardholder data.**
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

Number	Requirement	How Remote Desktop Manager (RDM) Helps
2	Do not use vendor-supplied defaults for system passwords and other security parameters.	By using RDM's Password Generator, you can easily generate random passwords that are strong, secure and virtually impossible to predict or guess. You can even make sure that nobody uses vendor-supplied default system passwords (like 123456 or qwerty) by adding them to your Forbidden Password list.
3	Protect stored cardholders data.	RDM helps your protect access to your servers where the data is stored.
6	Develop and maintain secure systems and applications.	Information stored within RDM is protected by a strong AES 256-bit encryption key. You can also control access by protecting your data source with 2-Factor authentication, or protect the application by using a passphrase.
8	Identify and authenticate access to system components.	RDM can help you manage security by creating a granular system of permissions which lets you select who has view, written or deleted access to your data.
10	Track and monitor all access to network resources and cardholder data.	The RDM session activity log captures all the information about your session activity, such as when it was opened, what actions were performed, and who performed them. Plus, if you're using Devolutions Server you can get real-time notification.

And there you go! PCI DSS compliance is essential, and we hope that RDM helps you cross some requirements off of your list. It's part of our commitment to making your life simpler, and helping you tame the IT chaos in your world.

As always, please let us know your thoughts by using the comment feature of the blog. You can also visit our forums to get help and submit feature requests, you can find them here.