PCI DSS and VNC Connect

Version 1.2

Contents

What is PCI DSS?

PCI DSS (Payment Card Industry Data Security Standard) compliance is mandated by many major credit card companies, including Visa, MasterCard, American Express, Discover and JCB, to ensure the safe handling of credit card information. To achieve PCI compliance, your business must adhere to the following security requirements:

Build and maintain a secure network	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
Protect cardholder data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security

How does VNC Connect enable PCI compliance?

With VNC Connect, your business can enjoy the business benefits of remote access without sacrificing PCI 3.2 compliance.

Note: No single piece of software makes your business PCI-compliant, nor is any software PCI-compliant in its own right. To achieve PCI compliance, your business must adhere in full to the security policies outlined in the table above; your choice of remote access software is merely one aspect of that.

Here's how VNC Connect meets each of the guidelines above:

Build and maintain a secure network

1. **Install and maintain a firewall configuration to protect cardholder data**

    a. VNC Connect does not require any inbound firewall configuration, meaning your existing PCI-compliant firewall need not be changed. If outbound rules are in place, certain domains must be whitelisted.

    b. In order to connect over the cloud, users must first create a RealVNC account. Administration of these accounts must be done on our web portal, which is only accessible via HTTPS on port 443.

    c. We store RealVNC account details on secure servers, which are protected by their own firewall. We never store connection-specific authentication credentials on these servers (these are only ever stored locally).

    d. VNC Connect allows system administrators to remotely install and configure a PCI-compliant firewall solution, if one has not already been established in your network.

2. **Do not use vendor-supplied defaults for system passwords and other security parameters**

    a. No default password is provided for any RealVNC service.

    In order to connect via the cloud, the user must first specify a RealVNC account password. We recommend this password is unique, and additionally recommend the use of a password manager such as Keypass.

    If the RealVNC account password *is* compromised, the malicious third party remains unable to connect. This is because each VNC Server computer also has its own unique password. By default, VNC Server is protected by system authentication, which mandates that the connecting user must enter the details they usually use to *log in* to that computer. If a malicious third party attempts to guess this password (via a brute force or dictionary attack), they are blacklisted after five unsuccessful attempts. The system administrator can configure this number.

    b. VNC Connect supports single sign-on.

    c. The VNC Viewer app, which is used to take control of remote computers, can be protected with a master password.

    d. By default, guest access to computers is disabled.

    e. VNC Connect supports two connection types: cloud and direct. If the user chooses, they can disable either of these.

    f. Any data we store, whether on RealVNC servers or PCI-compliant third-party servers, is locked behind unique and secure passwords.

Protect cardholder data

3. **Protect stored cardholder data**

    a. It is possible to transmit credit card information via remote access (e.g. via text chat or file transfer). These features can each be disabled by a system administrator.

4. **Encrypt transmission of cardholder data across open, public networks**

    a. VNC Connect uses the RFB 5 protocol, which mandates the use of modern cipher suites and uses strong cryptography throughout.

    b. All connections are protected by 128-bit or 256-bit AES-GCM encryption (depending on your settings and subscription type).

    c. All connections have perfect forward secrecy, ensuring they cannot be decrypted now or in the future.

    d. Access to our online portal is protected by mandatory TLS. We follow best practices for secure web development, and our website is graded A in the Qualys SSL Labs test.

Maintain a vulnerability management program

5. **Use and regularly update anti-virus software on all systems commonly affected by malware**

    a. VNC Connect is compatible with your existing PCI-compliant firewall/anti-virus software.

    b. Our own online infrastructure is similarly protected from malware.

6. **Develop and maintain secure systems and applications**

    a. We release free security updates for VNC Connect as and when new threats emerge. Any new code is subject to a security review before an update is pushed.

    b. VNC Connect will push update notifications to its users, ensuring you never miss these critical security updates.

    c. Our technical operations team monitors our online infrastructure 24 hours a day, 365 days a year. These systems are regularly patched. Any critical vulnerabilities in upstream dependencies are assessed and patched outside our regular patch schedule.

Implement strong access control measures

7. **Restrict access to cardholder data by business need-to-know**

    a. Separate access control lists regulate who can discover computers, who can connect to them, and what they can do once connected.

    - **Discovery**

      System administrators can use our web portal to determine which members of a team can discover which computers. If a user is unable to discover a computer, they cannot connect to it.

    - **Connectivity**

      System administrators can configure the VNC Server app to determine who has permissions to connect.

They can also determine which in-session features different users have access to (e.g. whether the connection is view only, or if they can transfer files).

b. The VNC Server computer can be configured to query connecting users. This means the local user is informed of - and must manually accept - each new connection.

8. Assign a unique ID to each person with computer access

a. As mentioned above, separate access control lists regulate who can discover and control which computers. We recommend you mandate that each user has a unique login, and you do not allow account sharing under any circumstances.

b. From the RealVNC website, you can remotely sign out of all VNC Viewer devices. This additionally removes cached data from each VNC Viewer device's Address book.

c. System administrators can choose how many authentication failures a user can make before they are blacklisted for a configurable amount of time.

d. By default, users are automatically disconnected when idle for one hour. System administrators can configure this limit.

e. PCI DSS mandates that any passwords used are at least seven characters long, and contain both alphabetic and numeric characters. When creating a RealVNC account, and when configuring our VNC Server or VNC Viewer apps, you can create a password which conforms to these restrictions.

f. VNC Connect can be protected by two factor authentication in the following places:

- When signing into the RealVNC web portal.
- When connecting to a VNC Server computer.

To see which two factor authentication mechanisms we use, please visit the relevant page on our website.

9. Restrict physical access to cardholder data

a. See *Restrict access to cardholder data by business need-to-know* above.

Regularly monitor and test networks

10. Track and monitor all access to network resources and cardholder data

a. VNC Server writes audits to the system log for every connection made, which are stored either locally or on a Domain Controller. A system administrator can configure the quality, quantity and destination of these logs.

b. If a RealVNC account's security settings (e.g. its password) are altered, an email is automatically sent to the user confirming these changes.

c. System administrators can choose how many authentication failures a user can make before they are blacklisted for a configurable amount of time.

d. From the RealVNC website, you can remotely sign out of all VNC Viewer devices. This additionally removes cached data from each device's Address book.

e. By default, users are automatically disconnected when idle for one hour. System administrators can change this limit.

11. Regularly test security systems and processes

a. Our dedicated security team are actively involved in VNC Connect’s maintenance, and have been involved throughout the entire software development lifecycle.

b. Based on our security team’s feedback, we release free security updates for VNC Connect as and when new threats emerge. Any new code is subject to a security review before an update is pushed.

Maintain an information security policy

12. Maintain a policy that addresses information security

a. By default, users are automatically disconnected when idle for one hour. System administrators can configure this limit or even turn it off.

b. If a system administrator deems specific features a security risk, they can disable them via policy. Examples may include remote printing, chat, or keyboard and mouse control.

If you have any questions about the topics raised in this paper, please contact us at privacy@realvnc.com.

RealVNC’s remote access and management software is used by hundreds of millions of people worldwide in every sector of industry, government and education. Our software helps organizations cut costs and improve the quality of supporting remote computers and applications. RealVNC is the original developer of VNC remote access software and supports an unrivalled mix of desktop and mobile platforms. Using our software SDKs, third-party technology companies also embed remote access technology direct into their products through OEM agreements.

www.realvnc.com