

Ensuring Desktop Central Compliance to Payment Card Industry (PCI) Data Security Standard



Introduction

Manage Engine Desktop Central is part of ManageEngine family that represents entire IT infrastructure with products such as Network monitoring, Helpdesk management, Application management, etc.

The Payment Card Industry Data Security Standard (PCI DSS) was developed to enhance cardholder data security. It facilitates the adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers. It also applies to entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

Under the PCI DSS, there are 12 different requirements concerning the security of cardholder data. All businesses that accept, store, process, or transmit card information online or offline must adhere to the requirements. Please refer to the following summary.

PCI DSS Overview


Requirement	Guidance
Build and Maintain Secure Network and Systems	<p>Install and maintain a firewall configuration to protect cardholder data</p> <p>Do not use vendor-supplied defaults for system passwords and other security parameters</p>
Protect Cardholder Data	<p>Protect stored cardholder data</p> <p>Encrypt transmission of cardholder data</p>



	across open, public network
Maintain a Vulnerability Management Program	<p>Protect all systems against malware and regularly update anti-virus software or programs</p> <p>Develop and maintain secure systems and applications</p>
Implement Strong Access Control Measures	<p>Restrict access to cardholder data by business need to know</p> <p>Identify and authenticate access to system components</p> <p>Restrict physical access to cardholder data</p>
Regularly Monitor and Test Networks	<p>Track and monitor all access to network resources and cardholder data</p> <p>Regularly test security systems and processes</p>
Maintain an Information Security Policy	Maintain a policy that addresses information security for all personnel

PCI DSS 3.0 Requirements Met by Desktop Central

Let us see how enterprises can use ManageEngine Desktop Central, the desktop and mobile device management solution, to comply with PCI DSS requirements. This document will help IT team gain an understanding of ManageEngine's Desktop Central and how it can help to meet PCI DSS requirements.



The following table outlines the PCI DSS control requirements that are fulfilled by Desktop Central. The requirement description listed is taken from the PCI Security Standards Council website.

(https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf)

Requirement	Requirement Description	How Desktop Central fulfills the requirement?
1.4	Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network.	<p>Desktop Central's software deployment helps IT admin install any kind of .exe or .msi applications, including firewall software. It will allow the IT admin to manage and monitor applications. This feature is supported for both Windows and Mac.</p> <p>For mobile devices, Desktop Central Mobile Device Management provides the ability to install firewall applications and allows IT admins to monitor the status of applications through an inventory console. Also, application management will restrict users from uninstalling applications deployed by Desktop Central, regardless of whether they are employee-owned or corporate-owned devices.</p>
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default	Desktop Central allows creating and configuring strong passwords to secure devices and prevent intruders from hacking the devices.



	accounts before installing a system on the network.	
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	Desktop Central scans desktops/servers/mobile devices in the network periodically to collect hardware and software details and stores them in the database. Then, IT admins will be able get up-to-date asset/inventory information in the form of reports with granular level details.
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Desktop Central allows IT admin to create a custom group (in this case, commonly affected systems) of systems and deploy anti-virus application to that particular group, ensuring system security.
5.1.2	For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	Desktop Central helps streamline the anti-virus definition update process and keeps a check on associated bandwidth costs. It also automates definition updates, which saves the administrator's time. These anti-virus definition updates include malwares and spywares in addition to traditional malicious software like viruses, trojans, and worms.
5.2	Ensure that all anti-virus mechanisms are maintained as follows: Are kept current	Desktop Central can detect and update outdated anti-virus software or patches. Also, Desktop Central provides exclusive support for MS Forefront Client Security



	<p>Perform periodic scans</p> <p>Generate audit logs which are retained per PCI DSS Requirement 10.7.</p>	Definitions.
6.1	<p>Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.</p>	<p>Desktop Central periodically scans the systems in the organization's network, identifies missing patches, and installs them based on system risk ranks such as healthy, vulnerable, and highly vulnerable. And, IT admin can use Desktop Central to customize these ranks.</p> <p>As a remediation action, IT admin can deploy patches based on the rank and ensure systems are secured with the latest patches.</p>
6.2	<p>Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release.</p>	<p>Using its vulnerability scanning and patch detection capabilities, Desktop Central Patch Management takes care of patch deployment based on missing Microsoft patches or system vulnerability. Also, Automatic Patch Deployment scheduler helps deploy security patches within one month of release (i.e. automation can be done to meet this requirement).</p> <p>After the patches are deployed, the agent applies relevant Windows and security patches in the system and updates the status in Desktop Central. The status can be downloaded in the form of reports for verification.</p>



7.1.1	<p>Define access needs for each role, including:</p> <p>System components and data resources that each role needs to access for their job function</p> <p>Level of privilege required (for example, user, administrator, etc.) for accessing resources.</p>	<p>Desktop Central's RBAC (Role Based Access Control) lets IT personnel to delegate routine activities to chosen users with well-defined permission levels. The IT manager can tailor make any number of roles and assign permissions based on policy needs and then associate these roles with Desktop Central Users.</p>
8.1.4	<p>Remove/disable inactive user accounts at least every 90 days.</p>	<p>Desktop Central notifies IT admins if the system is not active for the specified number of days. This notification ensures that the IT admin is updated about the status of the system in the enterprise network. The inactive users information can be viewed in the form of reports.</p>
8.1.6	<p>Limit repeated access attempts by locking out the user ID after not more than six attempts.</p>	<p>Desktop Central's Mobile Device Management helps the IT admin set permissible limits for the number of password attempts for the user. If the number of password attempt exceeds the limitation, the data present in the device will be wiped; this is only to maintain data confidentiality.</p> <p>Also, Desktop Central helps trace the number of failed password attempts.</p>
8.1.7	<p>Set the lockout duration to a minimum of 30 minutes or until an administrator enables</p>	<p>Desktop Central Mobile Device Management lets the IT admin specify the time limit for the device screen to be locked. If the device is idle for more than</p>



	the user ID.	the allowed time, the system gets locked automatically.
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	<p>Desktop Central's power management helps configure systems by enabling an option to prompt for password when the system is on Standby. The user can authenticate when the system resumes. The set configurations can be deployed to multiple systems from a central location, which gives the IT admin complete control.</p> <p>Also, remote session settings allow IT admin to configure maximum idle session time out, i.e. if the session exceeds the idle time, the session is disconnected, and the remote machine is locked automatically.</p>
8.2.3	<p>Passwords/phrases must meet the following:</p> <ul style="list-style-type: none">• Require a minimum length of at least seven characters• Contain both numeric and alphabetic characters.	<p>Desktop Central Mobile Device Management lets IT admins define parameters to create a passcode policy and configure passcode settings, such as numeric, alphabetic, password length, etc.</p> <p>For systems, Desktop Central provides an option to read the complexity of passwords.</p>
8.2.4	Change user passwords/passphrases at least every 90 days.	Desktop Central Mobile Device Management provides an option to specify the number of days for the passcode to be reset.




		For systems, the IT admin can configure alerts at specified dates in Desktop Central to notify the IT team based on which the team can take actions.
8.2.5	Do not allow an individual to submit a new password /phrase that is the same as any of the last four passwords /phrases he or she has used.	Desktop Central Mobile Device Management allows several passcodes to be maintained in the history, which means an IT admin can specify the number of previous passwords to be maintained, so that users do not reuse them.
9.7.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.	Desktop Central helps maintain hardware device usage logs, including USB device logs. This log information can be downloaded in the form of reports for audits and to find “who did what and when.”
11.2.1	Perform quarterly internal vulnerability scans and rescans as needed, until all “high-risk” vulnerabilities (As identified in requirement 6.1) are resolved. Scans must be performed by qualified personnel.	Patch Manager can perform system scanning with Desktop Central; it scans the entire system for missing patches in the operating system. The level of vulnerability is reported with details such as system vulnerability level, missing and applicable patches, task status, etc.
12.2	Implement a risk assessment process that: Is performed at least annually and upon	Desktop Central provides vulnerability scanning and Patch Management solution. The scanning results are also available as reports, which help to identify threats and keeps administrator updated.



	<p>significant changes to the environment.</p> <p>Identifies critical assets, threats, and vulnerabilities, and Results in a formal risk assessment.</p>	
12.3	<p>Develop usage policies for critical technologies and define proper use of these technologies.</p>	<p>Desktop Central lets IT admin implement policies such as configuring password and restricting the usage of Camera, YouTube, Safari Browser, etc. It also provides access to corporate accounts like email, Wi-Fi, VPN, and much more.</p> <p>Desktop Central helps secure and standardize desktops and devices across the network.</p>
12.3.4	<p>A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices).</p>	<p>Desktop Central's Inventory module provides comprehensive details about hardware and software details of the systems and devices present in the network.</p> <p>This includes hardware inventory details such as memory, operating system, manufacturer, device types, peripherals, etc. Software inventory includes details such as blacklisted application, license compliance, and software metering.</p>
12.3.8	<p>Automatic disconnect of sessions for remote-access technologies after a specific period of</p>	<p>Desktop Central's Idle session settings in the remote control tool can enhance security by specifying idle session time out.</p>



	inactivity.	An IT admin can specify the maximum time limit for the remote session to be idle. When the idle time limit exceeds the specified time, the session gets disconnected and the remote machine will be locked automatically.
12.3.9	Activation of remote access technologies for vendors and business partners only when needed vendors and business partners, with immediate deactivation after use.	With Desktop Central, the IT admin can create a separate login as and when needed. After the required troubleshooting or session is completed, the session can be deactivated.
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.	With Desktop Central's announcement feature, the IT admin can communicate information to the appropriate user as and when required.
12.5.4	Administer user accounts, including additions, deletions, and modifications.	Desktop Central's RBAC (Role Based Access Control) will enable to configure user roles, which includes role creation, modification, and deleting.
12.5.5	Monitor and Control all access to data.	Desktop Central enables the IT admin to restrict media devices such as USB for systems and SD card for mobile devices to ensure data is protected from leakage.



The essence of PCI DSS compliance is that vendors must demonstrate stringent security measures for systems and processes to protect cardholder information. The disadvantages of not following PCI DSS requirements are several; the brand and reputation of a business might suffer and the business might have to pay heavy penalties, if a data breach were to affect any customer's payment card data.

Desktop Central helps businesses stay compliant with PCI DSS. It facilitates monitoring and managing systems & mobile devices and provides granular level reports. To know more about Desktop Central, visit www.desktopcentral.com