



Using op5 Log Server for PCI Certification

The Payment Card Industry Security Standard is a joint standard and today accepted and adopted by Visa, MasterCard, American Express, Diners Card and JCB. The standard describes how credit card numbers and transaction information should be handled. This includes any kind of physical credit card transaction whether it is post, telephone or e-shops.

The overall purpose for PCI is to assure that the card or transaction data is handled in way so that no unauthorised personal can access the information.

The op5 LogServer - where it fits

The op5 LogServer is the perfect way to collect, store and search all the necessary logs created from the multiple of infrastructure involved in the card transactions. This includes logs from firewalls, authentication applications, web servers, ERP-system etc. All logs are automatically forwarded to the central op5LogServer where they are stored in a SQL database. This enables both traceability and secure storage of the sensitive log data. Efficient and secure handling of logdata is a key component for complying to the PCI Security Standards. op5 LogServer delivers just that.

Who is affected and how?

The PCI standards applies to all companies handling credit cards. The standard stipulates some basic criteria:

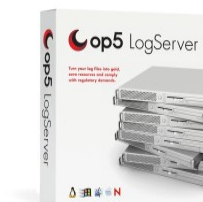
Level	Criteria	On-site Audit	Self Assessment	Network Security Scan
1	Companies with more than 6 million card transactions.	Yearly	No	Per quarter
2	Companies with 1-6 million card transactions	No	Yearly	Per quarter
3	Companies with 20k to 1 million card transactions	No	Yearly	Per quarter
4	The rest, below 30k transactions	No	Recommended yearly	Recommended yearly

Using op5 LogServer in complying to the PCI Standard.

The standard includes a full set of rules and regulations covering both technical aspects as well as process and procedures. For the complete list please see:

https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html

The op5 LogServer is the supporting solution for complying with:



Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Focusing on the R10 and R11 it includes multiple of tasks that can be broken in three main categories.

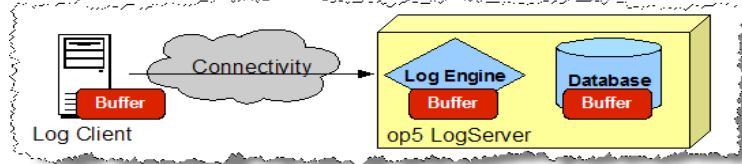
- Performing the actual logging tasks
- Reading the logs and creating the necessary actions
- Notifications

Make sure not to loose any logs - Smart Log Buffering

A lost log is not acceptable. Unfortunately network can be broken, connections can be congested etc. op5 LogServer support Smart Log Buffering.

This includes buffering at:

- Client to server, buffer and logs locally if there is no connection to the LogServer.
- Server to database, buffer the recived logs on disk before inserting into database.



The architecture of the op5 NMS that includes op5 LogServer, op5 Monitor and op5 Statistics.

Based on the requirements detailed in the Payment Card Industry (PCI) Data Security Standard, Version 1.1 Release: September, 2006 (the latest published) op5 fully support the requirement as showed in the list below.

op5 LogServer security features

op5 LogServer supports UDP & TCP log traffic between the logging host and the central LogServer. We also support TLS based encryption and with X.509 Certificate authentication.

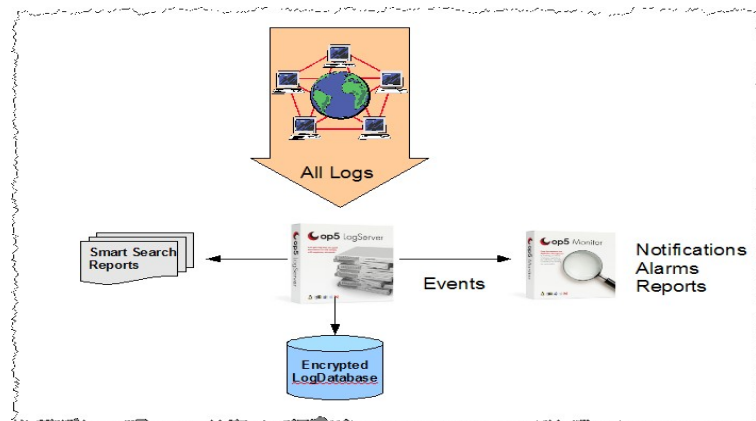
Next step: Demo or download for full trial

All op5 products are available for full demo or download. For more information:

- [Product information](#)
- [Screenshots from op5Log Server](#)
- [Sandbox](#)
- [Full Download](#)

PCI DSS Req	Testing Procedure	Op5 Product	Comments
10.1		Logserver	Help support the process by logging access
10.2.1		Logserver	Help auditing by logging
10.2.2		Logserver	Help auditing by logging
10.2.3		Logserver	Help auditing by logging
10.2.4		Logserver	Help auditing by logging
10.2.5		Logserver	Help auditing by logging
10.2.6		Logserver	Help auditing by logging
10.2.7		Logserver	Help auditing by logging
10.3.1		Logserver	Contained in log message
10.3.2		Logserver	Contained in log message
10.3.3		Logserver	Contained in log message
10.3.4		Logserver	Contained in log message
10.3.5		Logserver	Contained in log message
10.3.6		Logserver	Contained in log message
10.4	10.4.a	Monitor	Monitor can verify NTP
	10.4.b	Monitor	
	10.4.c	Monitor	
10.5		Logserver	By having two or more logservers, where one is locked in and only administrated from console the alternation of logs are impossible
10.5.1		Logserver	Only give the trusted admins user rights
10.5.2		Logserver	By having two or more logservers, where one is locked in and only administrated from console the alternation of logs are impossible
10.5.3		Logserver	By having two or more logservers, where one is locked in and only administrated from console the alternation of logs are impossible
10.5.4		Logserver	
10.5.5		Logserver/Monitor	By having two or more logservers, where one is locked in and only administrated from console the alternation of logs are impossible. Combined with Op5 monitor an alert can be generated if someone logs in.
10.6		Logserver	With a centralized Logserver makes it possible to review logs, without it is impossible
10.7		Logserver	
11.4	11.4.a	Logserver	Let NIDS and HIDS log to Logserver and with a centralized Logserver makes it possible to review logs, without it is impossible

Please go to: www.op5.com.



Summary

The op5 LogServer in provides the necessary functionality for upholding the PCI requirements as set forth in the v1.1. In the specific events were a notification is required this can either be supported by op5 Monitor or by any 3rd party management software enabled to perform the tasks.

Sources:

The PCI Security Standard: <https://www.pcisecuritystandards.org/index.shtml>

About op5 – www.op5.com

Our business concept is to offer the market the most cost effective solution for IT support organizations. We utilize the power and efficiency of Open Source as the prime component in our product development. Op5 has more than 300 satisfied customers in Scandinavia.

For further information please contact us on +46-8-23 02 25 or info@op5.com, www.op5.com