Print Audit 6

Print Audit 6 Security Overview

Version: 25
Date: 03-Dec-2018 17:19

Table of Contents

Database

- Microsoft Access databases are password protected and cannot be opened in Microsoft Access without the password.

- SQL databases are password protected by default and can utilize all of the security features of the Microsoft SQL Server platform if desired (including Windows/Integrated security).

Print Audit Applications

- The Administrator includes the ability to create different user security profiles. Some users can be granted full access to the system, others read-only access (for reporting), and others can be denied access except the ability to track their printing.

- Users can be prompted to enter either a secure PIN code or their network password to gain access to the administrator and reporting tools.

- Users can be prompted to enter either a secure PIN code or their network password for validation in order to print.

- PIN codes are stored in the database in encrypted form, never in clear text.

- Users can be authenticated against an Active Directory or Novell NDS server if desired.

Data

- All data is stored in the SQL or Microsoft Access database. The data is as secure as the network / server on which it resides.

Network

- Communication between the clients and the Database Communicator occurs on a single TCP port (17520 by default). This port number can be changed if desired.

- Strong encryption is used for all data transmissions between the client and Database Communicator.

Internet-Based License Activation

- Normally, Print Audit 6 licenses are activated via our secure licensing server using the HTTPS protocol. If it is not possible or desirable to activate over the Internet, the license can be activated manually.

Privacy

- No data is transmitted to third parties. Print Audit can be configured to not track the document names and / or user names for each print job.